
주요정보통신기반시설 기술적 취약점 분석 · 평가 방법 상세가이드

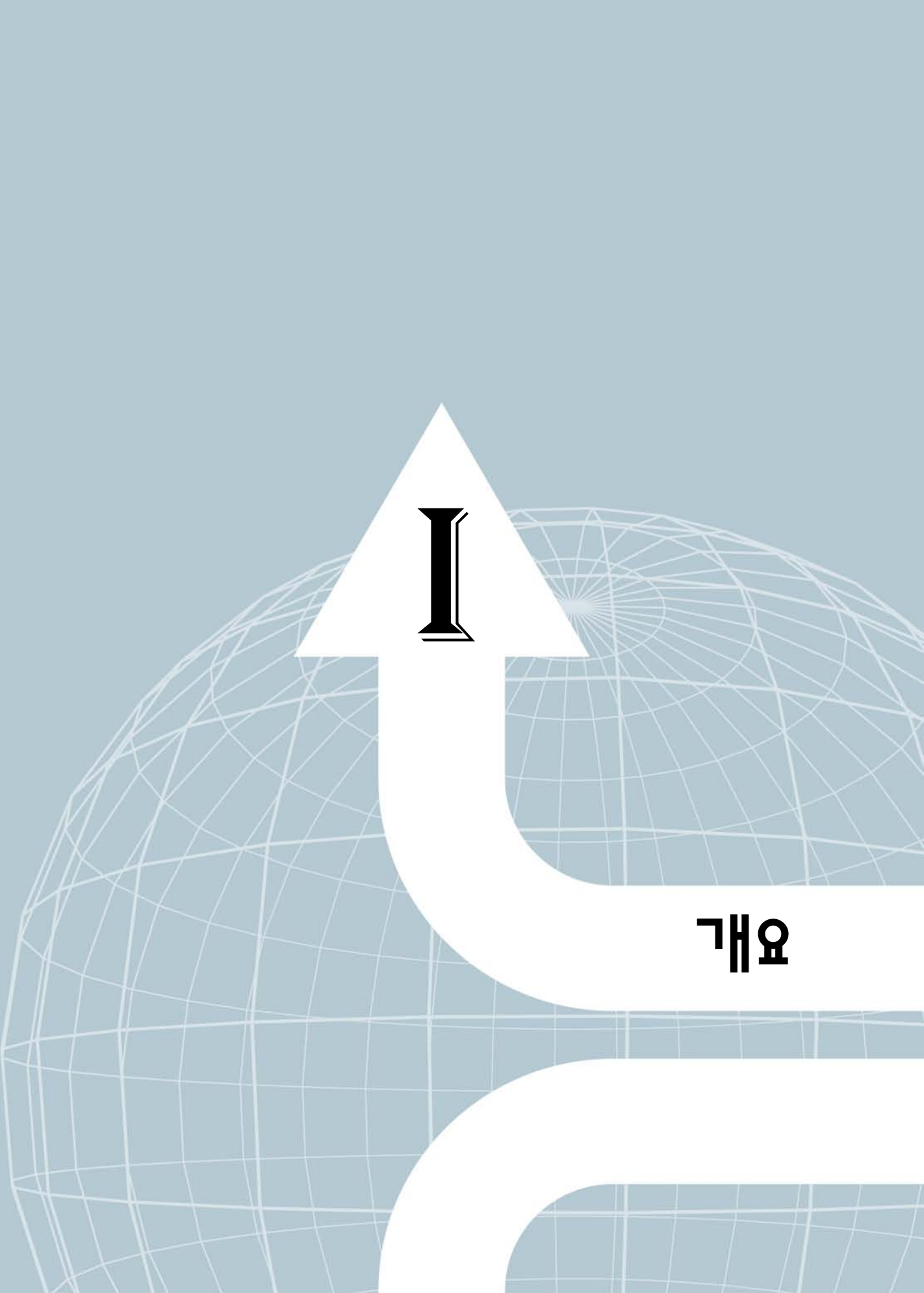
2014. 01.



안전행정부

KISA

한국인터넷진흥원
Korea Internet & Security Agency



I

개요

개요

1. 개요

「정보통신기반 보호법」 제9조에 따라, 주요정보통신기반시설 관리기관은 매년 취약점 분석·평가를 실시하여야 한다. 취약점 분석·평가는 453개의 관리적/물리적/기술적 점검항목에 대한 취약여부를 점검하고 모의해킹, 침투테스트 등을 수행하는 종합적인 위험진단에 해당한다.

한편 취약점 분석·평가를 수행함에 있어 기술적 점검은, 시스템에 대한 실제 보안값 설정에 관한 것으로 각 시스템에 대한 명령어 코드(Command), 메뉴 구성(UI)과 같은 기술적인 사항을 알아야만 가능하기에, 주요정보통신기반시설 담당자들의 어려움이 따르게 된다.

이러한 기술적 점검에 대한 어려움을 해소하고 주요정보통신기반시설 담당자들의 이해를 돕기 위해, 안전행정부는 전체 313개 기술적 점검항목에 대한 점검방법 및 조치방법 상세 매뉴얼을 개발하게 되었다.

각각의 점검항목이 의미하는 위험내역 설명과 함께, 점검방법 및 조치방법을 실제 시스템 입력화면 등을 활용하여 상세 설명하였으며, 특정 벤더사의 제품으로 한정하지 않고 대표적인 벤더사 제품별로 구분하여 설명을 제시하였다.

2. 목적 및 구성

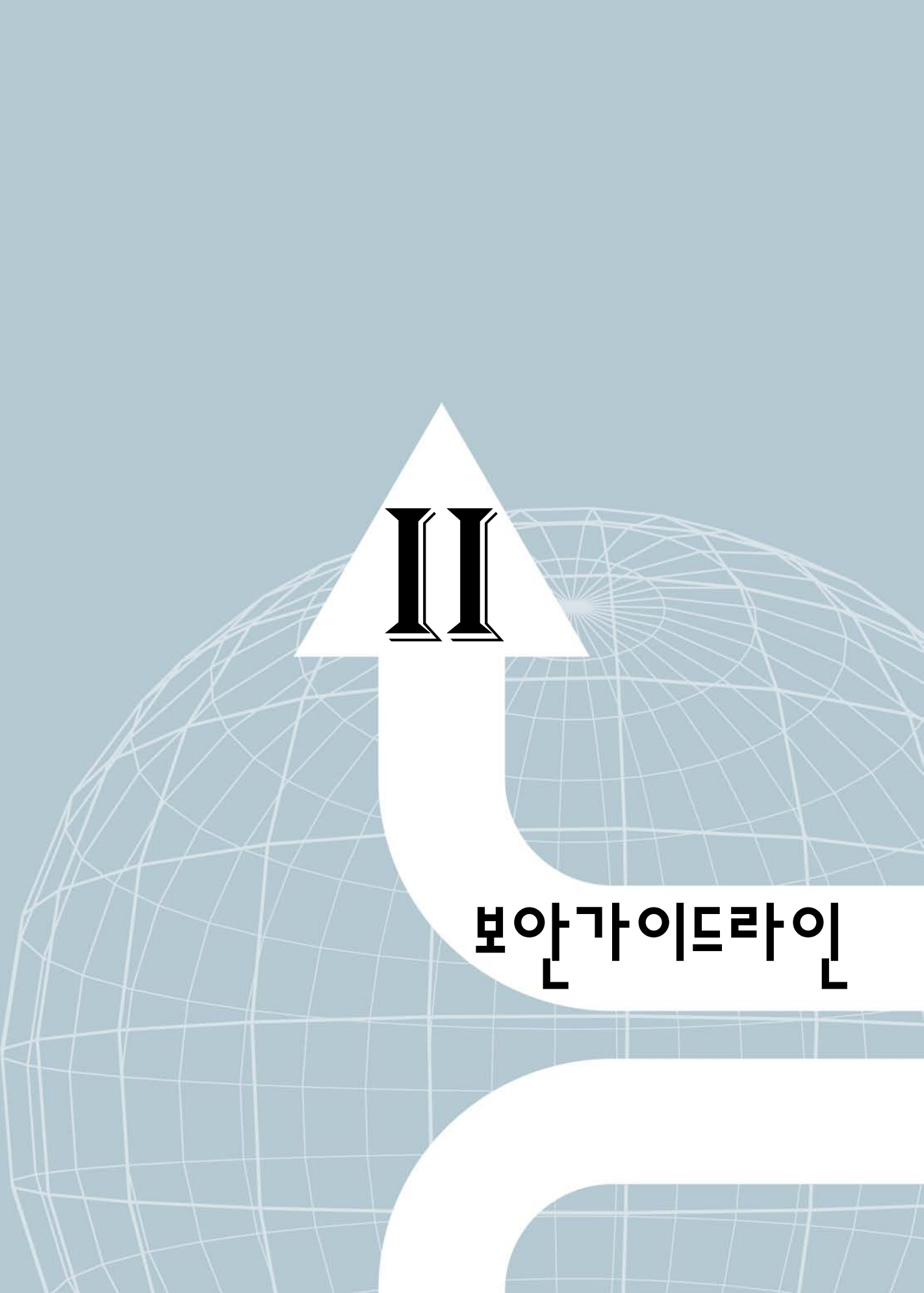
목적 주요정보통신기반시설 담당자의 기반시설 보호 역량강화를 위한 기술가이드 제공

대상 주요정보통신기반시설 담당자

범위 주요정보통신기반시설 기술적 취약점 분석·평가

구성 기술적 점검 기준(313개 항목)의 항목 설명, 점검(설정확인)방법, 조치방법 (Unix, Windows, 보안장비, 네트워크장비, 제어시스템, PC, DBMS, Web)

활용 주요정보통신기반시설 기술적 취약점 보안조치 시 활용



II

보안 가이드라인

Unix 서버 보안가이드라인

2014. 01



안전행정부 *희망의 새시대*

Unix 서버 취약점 분석·평가 항목

분류	점검항목	항목 중요도	항목코드
1. 계정관리	root 계정 원격 접속 제한	상	U-01
	패스워드 복잡성 설정	상	U-02
	계정 잠금 임계값 설정	상	U-03
	패스워드 파일 보호	상	U-04
	root 이외의 UID가 '0' 금지	중	U-05
	root 계정 su 제한	하	U-06
	패스워드 최소 길이 설정	중	U-07
	패스워드 최대 사용 기간 설정	중	U-08
	패스워드 최소 사용기간 설정	중	U-09
	불필요한 계정 제거	하	U-10
	관리자 그룹에 최소한의 계정 포함	하	U-11
	계정이 존재하지 않는 GID 금지	하	U-12
	동일한 UID 금지	중	U-13
	사용자 shell 점검	하	U-14
	Session Timeout 설정	하	U-15
2. 파일 및 디렉터리 관리	root 홈, 패스 디렉터리 권한 및 패스 설정	상	U-16
	파일 및 디렉터리 소유자 설정	상	U-17
	/etc/passwd 파일 소유자 및 권한 설정	상	U-18
	/etc/shadow 파일 소유자 및 권한 설정	상	U-19
	/etc/hosts 파일 소유자 및 권한 설정	상	U-20
	/etc/(x)inetd.conf 파일 소유자 및 권한 설정	상	U-21
	/etc/syslog.conf 파일 소유자 및 권한 설정	상	U-22
	/etc/services 파일 소유자 및 권한 설정	상	U-23
	SUID,SGID,Stick bit 설정 파일 점검	상	U-24
	사용자, 시스템 시작파일 및 환경파일 소유자 및 권한 설정	상	U-25
	world writable 파일 점검	상	U-26
	/dev에 존재하지 않는 device 파일 점검	상	U-27
	HOME/.rhosts, hosts.equiv 사용 금지	상	U-28
	hosts.lpd 파일 소유자 및 권한 설정	하	U-29
	NIS 서비스 비활성화	중	U-30
	UMASK 설정 관리	중	U-31
	홈디렉토리 소유자 및 권한 설정	중	U-32
	홈디렉토리로 지정한 디렉토리의 존재 관리	중	U-33
	숨겨진 파일 및 디렉토리 검색 및 제거	하	U-34
3. 서비스 관리	접속 IP 및 포트 제한	상	U-35
	finger 서비스 비활성화	상	U-36
	Anonymous FTP 비활성화	상	U-37

	r 계열 서비스 비활성화	상	U-38
	cron 파일 소유자 및 권한설정	상	U-39
	Dos 공격에 취약한 서비스 비활성화	상	U-40
	NFS 서비스 비활성화	상	U-41
	NFS 접근 통제	상	U-42
	automountd 제거	상	U-43
	RPC 서비스 확인	상	U-44
	NIS , NIS+ 점검	상	U-45
	tftp, talk 서비스 비활성화	상	U-46
	Sendmail 버전 점검	상	U-47
	스팸 메일 릴레이 제한	상	U-48
	일반사용자의 Sendmail 실행 방지	상	U-49
	DNS 보안 버전 패치	상	U-50
	DNS Zone Transfer 설정	상	U-51
	Apache 디렉토리 리스팅 제거	상	U-52
	Apache 웹 프로세스 권한 제한	상	U-53
	Apache 상위 디렉토리 접근 금지	상	U-54
	Apache 불필요한 파일 제거	상	U-55
	Apache 링크 사용 금지	상	U-56
	Apache 파일 업로드 및 다운로드 제한	상	U-57
	Apache 웹 서비스 영역의 분리	상	U-58
	ssh 원격접속 허용	중	U-59
	ftp 서비스 확인	하	U-60
	ftp 계정 shell 제한	중	U-61
	Ftpusers 파일 소유자 및 권한 설정	하	U-62
	Ftpusers 파일 설정	중	U-63
	at 파일 소유자 및 권한 설정	중	U-64
	SNMP 서비스 구동 점검	중	U-65
	SNMP 서비스 커뮤니티스트링의 복잡성 설정	중	U-66
	로그온 시 경고 메시지 제공	하	U-67
	NFS설정파일접근권한	중	U-68
	expn, vrfy 명령어 제한	중	U-69
	Apache 웹서비스 정보 숨김	중	U-70
4. 패치 관리	최신 보안패치 및 벤더 권고사항 적용	상	U-71
5. 로그 관리	로그의 정기적 검토 및 보고	상	U-72
	정책에 따른 시스템 로깅 설정	하	U-73

UNIX 서버

1. 계정 관리

취약점 항목		1.1. root 계정 원격 접속 제한			
대상 OS	SunOS, LINUX, AIX, HP-UX	위험도	상	Code	U-01
취약점 개요	*root는 시스템을 관리하는 매우 중요한 계정임. root 계정으로 직접 로그인하도록 허용하면 불법적인 침입자의 목표가 될 수 있으므로 root 계정 접속에 대한 관리가 필요함. root 계정의 원격 접속 허용은 공격자에게 더 좋은 기회를 제공할 수 있으므로 root의 원격 접속은 금지하여야 함.				
	*root 계정: 여러 사용자가 사용하는 컴퓨터에서 전체적으로 관리할 수 있는 총괄 권한을 가진 유일한 특별 계정. 유닉스 시스템의 루트(root)는 시스템 관리자인 운용 관리자(Super User)로서 윈도우의 관리자(Administrator)에 해당하며, 사용자 계정을 생성하거나 소프트웨어를 설치하고, 환경 및 설정을 변경하거나 시스템의 동작을 감시 및 제어할 수 있음.				
보안대책					
판단기준	양호: 원격 서비스를 사용하지 않거나, 사용 시 root 직접 접속을 차단한 경우 취약: root 직접 접속을 허용하고 원격 서비스를 사용하는 경우				
조치방법	원격 접속 시 root 계정으로 바로 접속 할 수 없도록 설정파일 수정				
보안설정방법					
OS별 점검 파일 위치 및 점검 방법					
SunOS	#cat /etc/default/login CONSOLE=/dev/console				
LINUX	#cat /etc/pam.d/login auth required /lib/security/pam_securetty.so #cat /etc/securetty pts/0 ~ pts/x 관련 설정이 존재하지 않음				
AIX	#cat /etc/security/user rlogin = false				
HP-UX	#cat /etc/securetty console				
위에 제시한 설정이 해당 파일에 적용되지 않은 경우 아래의 보안설정방법에 따라 설정을 변경함					
■ SunOS					
1. vi 편집기를 이용하여 "/etc/default/login" 파일을 연 후					
2. 아래와 같이 주석 제거 또는, 신규 삽입					
(수정 전) #CONSOLE=/dev/console					
(수정 후) CONSOLE=/dev/console					
<pre># If CONSOLE is set, root can only login on that device. # Comment this line out to allow remote login by root. # CONSOLE=/dev/console</pre>					

UNIX 서버

■ LINUX

1. "/etc/securetty" 파일에서 pts/0 ~ pts/x 설정 제거 또는, 주석 처리
2. "/etc/pam.d/login" 파일 수정

(수정 전) #auth required /lib/security/pam_securetty.so

(수정 후) auth required /lib/security/pam_securetty.so

※ /etc/securetty : Telnet 접속 시 root 접근 제한 설정 파일

"/etc/securetty" 파일 내 *pts/x 관련 설정이 존재하는 경우 PAM 모듈 설정과 관계없이 root 계정 접속을 허용하므로 반드시 "securetty" 파일에서 pts/x 관련 설정 제거 필요



USER	TTY	FROM	LOGIN@	IDLE	JCPU	PCPU	WHAT
root	tty1	-	02:34	11:59m	1:37	0.09s	-bash
root	pts/0	-	02:34	11:59m	0.17s	0.17s	/bin/bash
root	pts/1	192.168.100.254	11:11	15.00s	11.02s	10.95s	telnet
root	pts/2	192.168.100.254	08:52	3:28m	0.35s	0.35s	-bash
root	pts/3	192.168.100.254	11:12	23.00s	10.69s	10.63s	telnet
root	pts/4	192.168.100.254	14:05	0.00s	0.40s	0.04s	w
root	pts/5	192.168.100.254	12:50	56:07	0.56s	0.30s	vim .bash_profile

*pts/0 ~ pts/x 설정:

tty(terminal-teletype) : 서버와 연결된 모니터, 키보드 등을 통해 사용자가 콘솔로 직접 로그인함

pts(pseudo-terminal, 가상터미널) : Telnet, SSH, 터미널 등을 이용하여 접속함

■ AIX

1. vi 편집기를 이용하여 "/etc/security/user" 파일을 연 후
2. *rlogin 설정을 아래와 같이 수정 또는, 신규 삽입 (root 설정에 해당되는 부분 수정)

(수정 전) rlogin = true

(수정 후) rlogin = false

*rlogin(remote-login): 자주 접속하는 호스트에 대해 자동으로 원격 접속을 할 수 있도록 사용하는 명령어

■ HP-UX

1. vi 편집기를 이용하여 "/etc/securetty" 파일을 연 후
2. 아래와 같이 주석 제거 또는, 신규 삽입

(수정 전) #console

(수정 후) console

※ "/etc/securetty" 파일은 디폴트로 존재하지 않으므로 /etc 디렉터리 내에 "securetty" 파일이 존재하지 않는 경우 새로 생성한 후 적용함 (※ vi 편집기를 사용한 파일 생성: 부록 참고)

#vi /etc/securetty

조치 시 영향	일반적으로 영향 없음
---------	-------------

UNIX 서버

취약점 항목		1.2. 패스워드 복잡성 설정			
대상 OS	SunOS, LINUX, AIX, HP-UX	위험도	상	Code	U-02
취약점 개요	사용자 계정(root 및 일반 계정 모두 해당) 암호를 유추하기 쉽게 설정할 경우 비인가자의 시스템 접근을 허용하게 하는 위험이 존재함. 여러 문자를 혼합한 8자리 이상의 암호를 사용하게 하여 패스워드 복잡성을 높이면 비인가자에 의해 발생하는 침입 공격 발생률을 낮출 수 있음.				
보안대책					
판단기준	양호: 영문·숫자·특수문자가 혼합된 8자리 이상의 패스워드가 설정된 경우 취약: 영문·숫자·특수문자 혼합되지 않은 8자 미만의 패스워드가 설정된 경우				
조치방법	계정과 유사하지 않은 8자 이상의 영문, 숫자, 특수문자의 조합으로 암호 설정				
보안설정방법					
OS별 점검 파일 위치 및 점검 방법					
SunOS, LINUX, HP-UX		/etc/shadow 파일 내 설정된 패스워드 점검			
AIX		/etc/security/passwd 파일 내 설정된 패스워드 점검			
OS별 점검 파일을 열어 패스워드를 확인 한 후 아래의 보안설정방법에 따라 설정을 변경함					
■ SunOS, LINUX, AIX, HP-UX					
< 부적절한 패스워드 유형 >					
1. 사전에 나오는 단어나 이들의 조합					
2. 길이가 너무 짧거나, NULL(공백)인 패스워드					
3. 키보드 자판의 일련의 나열 (예) abcd, qwert, etc					
4. 사용자 계정 정보에서 유추 가능한 단어들 (예) 지역명, 부서명, 계정명, 사용자 이름의 이니셜, root, rootroot, root123, admin 등					
< 패스워드 관리 방법 >					
1. 영문, 숫자, 특수문자를 조합하여 계정명과 상이한 8자 이상의 패스워드 설정					
※ 다음 각 목의 문자 종류 중 2종류 이상을 조합하여 최소 10자리 이상 또는, 3종류 이상을 조합하여 최소 8자리 이상의 길이로 구성					
가. 영문 대문자(26개)					
나. 영문 소문자(26개)					
다. 숫자(10개)					
라. 특수문자(32개)					
2. 시스템마다 상이한 패스워드 사용					
3. 패스워드를 기록해 놓을 경우 변형하여 기록					
4. 가급적 자주 패스워드를 변경할 것					
조치 시 영향	패스워드 변경 시 Web, Was, DB연동 구간에서 문제가 발생할 수 있으므로 연동 구간에 미칠 수 있는 영향을 고려하여 적용 필요				

UNIX 서버

취약점 항목		1.3. 계정 잠금 임계값 설정			
대상 OS	SunOS, LINUX, AIX, HP-UX	위험도	상	Code	U-03
취약점 개요	침입자에 의한 패스워드 *무작위 대입 공격(Brute Force Attack)이나 패스워드 추측 공격>Password Guessing) 발생 시 암호입력 실패 횟수를 적정하게 제한함으로써 자동공격을 차단하고 공격 시간을 지체시켜 패스워드 유출 위험을 줄일 수 있음. *무작위 대입 공격(Brute Force Attack): 컴퓨터로 암호를 해독하기 위해 가능한 모든 키를 하나하나 추론해 보는 시도를 말함.				
보안대책					
판단기준	양호: 계정 잠금 임계값이 5 이하의 값으로 설정되어 있는 경우 취약: 계정 잠금 임계값이 설정되어 있지 않거나, 5 이하의 값으로 설정되지 않은 경우				
조치방법	계정 잠금 임계값을 5 이하로 설정				
보안설정방법					
OS별 점검 파일 위치 및 점검 방법					
SunOS	#cat /etc/default/login RETRIES=5 SunOS 5.9 이상 버전일 경우 추가적으로 "policy.conf" 파일 확인 #cat /etc/security/policy.conf LOCK_AFTER_RETRIES=YES				
LINUX	#cat /etc/pam.d/system-auth auth required /lib/security/pam_tally.so deny=5 unlock_time=120 no_magic_root account required /lib/security/pam_tally.so no_magic_root reset				
AIX	#cat /etc/security/user loginretries=5				
HP-UX	#cat /tcb/files/auth/system/default u_maxtries#5				

위에 제시한 설정이 해당 파일에 적용되지 않은 경우 아래의 보안설정방법에 따라 설정을 변경함

■ SunOS

- SunOS 5.9 이하 버전 -

1. vi 편집기를 이용하여 "/etc/default/login" 파일을 연 후

2. 아래와 같이 수정 또는, 신규 삽입

(수정 전) #RETRIES=2

(수정 후) RETRIES=5

- SunOS 5.9 이상 버전 -

1. vi 편집기를 이용하여 "/etc/default/login" 파일을 연 후

UNIX 서버

- 아래와 같이 수정 또는, 신규 삽입 (계정 잠금 횟수 설정)
(수정 전) #RETRIES=2
(수정 후) RETRIES=5
- vi 편집기를 이용하여 "/etc/security/policy.conf" 파일을 연 후
- 아래와 같이 수정 또는, 신규 삽입 (계정 잠금 정책사용 설정)
(수정 전) #LOCK_AFTER_RETRIES=NO
(수정 후) LOCK_AFTER_RETRIES=YES

■ LINUX

- vi 편집기를 이용하여 "/etc/pam.d/system-auth" 파일을 연 후
- 아래와 같이 수정 또는, 신규 삽입
auth required /lib/security/pam_tally.so deny=5 unlock_time=120 no_magic_root
account required /lib/security/pam_tally.so no_magic_root reset

옵션	설명
no_magic_root	root에게는 패스워드 잠금 설정을 적용하지 않음
deny=5	5회 입력 실패 시 패스워드 잠금
unlock_time	계정 잠금 후 마지막 계정 실패 시간부터 설정된 시간이 지나면 자동 계정 잠금 해제 (단위: 초)
reset	접속 시도 성공 시 실패한 횟수 초기화

■ AIX

- vi 편집기를 이용하여 "/etc/security/user" 파일을 연 후
- 아래와 같이 수정 또는, 신규 삽입
(수정 전) loginretries = 0
(수정 후) loginretries = 5

■ HP-UX

- vi 편집기를 이용하여 "/tcb/files/auth/system/default" 파일을 연 후
- 아래와 같이 수정 또는, 신규 삽입
(수정 전) u_maxtries#
(수정 후) u_maxtries#5

※ HP-UX 서버에 계정 잠금 정책 설정을 위해서는 HP-UX 서버가 Trusted Mode로 동작하고 있어야하므로 Trusted Mode로 전환한 후 잠금 정책 적용

조치 시 영향

Trusted Mode로 전환 시 파일시스템 구조가 변경되어 운영 중인 서비스에 문제가 발생할 수 있으므로 충분한 테스트를 거친 후 Trusted Mode로의 전환이 필요함

UNIX 서버

취약점 항목		1.4. 패스워드 파일 보호			
대상 OS	SunOS, LINUX, AIX, HP-UX	위험도	상	Code	U-04
취약점 개요	패스워드 정보를 평문으로 저장하는 경우 정보 유출 피해가 발생할 수 있으므로 패스워드를 암호화하여 보호하여야 함. 쉘도우 패스워드를 사용하여 "/etc/shadow" 파일에 암호화된 패스워드가 저장되도록 하고 특별 권한이 있는 사용자들만 읽을 수 있도록 제한함.				
보안대책					
판단기준	양호: 쉘도우 패스워드를 사용하거나, 패스워드를 암호화하여 저장하는 경우				
	취약: 쉘도우 패스워드를 사용하지 않고, 패스워드를 암호화하여 저장하지 않는 경우				
조치방법	패스워드 암호화 저장·관리 설정 적용				
보안설정방법					
OS별 점검 파일 위치 및 점검 방법					
SunOS, LINUX	1. /shadow 파일 존재 확인 (일반적으로 /etc디렉터리 내 존재) #ls /etc 2. /etc/passwd 파일 내 두 번째 필드가 "x" 표시되는지 확인 #cat /etc/passwd root:x:0:0:root:/root:/bin/bash (※ "passwd" 파일 구조: 부록 참조)				
HP-UX	1. /tcb 디렉터리 존재 확인 2. /etc/passwd 파일 내 두 번째 필드가 "x" 표시되는지 확인				
위에 제시한 설정이 적용되지 않은 경우 아래의 보안설정방법에 따라 설정을 변경함					
■ SunOS, LINUX					
1. #pwconv ---> 쉘도우 패스워드 정책 적용 방법					
2. #pwunconv ---> 일반 패스워드 정책 적용 방법					
■ AIX					
AIX 서버는 기본적으로 "/etc/security/passwd" 파일에 패스워드를 암호화하여 저장·관리함					
■ HP-UX					
HP-UX 서버는 Trusted Mode로 전환할 경우 패스워드를 암호화하여 "/tcb/files/auth" 디렉터리에 계정 이니셜과 계정 이름에 따라 파일로 저장·관리할 수 있으므로 Trusted Mode인지 확인 후 UnTrusted Mode인 경우 모드를 전환함					
1. Trusted Mode 전환 방법: root 계정으로 로그인한 후 아래 명령 수행 #/etc/tsconvert					
2. UnTrusted Mode 전환 방법: root 계정으로 로그인한 후 아래 명령 수행 #/etc/tsconvert -r					
조치 시 영향	Trusted Mode로 전환 시 파일시스템 구조가 변경되어 운영 중인 서비스에 문제가 발생할 수 있으므로 충분한 테스트를 거친 후 Trusted Mode로의 전환 필요				

UNIX 서버

취약점 항목	1.5. root 이외의 UID가 '0' 금지				
대상 OS	SunOS, LINUX, AIX, HP-UX	위험도	중	Code	U-05
취약점 개요	root(UID=0)와 동일한 *UID(User Identification)를 가진 계정 존재 시 root 권한으로 시스템 접근이 가능하므로 root의 UID를 가진 계정이 존재하지 않도록 확인하여야 함. root뿐만 아니라 사용자 간 UID 중복 시에도 권한 중복으로 인한 사용자 감사 추적이 어렵게 되는 문제가 발생하므로 계정 및 UID 확인이 필요함. *UID(User Identification): 여러 명의 사용자가 동시에 사용하는 시스템에서 사용자가 자신을 대표하기 위해 쓰는 이름.				
보안대책					
판단기준	양호: root 계정과 동일한 UID를 갖는 계정이 존재하지 않는 경우 취약: root 계정과 동일한 UID를 갖는 계정이 존재하는 경우				
조치방법	UID가 0인 계정 존재 시 변경할 UID를 확인 후 다른 UID로 변경 및 불필요 시 삭제, 계정이 사용 중이면 명령어로 조치가 안 되므로 /etc/passwd 파일 설정 변경				
보안설정방법					
OS별 점검 파일 위치 및 점검 방법					
SunOS, LINUX, AIX, HP-UX	<pre>#cat /etc/passwd (※ "passwd" 파일 구조: 부록 참조) root:x:0:0:root:/root:/bin/bash bin:x:1:1:bin:/bin:/sbin/nologin daemon:x:2:2:daemon:/sbin:/sbin/nologin</pre> "/etc/passwd" 파일 내 UID 확인 (세 번째 필드 값) root 이외의 계정이 "UID=0"인 경우 0이 아닌 적절한 UID 부여				
위에 제시한 설정이 해당 파일에 적용되지 않은 경우 아래의 보안설정방법에 따라 설정을 변경함					
■ SunOS, LINUX, HP-UX					
1. usermod 명령으로 UID가 0인 일반 계정의 UID를 100 이상으로 수정					
▪ SunOS, HP-UX의 경우 100 이상					
▪ LINUX의 경우 500 이상					
(예) test 계정의 UID를 2002 로 바꿀 경우					
#usermod -u 2002 test					
※ 각 OS별로 사용자 UID 체계가 달라 시스템 계정 및 일반 사용자 계정이 부여받는 값의 범위에 차이가 있으며, 공통적으로 관리자는 "UID=0"을 부여받음					
■ AIX					
1. chuser 명령으로 UID가 0인 일반 계정의 UID를 100 이상으로 수정					
(예) test 계정의 UID 를 2002 로 바꿀 경우					

UNIX 서버

#chuser id=2002 test

passwd 파일 구조

root:	x:	0:	1:	Super-User:	/:	/usr/bin/ksh
loginID:	x:	UID:	GID:	comment:	home_directory:	login_shell

(예) root:x:0:0:root:/root:/bin/bash
 bin:x:1:1:bin:/bin:/sbin/nologin
 daemon:x:2:2:daemon:/sbin:/sbin/nologin
 adm:x:3:4:adm:/var/adm:/sbin/nologin
 sync:x:5:0:sync:/sbin:/bin/sync
 shutdown:x:6:0:shutdown:/sbin:/sbin/shutdown
 halt:x:7:0:halt:/sbin:/sbin/halt
 mail:x:8:12:mail:/var/spool/mail:/sbin/nologin
 nobody:x:99:99:Nobody:./:/sbin/nologin

위의 예는 /etc/passwd 파일의 내용으로 ":"을 사용하여 필드를 구분함
 세 번째 필드(UID)가 "0"인 경우 슈퍼유저 권한을 갖으며, "0"이외의 계정은 일반 계정으로 볼 수 있음

조치 시 영향 해당 계정에 관리자 권한이 필요하지 않으면 일반적으로 영향 없음

UNIX 서버

취약점 항목	1.6. root 계정 su 제한				
대상 OS	SunOS, LINUX, AIX, HP-UX	위험도	하	Code	U-06
취약점 개요	권한이 없는 일반 사용자가 su 명령을 사용하여 로그인을 시도하고 패스워드 무작위 대입 공격(Brute Force Attack)이나 패스워드 추측 공격>Password Guessing)을 통해 root 권한을 획득할 수 있음. su 명령어 사용이 허용된 사용자만 root 계정으로 접속할 수 있도록 함.				
보안대책					
점검기준	양호: su 명령어를 특정 그룹에 속한 사용자만 사용하도록 제한되어 있는 경우 취약: su 명령어를 모든 사용자가 사용하도록 설정되어 있는 경우				
조치방법	일반 사용자의 su 명령 사용 제한 1. Group 생성(생성할 그룹 요청, 일반적으로 wheel 사용) 2. su 명령어의 그룹을 요청받은 그룹으로 변경 3. su 명령어의 권한 변경(4750) 4. su 명령어 사용이 필요한 계정을 새로 생성한 그룹에 추가(추가할 계정 요청) ※ LINUX의 경우, *PAM(Pluggable Authentication Module)을 이용한 설정 가능 *PAM(Pluggable Authentication Module): 사용자를 인증하고 그 사용자의 서비스에 대한 액세스를 제어하는 모듈화 된 방법을 말하며, PAM은 관리자가 응용프로그램들의 사용자 인증 방법을 선택할 수 있도록 해줌				
보안설정방법					
OS별 점검 파일 위치 및 점검 방법					
SunOS, LINUX, AIX, HP-UX	1. "wheel" 그룹(su 명령어 사용 그룹) 및 그룹 내 구성원 존재 여부 확인 #cat /etc/group (※ "group" 파일 구조: 부록 참조) wheel:x:10:root,admin 2. wheel 그룹이 su 명령어를 사용할 수 있는지 설정 여부 확인 [SunOS] #ls -al /usr/bin/su #chgrp security su #chmod 4750 su [AIX] #cat /etc/security/user ---> default의 "sugroups=staff" 설정 확인 /etc/group 에서 staff 그룹에 해당하는 계정만 su 사용 가능 [HP-UX] #vi /etc/default/security ---> SU_ROOT_GROUP=wheel 설정 확인 3. 파일 권한 확인 #ls -l /usr/bin/su -rwsr-x--- /usr/bin/su (파일 권한이 4750인 경우 양호)				

UNIX 서버

OS별 점검 파일 위치 및 점검 방법

LINUX PAM 모듈 이용 시	1. "wheel" 그룹(su 명령어 사용 그룹) 및 그룹 내 구성원 존재 여부 확인 #cat /etc/group <i>wheel:x:10:root,admin</i> 2. 허용 그룹(su 명령어 사용 그룹) 설정 여부 확인 #cat /etc/pam.d/su <i>auth required /lib/security/pam_wheel.so debug group=wheel 또는,</i> <i>auth required /lib/security/\$ISA/pam_wheel.so use_uid</i>
------------------------------	---

위에 제시한 설정이 해당 파일에 적용되지 않은 경우 아래의 보안설정방법에 따라 설정을 변경함

■ SunOS, LINUX, HP-UX

1. wheel group 생성 (wheel 그룹이 존재하지 않는 경우)
#groupadd wheel
2. su 명령어 그룹 변경
#chgrp wheel /usr/bin/su
3. su 명령어 사용권한 변경
#chmod 4750 /usr/bin/su
4. wheel 그룹에 su 명령 허용 계정 등록
#usermod -G wheel <user_name>
또는, 직접 /etc/group 파일을 수정하여 필요한 계정 등록
wheel:x:10: -> wheel:x:10:root,admin

■ AIX

1. wheel group 생성(wheel 그룹이 존재하지 않는 경우)
#mkgroup wheel
2. su 명령어 그룹 변경
#chgrp wheel /usr/bin/su
3. su 명령어 사용권한 변경
#chmod 4750 /usr/bin/su
4. wheel 그룹에 su 명령 허용 계정 등록
#chgroup users=<user_name> wheel
(예) chgroup users=admin wheel

■ LINUX PAM 모듈을 이용한 설정 방법

1. "/etc/pam.d/su" 파일을 아래와 같이 설정(주석제거)
auth sufficient /lib/security/pam_rootok.so
auth required /lib/security/pam_wheel.so debug group=wheel 또는,
auth sufficient /lib/security/\$ISA/pam_rootok.so
auth required /lib/security/\$ISA/pam_wheel.so use_uid

UNIX 서버

2. wheel 그룹에 su 명령어를 사용할 사용자 추가

```
#usermod -G wheel <user_name>
```

또는, 직접 "/etc/group" 파일을 수정하여 필요한 계정 추가

```
wheel:x:10: -> wheel:x:10:root,admin
```

조치 시 영향	그룹에 추가된 계정들은 모든 Session 종료 후 재로그인 시 su 명령어 사용 가능
----------------	--

UNIX 서버

취약점 항목	1.7. 패스워드 최소 길이 설정				
대상 OS	SunOS, LINUX, AIX, HP-UX	위험도	중	Code	U-07
취약점 개요	패스워드 무작위 대입 공격(Brute Force Attack)이나 패스워드 추측 공격>Password Guessing)을 피하기 위하여 패스워드 최소 길이가 설정되어 있는지 점검함. 패스워드 최소 길이가 설정되어 있지 않거나, 짧게 설정되어 있을 경우 쉽게 유추될 수 있음.				
보안대책					
판단기준	양호: 패스워드 최소 길이가 8자 이상으로 설정되어 있는 경우				
	취약: 패스워드 최소 길이가 8자 미만으로 설정되어 있는 경우				
조치방법	패스워드 정책 설정파일을 수정하여 패스워드 최소 길이를 8자 이상으로 설정				
보안설정방법					
OS별 점검 파일 위치 및 점검 방법					
SunOS	#cat /etc/default/passwd PASSLENGTH=8				
LINUX	#cat /etc/login.defs PASS_MIN_LEN 8				
AIX	#cat /etc/security/user minlen=8				
HP-UX	#cat /etc/default/security MIN_PASSWORD_LENGTH=8				

위에 제시한 설정이 해당 파일에 적용되지 않은 경우 아래의 보안설정방법에 따라 설정을 변경함

■ SunOS

1. vi 편집기를 이용하여 “/etc/default/passwd” 파일을 연 후

2. 아래와 같이 수정 또는, 신규 삽입
(수정 전) PASSLENGTH=6
(수정 후) PASSLENGTH=8

■ LINUX

1. vi 편집기를 이용하여 “/etc/login.defs” 파일을 연 후

2. 아래와 같이 수정 또는, 신규 삽입
(수정 전) PASS_MIN_LEN 6
(수정 후) PASS_MIN_LEN 8

■ AIX

1. vi 편집기를 이용하여 “/etc/security/user” 파일을 연 후

2. default: 부분을 아래와 같이 수정 또는, 신규 삽입
(수정 전) minlen=4
(수정 후) minlen=8

UNIX 서버

■ HP-UX

1. vi 편집기를 이용하여 "/etc/default/security" 파일을 연 후
2. 아래와 같이 수정 또는, 신규 삽입
(수정 전) MIN_PASSWORD_LENGTH=
(수정 후) MIN_PASSWORD_LENGTH=8

조치 시 영향	일반적으로 영향 없음
----------------	-------------

UNIX 서버

취약점 항목	1.8. 패스워드 최대 사용기간 설정				
대상 OS	SunOS, LINUX, AIX, HP-UX	위험도	중	Code	U-08
취약점 개요	패스워드 최대 사용기간을 설정하지 않은 경우 일정 기간 경과 후에도 유출된 패스워드로 접속이 가능함. 악의적인 사용자로부터 계속적인 접속을 차단하기 위해 패스워드 최대 사용기간을 설정하여 주기적으로 변경할 수 있도록 함.				
보안대책					
판단기준	양호: 패스워드 최대 사용기간이 90일(12주) 이하로 설정되어 있는 경우 취약: 패스워드 최대 사용기간이 90일(12주) 이하로 설정되어 있지 않는 경우				
조치방법	패스워드 정책 설정파일을 수정하여 패스워드 최대 사용기간을 90일(12주)로 설정				
보안설정방법					
OS별 점검 파일 위치 및 점검 방법					
SunOS	#cat /etc/default/passwd MAXWEEKS=12				
LINUX	#cat /etc/login.defs PASS_MAX_DAYS 90				
AIX	#cat /etc/security/user maxage=12				
HP-UX	#cat /etc/default/security PASSWORD_MAXDAYS=90				

위에 제시한 설정이 해당 파일에 적용되지 않은 경우 아래의 보안설정방법에 따라 설정을 변경함

■ SunOS

1. vi 편집기를 이용하여 “/etc/default/passwd” 파일을 연 후

2. 아래와 같이 수정 또는, 신규 삽입
(수정 전) MAXWEEKS=
(수정 후) MAXWEEKS=12 (단위: 주)

■ LINUX

1. vi 편집기를 이용하여 “/etc/login.defs” 파일을 연 후

2. 아래와 같이 수정 또는, 신규 삽입
(수정 전) PASS_MAX_DAYS 99999
(수정 후) PASS_MAX_DAYS 90 (단위: 일)

■ AIX

1. vi 편집기를 이용하여 “/etc/security/user” 파일을 연 후

2. default: 부분을 아래와 같이 수정 또는, 신규 삽입
(수정 전) maxage=0
(수정 후) maxage=12 (단위: 주)

UNIX 서버

■ HP-UX

1. vi 편집기를 이용하여 "/etc/default/security" 파일을 연 후
2. 아래와 같이 수정 또는, 신규 삽입
 (수정 전) PASSWORD_MAXDAYS=99999
 (수정 후) PASSWORD_MAXDAYS=90 (단위: 일)

조치 시 영향	일반적으로 영향 없음
---------	-------------

UNIX 서버

취약점 항목		1.9. 패스워드 최소 사용기간 설정			
대상 OS	SunOS, LINUX, AIX, HP-UX	위험도	중	Code	U-09
취약점 개요	패스워드 최소 사용기간을 설정하지 않은 경우 사용자에게 익숙한 패스워드로 변경이 가능하며, 이를 재사용함으로써 패스워드의 정기적인 변경은 무의미해질 수 있음. 이전 암호를 그대로 재사용하는 것을 방지하기 위해 최근 암호 기억 설정을 함께 적용하여 패스워드를 보호함.				
보안대책					
판단기준	양호: 패스워드 최소 사용기간이 1일(1주)로 설정되어 있는 경우				
	취약: 패스워드 최소 사용기간이 설정되어 있지 않는 경우				
조치방법	패스워드 정책 설정파일을 수정하여 패스워드 최소 사용기간을 1일(1주)로 설정				
보안설정방법					
OS별 점검 파일 위치 및 점검 방법					
SunOS	#cat /etc/default/passwd MINWEEKS=1				
LINUX	#cat /etc/login.defs PASS_MIN_DAYS 1				
AIX	#cat /etc/security/user minage=1				
HP-UX	#cat /etc/default/security PASSWORD_MINDAYS=1				
위에 제시한 설정이 해당 파일에 적용되지 않은 경우 아래의 보안설정방법에 따라 설정을 변경함					
■ SunOS					
1. vi 편집기를 이용하여 "/etc/default/passwd" 파일을 연 후					
2. 아래와 같이 수정 또는, 신규 삽입 (수정 전) MINWEEKS= (수정 후) MINWEEKS=1 (단위: 주)					
■ LINUX					
1. vi 편집기를 이용하여 "/etc/login.defs" 파일을 연 후					
2. 아래와 같이 수정 또는, 신규 삽입 (수정 전) PASS_MIN_DAYS (수정 후) PASS_MIN_DAYS 1 (단위: 일)					
■ AIX					
1. vi 편집기를 이용하여 "/etc/security/user" 파일을 연 후					
2. default 부분을 아래와 같이 수정 또는, 신규 삽입 (수정 전) minage=1					

UNIX 서버

(수정 후) minage=1 (단위: 주)

■ HP-UX

1. vi 편집기를 이용하여 "/etc/default/security" 파일을 연 후
2. 아래와 같이 수정 또는, 신규 삽입
 (수정 전) PASSWORD_MINDAYS=
 (수정 후) PASSWORD_MINDAYS=1 (단위: 일)

조치 시 영향	일반적으로 영향 없음
----------------	-------------

UNIX 서버

취약점 항목		1.10. 불필요한 계정 제거			
대상 OS	SunOS, LINUX, AIX, HP-UX	위험도	하	Code	U-10
취약점 개요	OS나 Package 설치 시 Default로 생성되는 계정은 대부분 Default 패스워드를 사용하는 경우가 많으며 패스워드 추측공격에 악용될 수 있으므로 시스템에서 이용하지 않는 "lp, uucp, nuucp" 등의 Default 계정 및 의심스러운 특이한 계정의 존재 유무를 확인 후 삭제함. 또한, 관리되지 않은 불필요한 계정으로 인해 시스템 접속이 가능하므로 퇴직, 전직, 휴직 등의 이유로 더 이상 사용하지 않는 계정, 불필요한 계정, 의심스러운 계정은 제거해야 함. 특히, 장기간 패스워드가 변경되지 않은 미사용 계정은 반복적인 패스워드 추측 공격(Password Guessing)이 가능하고 해당 계정 정보의 유출 여부 확인이 어려움.				
보안대책					
판단기준	양호: 불필요한 계정이 존재하지 않는 경우				
	취약: 불필요한 계정이 존재하는 경우				
조치방법	현재 등록된 계정 현황 확인 후 불필요한 계정 삭제				
보안설정방법					
OS별 점검 파일 위치 및 점검 방법					
SunOS, LINUX, AIX, HP-UX	1. 미사용 계정 및 의심스러운 계정 존재 여부 확인 (※ "passwd" 파일 구조: 부록 참조) #cat /etc/passwd 2. 사용하지 않는 Default 계정 점검 (lp, uucp, nuucp 계정 존재 확인 예시) #cat /etc/passwd egrep "lp uucp nuucp"				
LOG를 통한 확인	1. 로그인 실패 기록 점검을 통해 미사용 계정 및 의심스러운 계정 확인 #cat /var/adm/loginlog (SunOS, AIX, HP-UX) / #cat /var/log/loginlog (LINUX) #cat /var/adm/authlog (AIX, HP-UX) / #cat /var/log/authlog (SunOS) #cat /var/adm/sulog (SunOS, AIX, HP-UX) / #cat /var/log/sulog (LINUX) ※ 파일의 위치는 버전별 다를 수 있음				

위에 제시한 점검 방법에 의해 불필요한 계정 발견 시 아래의 보안설정방법에 따라 조치함

■ SunOS, LINUX, HP-UX

1. 서버에 등록된 불필요한 사용자 계정 확인
2. userdel 명령으로 불필요한 사용자 계정 삭제
#userdel <user_name>

※ /etc/passwd 파일에서 계정 앞에 #을 삽입하여도 주석처리가 되지 않으므로 조치 시에는 반드시 계정을 삭제하도록 권고함

■ AIX

1. 서버에 등록된 불필요한 사용자 계정 확인

UNIX 서버

2. rmuser 명령으로 불필요한 사용자 계정 삭제

```
#rmuser <user_name>
```

기본적으로 차단하는 Default 계정 (※ 계정 설명: 부록 참조)

adm, lp, sync, shutdown, halt, news, uucp, operator, games, gopher, nfsnobody, squid 등

조치 시 영향	일반적으로 영향 없음
----------------	-------------

UNIX 서버

취약점 항목		1.11. 관리자 그룹에 최소한의 계정 포함			
대상 OS	SunOS, LINUX, AIX, HP-UX	위험도	하	Code	U-11
취약점 개요	시스템을 관리하는 root 계정이 속한 그룹은 시스템 운영 파일에 대한 접근권한이 부여되어 있으므로 최소한의 계정만 등록되어 있어야 함. 해당 그룹 관리가 이루어지지 않으면 허가되지 않은 일반 사용자가 관리자의 권한으로 시스템에 접근할 수 있으며, 파일 수정 및 변경 등의 악의적인 작업으로 인해 시스템 운영에 피해를 줄 수 있음.				
보안대책					
판단기준	양호: 관리자 그룹에 불필요한 계정이 등록되어 있지 않은 경우				
	취약: 관리자 그룹에 불필요한 계정이 등록되어 있는 경우				
조치방법	현재 등록된 계정 현황 확인 후 불필요한 계정 삭제				
보안설정방법					
OS별 점검 파일 위치 및 점검 방법					
SunOS, LINUX, HP-UX	#cat /etc/group (※ "group" 파일 구조: 부록 참조) root:x:0:root				
AIX	#cat /etc/group system:!:0:root				
불필요한 계정이 관리자 그룹에 포함되어 있는 경우 아래의 보안설정방법에 따라 설정을 변경함					
■ SunOS, LINUX, HP-UX					
1. vi 편집기를 이용하여 "/etc/group" 파일을 연 후					
2. root 그룹에 등록된 불필요한 계정 삭제					
(예) root 그룹에 등록된 불필요한 test 계정 삭제					
(수정 전) root:x:0:root,test					
(수정 후) root:x:0:root					
■ AIX					
1. vi 편집기를 이용하여 "/etc/group" 파일을 연 후					
2. system 그룹에 등록된 불필요한 계정 삭제					
(예) system 그룹에 등록된 불필요한 test 계정 삭제					
(수정 전) system:!:0:root,test					
(수정 후) system:!:0:root					
조치 시 영향	일반적으로 영향 없음				

UNIX 서버

취약점 항목		1.12. 계정이 존재하지 않는 GID 금지			
대상 OS	SunOS, LINUX, AIX, HP-UX	위험도	하	Code	U-12
취약점 개요	미흡한 계정 그룹 관리로 인해 구성원이 없는 그룹이 존재할 경우 해당 그룹 소유의 파일이 비인가자에게 노출될 위험이 있음. 계정이 존재하지 않는 *GID(Group Identification) 설정을 관리자와 검토 후 제거하여야 함.				
	*GID(Group Identification): 다수의 사용자가 특정 개체를 공유할 수 있게 연계시키는 특정 그룹의 이름으로 주로 계정처리 목적으로 사용되며, 한 사용자는 여러 개의 GID를 가질 수 있음.				
보안대책					
판단기준	양호: 존재하지 않는 계정에 GID 설정을 금지한 경우				
	취약: 존재하지 않은 계정에 GID 설정이 되어있는 경우				
조치방법	구성원이 존재하지 않는 그룹이 있을 경우 관리자와 검토하여 제거				
보안설정방법					
OS별 점검 파일 위치 및 점검 방법					
SunOS, LINUX, HP-UX, AIX	<pre>#cat /etc/group (※ "group" 파일 구조: 부록 참조) gnats:x:41: shadow:x:42: utmp:x:43: video:x:44:administrador sasl:x:45: plugdev:x:46:haldaemon,administrador,xan,noa staff:x:50: games:x:60: users:x:100: nogroup:x:65534: dhcp:x:101: syslog:x:102: klog:x:103: scanner:x:104:cupsys,hplip,administrador,xan,noa nvram:x:105: messagebus:x:106: ssl-cert:x:107:cupsys</pre>				
LINUX,	<pre>#cat /etc/gshadow *gshadow 파일: "shadow" 파일에 사용자 계정의 암호가 저장되어 있는 것처럼 시스템 내 존재하는 그룹의 암호 정보 저장 파일로 그룹 관리자 및 구성원 설정 가능 "gshadow" 파일 내 필드는 다음과 구조로 구성됨 [그룹명 : 패스워드 : 관리자, 관리자 ... : 멤버, 멤버 ...]</pre>				
구성원이 없는 그룹이 존재하는 경우 아래의 보안설정방법에 따라 그룹을 제거함					
■ SunOS, LINUX, AIX, HP-UX					
#groupdel <group_name>					
※ 구성원이 없거나, 더 이상 사용하지 않는 그룹명 삭제					
조치 시 영향	일반적으로 영향 없음				

UNIX 서버

취약점 항목	1.13. 동일한 UID 금지				
대상 OS	SunOS, LINUX, AIX, HP-UX	위험도	하	Code	U-13
취약점 개요	UNIX 시스템은 모든 사용자 계정에 UID를 부여하여 해당 UID로 사용자 이름, 패스워드, 홈 디렉터리 등과 같은 사용자 정보를 대응시킴. 만약 중복된 UID가 존재할 경우 시스템에서 동일한 사용자로 인식하여 문제가 발생할 수 있으며, 공격자에 의한 개인 정보 및 관련 데이터 유출 발생 시에도 감사 추적이 어렵게 됨.				
보안대책					
판단기준	양호: 동일한 UID로 설정된 사용자 계정이 존재하지 않는 경우				
	취약: 동일한 UID로 설정된 사용자 계정이 존재하는 경우				
조치방법	동일한 UID로 설정된 사용자 계정의 UID를 서로 다른 값으로 변경				
보안설정방법					
OS별 점검 파일 위치 및 점검 방법					
SunOS, LINUX, AIX, HP-UX	#cat /etc/passwd (※ "passwd" 파일 구조: 부록 참조) <pre>[root@root root]# cat /etc/passwd root:x:0:0:root:/root:/bin/bash bin:x:1:1:bin:/bin:/sbin/nologin daemon:x:2:2:daemon:/sbin:/sbin/nologin adm:x:3:4:adm:/var/adm:/sbin/nologin</pre>				
동일한 UID를 갖는 계정이 존재하는 경우 아래의 보안설정방법에 따라 설정을 변경함					
■ SunOS, LINUX, HP-UX usermod 명령으로 동일한 UID로 설정된 사용자 계정의 UID 변경 #usermod -u <변경할 UID값> <user_name>					
■ AIX chuser 명령으로 동일한 UID로 설정된 사용자 계정의 UID 변경 #chuser id=<변경할 UID값> <user_name>					
조치 시 영향	일반적으로 영향 없음				

UNIX 서버

취약점 항목		1.14. 사용자 shell 점검			
대상 OS	SunOS, LINUX, AIX, HP-UX	위험도	하	Code	U-14
취약점 개요	로그인이 필요 없는 계정을 이용해 시스템에 접근하여 사용자의 명령어를 해석하고 악용할 가능성이 있으므로, /bin/false *셸(Shell)을 부여해 로그인을 금지함.				
	*셸(Shell): 대화형 사용자 인터페이스로써, 운영체제(OS) 가장 외곽계층에 존재하여 사용자의 명령어를 이해하고 실행함.				
보안대책					
판단기준	양호: 로그인 필요하지 않은 계정에 /bin/false(nologin) 셸이 부여되어 있는 경우				
	취약: 로그인 필요하지 않은 계정에 /bin/false(nologin) 셸이 부여되지 않은 경우				
조치방법	로그인이 필요하지 않은 계정에 대해 /bin/false(nologin) 셸 부여				
보안설정방법					
OS별 점검 파일 위치 및 점검 방법					
SunOS, LINUX, AIX, HP-UX	<pre>#cat /etc/passwd egrep "^daemon ^bin ^sys ^adm ^listen ^nobody ^nobody4 ^noaccess ^diag ^listen ^operator ^games ^gopher" grep -v "admin"</pre>				
	<pre>games: x: 12: 100: games: /usr/games: /sbin/nologin gopher: x: 13: 30: gopher: /var/gopher: /sbin/nologin ftp: x: 14: 50: FTP User: /var/ftp: /sbin/nologin nobody: x: 99: 99: Nobody: /: /sbin/nologin nfsnobody: x: 65534: 65534: Anonymous NFS User: /var/lib/nfs: /sbin/nologin</pre>				
시스템에 불필요한 계정을 확인한 후 /bin/false(nologin) 셸이 부여되어 있지 않은 경우 아래의 보안설정방법에 따라 설정을 변경함 (※ 불필요한 계정은 시스템 용도에 따라 차이가 있음)					
■ SunOS, LINUX, AIX, HP-UX					
1. vi 편집기를 이용하여 "/etc/passwd" 파일을 연 후					
2. 로그인 셸 부분인 계정 맨 마지막에 /bin/false(nologin) 부여 및 변경					
(수정 전) daemon:x:1:1:::/sbin/ksh					
(수정 후) daemon:x:1:1:::/bin/false 또는, daemon:x:1:1:::/sbin/nologin					
일반적으로 로그인이 불필요한 계정 (※ 계정 설명: 부록 참조)					
daemon, bin, sys, adm, listen, nobody, nobody4, noaccess, diag, listen, operator, games, gopher 등 일반적으로 UID 100 이하 60000 이상의 시스템 계정 해당					
조치 시 영향	일반적인 경우 영향 없음				
	모호한 경우 "/etc/shadow" 파일에서 해당 계정에 패스워드 존재 여부로 확인				

UNIX 서버

취약점 항목	1.15. Session Timeout 설정				
대상 OS	SunOS, LINUX, AIX, HP-UX	위험도	하	Code	U-15
취약점 개요	계정이 접속된 상태로 방치될 경우 권한이 없는 사용자에게 중요시스템이 노출되어 악의적인 목적으로 사용될 수 있으므로 일정 시간 이후 어떠한 이벤트가 발생하지 않으면 연결을 종료하는 Session Timeout 설정이 필요함.				
보안대책					
판단기준	양호: Session Timeout이 600초(10분) 이하로 설정되어 있는 경우				
	취약: Session Timeout이 600초(10분) 이하로 설정되지 않은 경우				
조치방법	600초(10분) 동안 입력이 없을 경우 접속된 Session을 끊도록 설정				
보안설정방법					

OS별 점검 파일 위치 및 점검 방법	
SunOS	<pre>#cat /etc/default/login TIMEOUT=600 export TMOUT</pre>
LINUX, AIX, HP-UX	<pre><sh, ksh, bash 사용 시> #cat /etc/profile(.profile) TIMEOUT=600 export TMOUT <csh 사용 시> #cat /etc/csh.login 또는, #cat /etc/csh.cshrc set autologout=10</pre>

위에 제시한 설정이 해당 파일에 적용되지 않은 경우 아래의 보안설정방법에 따라 설정을 변경함

■ SunOS

1. vi 편집기를 이용하여 "/etc/default/login" 파일을 연 후
2. 아래와 같이 수정 또는, 신규 삽입
TIMEOUT=600 (단위: 초)
export TMOUT

■ LINUX, AIX, HP-UX

- sh(born shell), ksh(korn shell), bash(born again shell)을 사용하는 경우 -
1. vi 편집기를 이용하여 "/etc/profile(.profile)" 파일을 연 후
 2. 아래와 같이 수정 또는, 추가
TIMEOUT=600 (단위: 초)
export TMOUT

UNIX 서버

- csh 을 사용하는 경우 -

1. vi 편집기를 이용하여 "/etc/csh.login" 또는, "/etc/csh.cshrc" 파일을 연 후
2. 아래와 같이 수정 또는, 추가
set autologout=10 (단위: 분)

조치 시 영향

모니터링 용도로 사용할 경우 해당 계정의 환경변수 파일에만 예외적으로 600초 이상의 시간 입력
(예) root 로 모니터링 할 경우 /.profile, /.bash_profile 등에 600초 이상 입력

UNIX 서버

2. 파일 및 디렉터리 관리

취약점 항목		2.1. root 홈, 패스 디렉터리 권한 및 패스 설정			
대상 OS	SunOS, LINUX, AIX, HP-UX	위험도	상	Code	U-16
취약점 개요	root 계정의 PATH 환경변수에 "." (현재 디렉터리 지칭)이 포함되어 있으면, root 계정의 인가자로 인해 비의도적으로 현재 디렉터리에 위치하고 있는 명령어가 실행될 수 있음. 즉 "."이 /usr/bin이나 /bin, /sbin 등 명령어들이 위치하고 있는 디렉터리보다 우선하여 위치하고 있을 경우, root 계정의 인가자가 특정 명령을 실행하면, 비인가자가 불법적으로 위치시킨 파일을 실행하여 예기치 않은 결과를 가져올 수 있음. 잘못된 PATH의 우선순위 등이 침해사고에 이용될 수 있으므로 "." 뿐만 아니라 비인가자가 불법적으로 생성한 디렉터리를 우선으로 가리지 않도록 설정함.				
보안대책					
판단기준	양호: PATH 환경변수에 "." 이 맨 앞이나 중간에 포함되지 않은 경우				
	취약: PATH 환경변수에 "." 이 맨 앞이나 중간에 포함되어 있는 경우				
조치방법	root 계정의 환경변수 설정파일("/.profile", "/.cshrc" 등)과 "/etc/profile" 등에서 PATH 환경변수에 포함되어 있는 현재 디렉터리를 나타내는 "."을 PATH 환경변수의 마지막으로 이동 "/etc/profile", root 계정의 환경변수 파일, 일반계정의 환경변수 파일을 순차적으로 검색하여 확인				
보안설정방법					
OS별 점검 파일 위치 및 점검 방법					
SunOS, LINUX, AIX, HP-UX	#echo \$PATH /usr/local/sbin:/sbin:/usr/sbin:/bin:/usr/bin:/usr/bin/X11:/usr/local/bin:/usr/bin:/usr/X11R6/bin:/root/bin 위와 같이 출력되는 PATH 변수 내에 "." 또는, "::" 포함 여부 확인				
PATH 변수 내에 ".", "::" 이 맨 앞에 존재하는 경우 아래의 보안설정방법에 따라 설정을 변경함					
SHELL에 따라 참조되는 환경 설정파일					
/bin/sh	/etc/profile, \$HOME/.profile				
/bin/csh	\$HOME/.cshrc, \$HOME/.login, /etc/.login				
/bin/ksh	/etc/profile, \$HOME/.profile, \$HOME/.kshrc				
/bin/bash	/etc/profile, \$HOME/.bash_profile				
※ 홈 디렉터리에 설정된 값이 가장 늦게 적용되어 최종 PATH로 설정됨					

UNIX 서버

■ SunOS, LINUX, AIX, HP-UX

1. vi 편집기를 이용하여 root 계정의 설정파일(~/.profile 과 /etc/profile)을 연 후

#vi /etc/profile

2. 아래와 같이 수정

(수정 전) PATH=.:\$PATH:\$HOME/bin

(수정 후) PATH=\$PATH:\$HOME/bin

※ 환경변수 파일은 OS별로 약간씩 다를 수 있음

조치 시 영향	일반적인 경우 영향 없음
----------------	---------------

UNIX 서버

취약점 항목	2.2. 파일 및 디렉터리 소유자 설정				
대상 OS	SunOS, LINUX, AIX, HP-UX	위험도	상	Code	U-17
취약점 개요	소유자가 존재하지 않는 파일 및 디렉터리는 현재 권한이 없는 자(퇴직, 전직, 휴직 등)의 소유였거나, 관리 소홀로 인해 생긴 파일일 가능성이 있음. 만약 중요 파일 및 디렉터리일 경우 문제가 발생할 수 있으므로 관리가 필요함.				
보안대책					
판단기준	양호: 소유자가 존재하지 않은 파일 및 디렉터리가 존재하지 않는 경우				
	취약: 소유자가 존재하지 않은 파일 및 디렉터리가 존재하는 경우				
조치방법	소유자가 존재하지 않은 파일 및 디렉터리 삭제 또는, 소유자 변경				
보안설정방법					
OS별 점검 파일 위치 및 점검 방법					
SunOS, AIX	소유자가 nouser, nogroup인 파일이나 디렉터리 검색 #find / -nouser -o -nogroup -xdev -ls 2> /dev/null				
HP-UX	#find / ₩(-nouser -o -nogroup ₩) -xdev -exec ls -al {} ₩; 2> dev/null				
LINUX	#find / -nouser -print #find / -nogroup -print				
소유자가 nouser, nogroup인 파일이나 디렉터리 존재하는 경우 아래의 보안설정방법에 따라 디렉터리 및 파일 삭제 또는, 소유자 및 그룹을 변경함					
■ SunOS, LINUX, AIX, HP-UX					
1. 소유자가 존재하지 않는 파일이나 디렉터리가 불필요한 경우 rm 명령으로 삭제 #rm <file_name> #rm <directory_name> ※ 삭제할 파일명 또는, 디렉터리명 입력					
2. 필요한 경우 chown 명령으로 소유자 및 그룹 변경 #chown <user_name> <file_name>					
조치 시 영향	일반적인 경우 영향 없음				

UNIX 서버

취약점 항목	2.3. /etc/passwd 파일 소유자 및 권한 설정								
대상 OS	SunOS, LINUX, AIX, HP-UX	위험도	상	Code	U-18				
취약점 개요	"/etc/passwd" 파일은 사용자의 ID, 패스워드(보안상 'x'로 표시), UID, GID, 홈 디렉터리, 쉘 정보를 담고 있는 중요 파일로 관리자 이외의 사용자가 "/etc/passwd" 파일에 접근 시 root 권한 획득이 가능하므로 해당 파일의 접근을 제한하여야 함.								
보안대책									
판단기준	양호: /etc/passwd 파일의 소유자가 root이고, 권한이 644 이하인 경우								
	취약: /etc/passwd 파일의 소유자가 root가 아니거나, 권한이 644 이하가 아닌 경우								
조치방법	"/etc/passwd" 파일의 소유자 및 권한 변경 (소유자 root, 권한 644)								
보안설정방법									
<table><tr><th colspan="2">OS별 점검 파일 위치 및 점검 방법</th></tr><tr><td>SunOS, LINUX, AIX, HP-UX</td><td>"/etc/passwd" 파일의 소유자 및 권한 확인 #ls -l /etc/passwd r--r--r-- root <passwd 파일></td></tr></table>						OS별 점검 파일 위치 및 점검 방법		SunOS, LINUX, AIX, HP-UX	"/etc/passwd" 파일의 소유자 및 권한 확인 #ls -l /etc/passwd r--r--r-- root <passwd 파일>
OS별 점검 파일 위치 및 점검 방법									
SunOS, LINUX, AIX, HP-UX	"/etc/passwd" 파일의 소유자 및 권한 확인 #ls -l /etc/passwd r--r--r-- root <passwd 파일>								
"passwd" 파일의 소유자가 root가 아니거나 파일의 권한이 644 이하가 아닌 경우 아래의 보안설정방법에 따라 설정을 변경함 ■ SunOS, LINUX, AIX, HP-UX "/etc/passwd" 파일의 소유자 및 권한 변경 (소유자 root, 권한 644, HP-UX 는 400) #chown root /etc/passwd #chmod 444 /etc/passwd									
조치 시 영향	일반적인 경우 영향 없음								

UNIX 서버

취약점 항목		2.4. /etc/shadow 파일 소유자 및 권한 설정			
대상 OS	SunOS, LINUX, AIX, HP-UX	위험도	상	Code	U-19
취약점 개요	"/etc/shadow" 파일은 시스템에 등록된 모든 계정의 패스워드를 암호화된 형태로 저장 및 관리하고 있는 중요 파일로 root 계정을 제외한 모든 사용자의 접근을 제한하여야 함. 해당 파일에 대한 권한 관리가 이루어지지 않을 경우 ID 및 패스워드 정보가 외부로 노출될 수 있는 위험이 존재함.				
보안대책					
판단기준	양호: /etc/shadow 파일의 소유자가 root이고, 권한이 400인 경우				
	취약: /etc/shadow 파일의 소유자가 root가 아니거나, 권한이 400이 아닌 경우				
조치방법	"/etc/shadow" 파일의 소유자 및 권한 변경 (소유자 root, 권한 400)				
보안설정방법					
OS별 점검 파일 위치 및 점검 방법					
SunOS, LINUX		# ls -l /etc/shadow (※ shadow 파일 구조: 부록 참고) r----- root <shadow 파일>			
AIX		# ls -ld /etc/security/passwd (※ passwd 파일 구조: 부록 참고) r----- root <passwd 파일>			
HP-UX		# ls -ld /tcb/files/auth r----- root <auth 디렉터리>			

위에 제시된 파일 및 디렉터리의 소유자가 root가 아니거나 파일의 권한이 400이 아닌 경우 아래의 보안설정방법에 따라 설정을 변경함

■ SunOS, LINUX

1. "/etc/shadow" 파일의 소유자 및 권한 확인

#ls -l /etc/shadow

2. "/etc/shadow" 파일의 소유자 및 권한 변경 (소유자 root, 권한 400)

#chown root /etc/shadow

#chmod 400 /etc/shadow

■ AIX

AIX 서버는 기본적으로 "/etc/security/passwd" 파일에 패스워드를 암호화하여 저장·관리하므로 해당 디렉터리 권한을 기준에 맞게 설정

1. /etc/security/passwd 디렉터리의 소유자 및 권한 확인

#ls -ld /etc/security/passwd

2. /etc/security/passwd 디렉터리의 소유자 및 권한 변경 (소유자 root, 권한 400)

#chown root /etc/security/passwd

#chmod 400 /etc/security/passwd

UNIX 서버

■ HP-UX

HP-UX 서버는 Trusted Mode로 전환할 경우 패스워드를 암호화하여 "/tcb/files/auth" 디렉터리에 계정 이니셜과 계정명에 따라 파일로 저장·관리 가능

1. /tcb/files/auth 디렉터리의 소유자 및 권한 확인

```
#ls -ld /tcb/files/auth
```

2. /tcb/files/auth 디렉터리의 소유자 및 권한 변경 (소유자 root, 권한 400)

```
#chown root /tcb/files/auth
```

```
#chmod 400 /tcb/files/auth
```

조치 시 영향	일반적인 경우 영향 없음
----------------	---------------

UNIX 서버

취약점 항목		2.5. /etc/hosts 파일 소유자 및 권한 설정			
대상 OS	SunOS, LINUX, AIX, HP-UX	위험도	상	Code	U-20
취약점 개요	"/etc/hosts" 파일은 IP 주소와 호스트네임을 매핑 하는데 사용되는 파일이며, 이 파일의 접근권한 설정이 잘못 설정되어 있을 경우 악의적인 시스템을 신뢰하게 되므로 "/etc/hosts" 파일에 대한 접근권한을 제한하고 있는지 점검함.				
보안대책					
판단기준	양호: /etc/hosts 파일의 소유자가 root이고, 권한이 600인 경우				
	취약: /etc/hosts 파일의 소유자가 root가 아니거나, 권한이 600이 아닌 경우				
조치방법	"/etc/hosts" 파일의 소유자 및 권한 변경 (소유자 root, 권한 600)				
보안설정방법					
OS별 점검 파일 위치 및 점검 방법					
SunOS, LINUX, AIX, HP-UX		# ls -l /etc/hosts rw----- root <hosts 파일>			
"hosts" 파일의 소유자가 root가 아니거나 파일의 권한이 600이 아닌 경우 아래의 보안설정방법에 따라 설정을 변경함					
■ SunOS, LINUX, AIX, HP-UX					
"/etc/hosts" 파일의 소유자 및 권한 변경 (소유자 root, 권한 600)					
#chown root /etc/hosts					
#chmod 600 /etc/hosts					
조치 시 영향	일반적인 경우 영향 없음				

UNIX 서버

취약점 항목		2.6. /etc/(x)inetd.conf 파일 소유자 및 권한 설정			
대상 OS	SunOS, LINUX, AIX, HP-UX	위험도	상	Code	U-21
취약점 개요	*인터넷 슈퍼데몬 서비스 설정파일인 inetd.conf(xinetd.d) 파일에 대한 접근권한 제한 여부를 점검함. Inetd.conf(xinetd.d)의 접근권한이 잘못 설정되어 있을 경우 비인가자가 악의적인 프로그램을 등록하고 root 권한으로 서비스를 실행시켜 기존 서비스에 영향을 줄 수 있음.				
	*인터넷 슈퍼데몬: 외부 네트워크의 요청이 있을 때 "/etc/inetd.conf"에 등록된 내부 프로그램인 인터넷 서비스들의 데몬을 실행시켜주는 역할을 함.				
보안대책					
판단기준	양호: /etc/inetd.conf 파일의 소유자가 root이고, 권한이 600인 경우				
	취약: /etc/inetd.conf 파일의 소유자가 root가 아니거나, 권한이 600이 아닌 경우				
조치방법	"/etc/inetd.conf" 파일의 소유자 및 권한 변경 (소유자 root, 권한 600)				
보안설정방법					
OS별 점검 파일 위치 및 점검 방법					
SunOS, LINUX, AIX, HP-UX		"/etc/inetd.conf" 파일의 소유자 및 권한 확인 #ls -l /etc/inetd.conf rw----- root <inetd.conf 파일>			
LINUX (Xinetd)		"/etc/xinetd.conf" 파일 및 "/etc/xinetd.d/" 하위 모든 파일의 소유자 및 권한 확인 #ls -l /etc/xinetd.conf #ls -al /etc/xinetd.d/* rw----- root <xinetd.conf 파일> rw----- root <xinetd.d 디렉터리 내 모든 파일>			
인터넷 슈퍼데몬 서비스 설정파일의 소유자가 root가 아니거나 파일의 권한이 600이 아닌 경우 아래의 보안설정방법에 따라 설정을 변경함					
■ SunOS, LINUX, AIX, HP-UX					
"/etc/inetd.conf" 파일의 소유자 및 권한 변경 (소유자 root, 권한 600)					
#chown root /etc/inetd.conf					
#chmod 600 /etc/inetd.conf					
■ LINUX - xinetd					
"/etc/inetd.conf" 파일의 소유자 및 권한 변경 (소유자 root, 권한 600)					
#chown root /etc/xinetd.conf					
#chmod 600 /etc/xinetd.conf					
※ "/etc/xinetd.d/" 하위 디렉터리에 취약한 파일도 위와 동일한 방법으로 조치					
조치 시 영향	일반적인 경우 영향 없음				

UNIX 서버

취약점 항목	2.7. /etc/syslog.conf 파일 소유자 및 권한 설정				
대상 OS	SunOS, LINUX, AIX, HP-UX	위험도	상	Code	U-22
취약점 개요	"/etc/syslog.conf" 파일은 시스템 운영 중 발생하는 주요 로그 기록을 설정하는 파일로 관리자 이외의 사용자는 해당 파일을 변경할 수 없도록 하여야 함. 만약, 해당 파일의 접근권한이 적절하지 않을 경우 시스템 로그가 정상적으로 기록되지 않아 침입자의 흔적 또는, 시스템 오류 사항을 정확히 분석할 수 없음.				
보안대책					
판단기준	양호: /etc/syslog.conf 파일의 소유자가 root이고, 권한이 644인 경우				
	취약: /etc/syslog.conf 파일의 소유자가 root가 아니거나, 권한이 644가 아닌 경우				
조치방법	"/etc/syslog.conf" 파일의 소유자 및 권한 변경 (소유자 root, 권한 644)				
보안설정방법					
OS별 점검 파일 위치 및 점검 방법					
SunOS, LINUX, AIX, HP-UX	"/etc/syslog.conf" 파일의 소유자 및 권한 확인 #ls -l /etc/syslog.conf rw-r--r-- root <syslog.conf 파일>				
"syslog.conf" 파일의 소유자가 root가 아니거나 파일의 권한이 644가 아닌 경우 아래의 보안설정방법에 따라 설정을 변경함					
■ SunOS, LINUX, AIX, HP-UX					
"/etc/syslog.conf" 파일의 소유자 및 권한 변경 (소유자 root, 권한 644)					
#chown root /etc/syslog.conf					
#chmod 644 /etc/syslog.conf					
조치 시 영향	일반적인 경우 영향 없음				

UNIX 서버

취약점 항목	2.8. /etc/services 파일 소유자 및 권한 설정				
대상 OS	SunOS, LINUX, AIX, HP-UX	위험도	상	Code	U-23
취약점 개요	서비스 관리를 위해 사용되는 /etc/services 파일이 일반 사용자에게 의해 접근 및 변경이 가능하면, 정상적인 서비스를 제한하거나 허용되지 않은 서비스를 악의적으로 실행시켜 침해사고를 발생시킬 수 있음. 따라서 소유자 권한 설정을 통해 접근을 제한하여야 함.				
보안대책					
판단기준	양호: /etc/services 파일의 소유자가 root이고, 권한이 644인 경우				
	취약: /etc/services 파일의 소유자가 root가 아니거나, 권한이 644가 아닌 경우				
조치방법	"/etc/services" 파일의 소유자 및 권한 변경 (소유자 root, 권한 644)				
보안설정방법					
OS별 점검 파일 위치 및 점검 방법					
SunOS, LINUX, AIX, HP-UX		"/etc/services" 파일의 소유자 및 권한 확인 #ls -l /etc/services rw-r--r-- root <services 파일>			
"services" 파일의 소유자가 root가 아니거나 파일의 권한이 644가 아닌 경우 아래의 보안설정방법에 따라 설정을 변경함					
■ SunOS, LINUX, AIX, HP-UX					
"/etc/services" 파일의 소유자 및 권한 변경 (소유자 root, 권한 644)					
#chown root /etc/services					
#chmod 644 /etc/services					
조치 시 영향	일반적인 경우 영향 없음				

UNIX 서버

취약점 항목		2.9. SUID, SGID, Sticky bit 설정파일 점검			
대상 OS	SunOS, LINUX, AIX, HP-UX	위험도	상	Code	U-24
취약점 개요	*SUID(Set User-ID)와 *SGID(Set Group-ID)가 설정된 파일은(특히, root 소유의 파일인 경우) 특정 명령어를 실행하여 root 권한 획득 및 정상서비스 장애를 발생시킬 수 있으며, 로컬 공격에 많이 이용되므로 보안상 철저한 관리가 필요함. root 소유의 SUID 파일의 경우에는 꼭 필요한 파일을 제외하고는 SUID, SGID 속성을 제거해주고, 잘못 설정되어 보안 위협이 되고 있는지 주기적인 진단 및 관리가 요구됨.				
	*SUID(Set User-ID): 설정된 파일 실행 시, 특정 작업 수행을 위하여 일시적으로 파일 소유자의 권한을 얻게 됨.				
	*SGID(Set Group-ID): 설정된 파일 실행 시, 특정 작업 수행을 위하여 일시적으로 파일 소유 그룹의 권한을 얻게 됨.				
보안대책					
판단기준	양호: 주요 파일의 권한에 SUID와 SGID에 대한 설정이 부여되어 있지 않은 경우				
	취약: 주요 파일의 권한에 SUID와 SGID에 대한 설정이 부여되어 있는 경우				
조치방법	1. 불필요한 SUID, SGID 파일 제거 2. 아래의 목록 이외에 애플리케이션에서 생성한 파일이나, 사용자가 임의로 생성한 파일 등 의심스럽거나 특이한 파일의 발견 시 SUID 제거 필요				
보안설정방법					
OS별 점검 파일 위치 및 점검 방법					
SunOS, LINUX, AIX, HP-UX		OS별 주요 파일에 대한 SUID/SGID 설정 여부 확인 #ls -alL [check_file] awk '{print \$1}' grep -i 's'			
주요 파일에 불필요한 SUID/SGID가 설정된 경우 아래의 보안설정방법에 따라 SUID/SGID를 제거함					
■ SunOS, LINUX, AIX, HP-UX					
1. 제거 방법					
#chmod -s <file_name>					
2. 주기적인 감사 방법					
#find / -user root -type f ₩(-perm -04000 -o -perm -02000 ₩) -xdev -exec ls -al {} ₩;					
3. 반드시 사용이 필요한 경우 특정 그룹에서만 사용하도록 제한하는 방법					
일반 사용자의 Setuid 사용을 제한함 (임의의 그룹만 가능)					
#/usr/bin/chgrp <group_name> <setuid_file_name>					
#/usr/bin/chmod 4750 <setuid_file_name>					

UNIX 서버

■ 아래의 표에서 파일명을 확인하여 SUID, SGID을 제거하여야 함

SunOS		
/usr/bin/admintool	/usr/dt/bin/dtprintinfo	/usr/sbin/arp
/usr/bin/at	/usr/dt/bin/sdtcm_convert	/usr/sbin/lpmove
/usr/bin/atq	/usr/lib/fs/ufs/ufsdump	/usr/sbin/prtconf
/usr/bin/atrm	/usr/lib/fs/ufs/ufsrestore	/usr/sbin/sysdef
/usr/bin/lpset	/usr/lib/lp/bin/netpr	/usr/sbin/sparcv7/prtconf
/usr/bin/newgrp	/usr/openwin/bin/ff.core	/usr/sbin/sparcv7/sysdef
/usr/bin/nispasswd	/usr/openwin/bin/kcms_calibrate	/usr/sbin/sparcv9/prtconf
/usr/bin/rdist	/usr/openwin/bin/kcms_configure	/usr/sbin/sparcv9/sysdef
/usr/bin/yppasswd	/usr/openwin/bin/xlock	
/usr/dt/bin/dtappgather	/usr/platform/sun4u/sbin/prtdiag	

Linux		
/sbin/dump	/usr/bin/lpq-lpd	/usr/bin/newgrp
/sbin/restore	/usr/bin/lpr	/usr/sbin/lpc
/sbin/unix_chkpwd	/usr/bin/lpr-lpd	/usr/sbin/lpc-lpd
/usr/bin/at	/usr/bin/lprm	/usr/sbin/traceroute
/usr/bin/lpq	/usr/bin/lprm-lpd	

AIX		
/usr/dt/bin/dtaction	/usr/dt/bin/dtterm	/usr/bin/X11/xlock
/usr/sbin/mount	/usr/sbin/lchangelv	

HP-UX		
/opt/perf/bin/glance	/usr/dt/bin/dtprintinfo	/usr/sbin/swreg
/opt/perf/bin/gpm	/usr/sbin/arp	/usr/sbin/swremove
/opt/video/lbin/camServer	/usr/sbin/lanadmin	/usr/contrib/bin/traceroute
/usr/bin/at	/usr/sbin/landiag	/usr/dt/bin/dtappgather
/usr/bin/lpalt	/usr/sbin/lpsched	/usr/sbin/swmodify
/usr/bin/mediainit	/usr/sbin/swacl	/usr/sbin/swpackage
/usr/bin/newgrp	/usr/sbin/swconfig	
/usr/bin/rdist	/usr/sbin/swinstall	

조치 시 영향 SUID 제거 시 OS 및 응용 프로그램 등 서비스 정상작동 유무 확인 필요

UNIX 서버

취약점 항목	2.10. 사용자, 시스템 시작파일 및 환경파일 소유자 및 권한 설정				
대상 OS	SunOS, LINUX, AIX, HP-UX	위험도	상	Code	U-25
취약점 개요	환경변수 파일의 접근권한 설정이 잘못되어 있을 경우 비인가자가 다양한 방법으로 사용자 환경을 변경하여 침해사고를 일으킬 수 있으므로 홈 디렉터리 내의 환경변수 파일에 대한 접근 권한(읽기/쓰기/실행)의 적정성을 점검함.				
보안대책					
판단기준	양호: 홈 디렉터리 환경변수 파일 소유자가 root 또는, 해당 계정으로 지정되어 있고, 홈 디렉터리 환경변수 파일에 root와 소유자만 쓰기 권한이 부여된 경우				
	취약: 홈 디렉터리 환경변수 파일 소유자가 root 또는, 해당 계정으로 지정되지 않고, 홈 디렉터리 환경변수 파일에 root와 소유자 외에 쓰기 권한이 부여된 경우				
조치방법	환경변수 파일의 권한 중 타 사용자 쓰기 권한 제거 (".profile", ".kshrc", ".cshrc", ".bashrc", ".bash_profile", ".login", ".exrc", ".netrc" 등)				
보안설정방법					
OS별 점검 파일 위치 및 점검 방법					
SunOS, LINUX, AIX, HP-UX	홈 디렉터리 환경변수 파일의 소유자 및 권한 확인 #ls -l <홈 디렉터리 환경변수 파일>				
홈 디렉터리 환경변수 파일의 소유자가 root 또는, 해당 계정으로 설정되어 있는지 확인 후 소유자 이외의 사용자에게 쓰기 권한이 부여되어 있을 경우 아래의 보안설정방법에 따라 설정을 변경함					
■ SunOS, LINUX, AIX , HP-UX					
1. 소유자 변경 방법 #chown <user_name> <file_name>					
2. 일반 사용자 쓰기 권한 제거 방법 #chmod o-w <file_name>					
조치 시 영향	일반적인 경우 영향 없음				

UNIX 서버

취약점 항목	2.11. world writable 파일 점검				
대상 OS	SunOS, LINUX, AIX, HP-UX	위험도	상	Code	U-26
취약점 개요	모든 사용자가 접근 및 수정할 수 있는 권한으로 설정된 파일이 존재할 경우 일반 사용자의 실수 또는, 악의적인 행위로 인해 주요 파일 정보가 노출되거나 시스템 장애를 유발할 수 있음. 만약 의도적으로 변경된 스크립트 파일을 root가 확인하지 않고 실행시켰을 경우 시스템 권한 노출을 비롯해 다양한 보안 위험이 초래될 수 있음.				
보안대책					
판단기준	양호: world writable 파일이 존재하지 않거나, 존재 시 설정 이유를 확인하고 있는 경우				
	취약: world writable 파일이 존재하나 해당 설정 이유를 확인하고 있지 않는 경우				
조치방법	world writable 파일 존재 여부를 확인하고 불필요한 경우 제거				
보안설정방법					
OS별 점검 파일 위치 및 점검 방법					
SunOS, LINUX, AIX, HP-UX		world writable 파일 존재 여부 확인 #find / -perm -2 -ls			
“world writable” 파일 존재 시 사용 목적을 확실히 알고 불필요 시 삭제, 필요 시 아래의 보안설정방법에 따라 설정을 변경함					
■ SunOS, LINUX, AIX, HP-UX					
1. 일반 사용자 쓰기 권한 제거 방법 #chmod o-w <file_name>					
2. 파일 삭제 방법 #rm -rf <world-writable 파일명>					
조치 시 영향	일반적인 경우 영향 없음				

UNIX 서버

취약점 항목		2.12. /dev에 존재하지 않는 device 파일 점검			
대상 OS	SunOS, LINUX, AIX, HP-UX	위험도	상	Code	U-27
취약점 개요	디바이스가 존재하지 않거나 이름이 잘못 입력된 경우 시스템은 */dev 디렉터리에 계속해서 파일을 생성하여 에러를 발생시킴. 따라서 실제 존재하지 않는 디바이스를 찾아 제거함으로써 root 파일 시스템 손상 및 다운 등의 문제를 방지하여야 함.				
	* /dev 디렉터리: 논리적 장치 파일을 담고 있는 /dev 디렉터리는 /devices 디렉터리에 있는 물리적 장치 파일에 대한 심볼릭 링크임. 예를 들어 rmt0를 rmto로 잘못 입력한 경우 rmto 파일이 새로 생성되는 것과 같이 디바이스 이름 입력 오류 시 root 파일 시스템이 에러를 일으킬 때까지 /dev 디렉터리에 계속해서 파일을 생성함.				
보안대책					
판단기준	양호: dev에 대한 파일 점검 후 존재하지 않은 device 파일을 제거한 경우				
	취약: dev에 대한 파일 미점검, 또는, 존재하지 않은 device 파일을 방치한 경우				
조치방법	major, minor, number를 가지지 않는 device 파일 제거				
보안설정방법					
OS별 점검 파일 위치 및 점검 방법					
SunOS, LINUX, AIX, HP-UX		dev에 존재하지 않는 device 파일 점검 #find /dev -type f -exec ls -l {} \;			
존재하지 않는 디바이스가 "dev" 디렉터리 내에 존재하는 경우 아래의 보안설정방법에 따라 제거함					
■ SunOS, LINUX, AIX, HP-UX					
#find /dev -type f -exec ls -l {} \; 명령으로 확인 후					
※ major, minor number를 가지지 않는 device일 경우 삭제					
조치 시 영향	일반적인 경우 영향 없음				

UNIX 서버

취약점 항목	2.13. \$HOME/.rhosts, hosts.equiv 사용 금지				
대상 OS	SunOS, LINUX, AIX, HP-UX	위험도	상	Code	U-28
취약점 개요	*r'command 사용을 통한 원격 접속은 *NET Backup이나 다른 용도로 사용되기도 하나, 보안상 매우 취약하여 서비스 포트가 열려있을 경우 중요 정보 유출 및 시스템 장애 발생 등 침해사고의 원인이 됨. 만약 사용이 불가피한 경우 /etc/hosts.equiv 파일 및 .rhosts 파일 사용자를 root 또는, 해당 계정으로 설정한 뒤 권한을 600으로 설정하고 해당 파일 설정에 '+' 설정(모든 호스트 허용)이 포함되지 않도록 함. *r'command: 인증 없이 관리자의 원격접속을 가능하게 하는 명령어들로 rsh(remsh), rlogin, rexec 등이 있음. *NET Backup: 이기종 운영체제 간 백업을 지원하는 Symantec 사의 백업 및 복구 툴을 말함.				
보안대책					
판단기준	양호: login, shell, exec 서비스를 사용하지 않거나, 사용 시 아래와 같은 설정이 적용된 경우 1. /etc/hosts.equiv 및 \$HOME/.rhosts 파일 소유자가 root 또는, 해당 계정인 경우 2. /etc/hosts.equiv 및 \$HOME/.rhosts 파일 권한이 600 이하인 경우 3. /etc/hosts.equiv 및 \$HOME/.rhosts 파일 설정에 '+' 설정이 없는 경우 취약: login, shell, exec 서비스를 사용하고, 위와 같은 설정이 적용되지 않은 경우				
조치방법	1. /etc/hosts.equiv 및 \$HOME/.rhosts 파일 소유자를 root 또는, 해당 계정으로 변경 2. /etc/hosts.equiv 및 \$HOME/.rhosts 파일 권한을 600 이하로 변경 3. /etc/hosts.equiv 및 \$HOME/.rhosts 파일에서 "+"를 제거하고 반드시 필요한 호스트 및 계정만 등록 (해당 내역 요청)				
보안설정방법					
OS별 점검 파일 위치 및 점검 방법					
SunOS, LINUX, AIX, HP-UX	1. 파일 소유자 및 권한 확인 #ls -al /etc/hosts.equiv #ls -al \$HOME/.rhosts rw----- root <hosts.equiv 파일> rw----- root <\$HOME/.rhosts 파일> 2. 계정 별 '+' 부여 적절성 확인 #cat /etc/hosts.equiv #cat \$HOME/.rhosts /etc/hosts.equiv : 서버 설정 파일 \$HOME/.rhosts : 개별 사용자의 설정 파일				
"/etc/hosts.equiv 및 \$HOME/.rhosts" 파일의 소유자가 root가 아니거나 파일의 권한이 600이 아닌 경우 아래의 보안설정방법에 따라 설정을 변경함					

UNIX 서버

■ SunOS, LINUX, AIX, HP-UX

1. "/etc/hosts.equiv" 및 "\$HOME/.rhosts" 파일의 소유자를 root 또는, 해당 계정으로 변경
 #chown root /etc/hosts.equiv
 #chown <user_name> \$HOME/.rhosts
2. "/etc/hosts.equiv" 및 "\$HOME/.rhosts" 파일의 권한을 600 이하로 변경
 #chmod 600 /etc/hosts.equiv
 #chmod 600 \$HOME/.rhosts
3. "/etc/hosts.equiv" 및 "\$HOME/.rhosts" 파일에서 "+"를 제거하고 허용 호스트 및 계정 등록
 #cat /etc/hosts.equiv (or \$HOME/.rhosts)

+ +	모든 호스트의 모든 계정을 신뢰
+ test	모든 호스트의 test 계정을 신뢰
Web1 +	Web1 호스트의 모든 계정을 신뢰

조치 시 영향	일반적인 경우 영향 없음
----------------	---------------

UNIX 서버

취약점 항목		2.14. 접속 IP 및 포트 제한			
대상 OS	SunOS, LINUX, AIX, HP-UX	위험도	상	Code	U-29
취약점 개요	UNIX 시스템이 제공하는 Telnet, FTP 등 많은 네트워크 서비스를 통한 외부 비인가자의 불법적인 접근 및 시스템 침해사고를 방지하기 위하여 TCP Wrapper를 이용하여 제한된 IP 주소에서만 접속할 수 있도록 설정함.				
보안대책					
판단기준	양호: /etc/hosts.deny 파일에 ALL Deny 설정 후 /etc/hosts.allow 파일에 접근을 허용할 특정 호스트를 등록한 경우				
	취약: 위와 같이 설정되지 않은 경우				
조치방법	/etc/hosts.deny 파일에 ALL Deny 설정 후 /etc/hosts.allow 파일에 접근 허용 IP 등록				
보안설정방법					
OS별 점검 파일 위치 및 점검 방법					
SunOS, LINUX, AIX		All deny 적용 확인 및 접근 허용 IP 적절성 확인 #cat /etc/hosts.deny #cat /etc/hosts.allow			
HP-UX		All deny 적용 확인 및 서비스 접근 가능 IP 확인 #cat /var/adm/inetd.sec			

위에 제시한 파일이 존재하지 않거나 All deny 설정이 적용되지 않은 경우 또는, 시스템 접근 제한 IP 설정 필요 시 아래의 보안설정방법에 따라 설정을 변경함

■ SunOS, LINUX, AIX

1. vi 편집기를 이용하여 “/etc/hosts.deny” 파일을 연 후 (해당 파일이 없을 경우 새로 생성)

2. 아래와 같이 수정 또는, 신규 삽입 (ALL Deny 설정)
(수정 전) 설정 없음
(수정 후) ALL:ALL

3. vi 편집기를 이용하여 “/etc/hosts.allow” 파일을 연 후 (해당 파일이 없을 경우 생성)
(수정 전) 설정 없음
(수정 후) sshd : 192.168.0.148, 192.168.0.6 (다른 서비스도 동일한 방식으로 설정)

< TCP Wrapper 접근제어 가능 서비스 >

▪ SYSTAT, FINGER, FTP, TELNET, RLOGIN, RSH, TALK, EXEC, TFTP, SSH

< TCP Wrapper는 다음 두 파일에 의해 접근이 제어됨 >

▪ /etc/hosts.deny --> 시스템 접근을 제한할 IP 설정

▪ /etc/hosts.allow --> 시스템 접근을 허용할 IP 설정

▪ not in either --> 모든 접근 허용

UNIX 서버

■ HP-UX

HP-UX 서버의 경우 `/var/adm/inetd.sec` 파일을 이용하여 서버 자체적으로 접근제어를 할 수 있으며, 해당 파일이 존재하지 않을 경우 `/usr/newconfig/var/adm/inetd.sec` 샘플 파일을 복사하여 사용함

1. vi 편집기를 이용하여 `/var/adm/inetd.sec` 파일을 연 후 (해당 파일이 없을 경우 새로 생성)
2. 아래와 같이 수정 또는, 신규 삽입 (ALL Deny 설정)
 - telnet 으로의 모든 접속 차단 => `telnet deny *.*.*`
 - telnet 접속을 허용할 IP 등록 => `telnet allow [telnet 접속 허용 IP 등록]`
 (다른 서비스들도 위와 동일한 방법으로 설정)

조치 시 영향	허용되지 않은 IP는 접속 불가
----------------	-------------------

UNIX 서버

취약점 항목	2.15. hosts.lpd 파일 소유자 및 권한 설정				
대상 OS	SunOS, LINUX, AIX, HP-UX	위험도	하	Code	U-30
취약점 개요	* /etc/hosts.lpd 파일에 일반 사용자가 접근할 수 있다면 이 파일을 가지고 host 파일에 접근하여 공격을 할 수 있으므로 /etc/hosts.lpd 파일의 소유자와 퍼미션 설정을 확인하여야 함. * hosts.lpd 파일: 로컬 프린트 서비스를 사용할 수 있는 허가된 호스트(사용자) 정보를 담고 있는 파일을 말함. (hostname 또는, IP 주소를 포함하고 있음)				
보안대책					
판단기준	양호: 파일의 소유자가 root이고 Other에 쓰기 권한이 부여되어 있지 않는 경우				
	취약: 파일의 소유자가 root가 아니고 Other에 쓰기 권한이 부여되어 있는 경우				
조치방법	hosts.lpd 파일의 퍼미션을 확인하여 퍼미션 600, 파일 소유자를 root로 변경				
보안설정방법					
OS별 점검 파일 위치 및 점검 방법					
SunOS, LINUX, AIX, HP-UX		#ls -l /etc/hosts.lpd rw----- root <hosts.lpd 파일>			
"hosts.lpd " 파일의 소유자가 root가 아니거나 파일의 권한이 600이 아닌 경우 아래의 보안설정방법에 따라 설정을 변경함					
■ SunOS, LINUX, AIX, HP-UX					
1. 파일의 퍼미션 변경. #chmod 600 /etc/hosts.lpd					
2. 소유자를 root로 변경 #chown root /etc/hosts.lpd					
조치 시 영향	일반적인 경우 영향 없음				

UNIX 서버

취약점 항목	2.16. NIS 서비스 비활성화				
대상 OS	SunOS, LINUX, AIX, HP-UX	위험도	중	Code	U-31
취약점 개요	NIS(Network Information Service) 주 서버는 정보표를 소유하여 NIS 대응 파일들로 변환하고, 이 대응 파일들이 네트워크를 통해 제공됨으로써 모든 컴퓨터에 정보가 갱신되도록 할 수 있으며 사용자들은 패스워드를 한 번만 바꾸어 NIS 영역에 들어 있는 모든 컴퓨터의 정보를 갱신할 수 있음. 하지만 NIS 이용 시 서버 정보 유출 위험이 존재하는 등 보안에 취약함.				
보안대책					
판단기준	양호: 불필요한 NIS 서비스가 비활성화 되어있는 경우				
	취약: 불필요한 NIS 서비스가 활성화 되어있는 경우				
조치방법	NIS 서비스를 사용하지 않는 경우 NIS 서비스 비활성화				
보안설정방법					
OS별 점검 파일 위치 및 점검 방법					
SunOS, LINUX, AIX		NIS 서비스 활성화 여부 확인 #ps -ef grep yp			
불필요한 “NIS” 서비스가 실행중인 경우 아래의 보안설정방법에 따라 비활성화 상태로 변경함					
■ SunOS, LINUX, AIX					
1. NIS 서비스가 불필요하다면 비활성화 상태로 설정 - NIS 서비스 정지: #/usr/lib/netshvc/yp/ypstop - 서비스 확인: #ps -ef grep yp #rm -r /var/yp/blue.org #rm /etc/ethers /etc/netgroup /etc/timezone /etc/bootparams #vi /etc/nsswitch.conf					
2. NIS 설정 삭제					
조치 시 영향	일반적인 경우 영향 없음				

UNIX 서버

취약점 항목		2.17. UMASK 설정 관리			
대상 OS	SunOS, LINUX, AIX, HP-UX	위험도	중	Code	U-32
취약점 개요	시스템 내에서 사용자가 새로 생성하는 파일의 접근권한은 *UMASK 값에 따라 정해짐. 현재 설정된 UMASK는 명령 프롬프트에서 "umask"를 수행하여 확인할 수 있으며 UMASK 값이 "027" 또는, "022"이기를 권장함. UMASK 값 "027"은 "rw-r-----" 접근권한으로 파일이 생성됨. UMASK 값 "022"는 "rw-r--r--" 접근권한으로 파일이 생성됨. 계정의 Start Profile(/etc/profile, /etc/default/login, .cshrc, .kshrc, .bashrc, .login, .profile 등)에 명령을 추가하면, 사용자가 로그인 한 후에도 변경된 UMASK 값을 적용 받게 되며 잘못 설정된 UMASK 값은 잘못된 권한의 파일을 생성시킴. *UMASK: 파일 및 디렉터리 생성 시 기본 퍼미션을 지정해 주는 명령어를 말함.				
	보안대책				
판단기준	양호: UMASK 값이 022 이하로 설정된 경우				
	취약: UMASK 값이 022 이하로 설정되지 않은 경우				
조치방법	설정파일에 UMASK 값을 "022"로 설정.				
보안설정방법					
OS별 점검 파일 위치 및 점검 방법					
SunOS, AIX, LINUX, HP-UX		#vi /etc/profile UMASK=022			
위에 제시한 UMASK 값이 해당 파일에 적용되지 않은 경우 아래의 보안설정방법에 따라 적용함					
■ SunOS					
방법-1. "/etc/profile" 파일을 이용한 UMASK 설정 변경					
1. vi 편집기를 이용하여 "/etc/profile" 파일을 연 후					
2. 아래와 같이 수정 또는, 신규 삽입					
umask 022					
export umask					
방법-2. "/etc/default/login" 파일을 이용한 UMASK 설정 변경					
1. vi 편집기를 이용하여 "/etc/default/login" 파일을 연 후					
2. 아래와 같이 수정 또는, 신규 삽입					
(수정 전) #UMASK=022					
(수정 후) UMASK=022					
■ LINUX, HP-UX					
1. vi 편집기를 이용하여 "/etc/profile" 파일을 연 후					

UNIX 서버

2. 아래와 같이 수정 또는, 신규 삽입

```
umask 022
export umask
```

■ AIX

방법-1. "/etc/profile" 파일을 이용한 UMASK 설정 변경

1. vi 편집기를 이용하여 "/etc/profile" 파일을 연 후
2. 아래와 같이 수정 또는, 신규 삽입

```
umask 022
export umask
```

방법-2. "/etc/security/user" 파일을 이용한 UMASK 설정 변경

1. vi 편집기를 이용하여 "/etc/security/user" 파일을 연 후
2. default 설정 부분을 아래와 같이 수정 또는, 신규 삽입

```
(수정 전) umask =
(수정 후) umask = 022
```

조치 시 영향	일반적인 경우 영향 없음
----------------	---------------

UNIX 서버

취약점 항목	2.18. 홈 디렉터리 소유자 및 권한 설정				
대상 OS	SunOS, LINUX, AIX, HP-UX	위험도	중	Code	U-33
취약점 개요	사용자 홈 디렉터리 내 설정파일이 비인가자에 의해 변조되면 정상적인 사용자 서비스가 제한됨, 해당 홈 디렉터리의 소유자 외 일반 사용자들이 해당 홈 디렉터리를 수정할 수 없도록 제한하고 있는지 점검하여 정상적인 사용자 환경 구성 및 서비스 제공 유무를 확인함.				
보안대책					
판단기준	양호: 홈 디렉터리 소유자가 해당 계정이고, 일반 사용자 쓰기 권한이 제거된 경우				
	취약: 홈 디렉터리 소유자가 해당 계정이 아니고, 일반 사용자 쓰기 권한이 부여된 경우				
조치방법	사용자별 홈 디렉터리 소유주를 해당 계정으로 변경하고, 타사용자의 쓰기 권한 제거 ("/etc/passwd" 파일에서 홈 디렉터리 확인, 진단 보고서에서 조치할 홈 디렉터리 확인)				
보안설정방법					
OS별 점검 파일 위치 및 점검 방법					
SunOS, LINUX, AIX, HP-UX	"/etc/passwd" 파일에서 사용자별 홈 디렉터리 확인 후 소유자 및 권한 확인 #cat /etc/passwd #ls -ald <user-home-directory>				
"/etc/passwd" 파일 내 존재하는 모든 사용자 계정이 적절한 홈 디렉터리를 갖는지 확인함 홈 디렉터리 소유자가 해당 계정이 아니거나, 부적절한 권한 설정이 적용된 경우 아래의 보안설정방법에 따라 적용함					
■ SunOS, LINUX, AIX, HP-UX "/etc/passwd" 파일의 소유자 및 권한 변경 #chown <user_name> <user_home_directory> #chmod o-w <user_home_directory>					
조치 시 영향	홈 디렉터리를 업로드 등의 용도로 애플리케이션에서 사용할 수 있기 때문에 권한 변경 시 확인이 필요함				

UNIX 서버

취약점 항목		2.19. 홈 디렉터리로 지정한 디렉터리의 존재 관리			
대상 OS	SunOS, LINUX, AIX, HP-UX	위험도	중	Code	U-34
취약점 개요	사용자 홈 디렉터리는 사용자가 로그인한 후 작업을 수행하는 디렉터리임. 로그인 후 사용자 홈 디렉터리에 존재하는 사용자 환경 설정파일에 의해 사용자 환경이 구성되며 홈 디렉터리의 부재로 인한 다음의 보안상 문제가 발생할 수 있음.				
	1. 홈 디렉터리가 존재하지 않는 경우 root 계정이 아닌 일반 사용자의 홈 디렉터리가 /로 되어있을 경우 로그인 시 사용자 현재 디렉터리가 /로 로그인 되므로 관리·보안상 문제가 발생됨. 2. 홈 디렉터리 내에 숨겨진 디렉터리가 존재하는 경우 정당하지 못한 사용자가 파일을 숨길 목적으로 만들어 놓은 것일 수 있음. 3. 홈 디렉터리 내에 시스템 명령의 이름을 가진 불법적인 실행파일이 존재하는 경우 상대경로와 시스템 명령을 입력하여 불법적인 파일이 실행되게 함.				
보안대책					
판단기준	양호: 홈 디렉터리가 존재하지 않는 계정이 발견되지 않는 경우				
	취약: 홈 디렉터리가 존재하지 않는 계정이 발견된 경우				
조치방법	홈 디렉터리가 존재하지 않는 계정에 홈 디렉터리 설정 또는, 계정 삭제				
보안설정방법					
OS별 점검 파일 위치 및 점검 방법					
SunOS, LINUX, AIX, HP-UX		사용자 계정 별 홈 디렉터리 지정 여부 확인 #cat /etc/passwd			
"/etc/passwd" 파일 내 존재하는 모든 사용자 계정이 적절한 홈 디렉터리를 갖는지 확인한 후 홈 디렉터리가 존재하지 않는 계정이 발견된 경우 아래의 보안설정방법에 따라 적용함					
■ SunOS, LINUX, AIX, HP-UX					
1. 홈 디렉터리가 없는 사용자 계정 삭제					
• SunOS, LINUX, HP-UX 설정: #userdel <user_name>					
• AIX 설정: #rmuser <user_name>					
2. 홈 디렉터리가 없는 사용자 계정에 홈 디렉터리 지정					
#vi /etc/passwd					
#test:x:501:501::/home/test:/bin/bash (/home/test=홈 디렉터리)					
#test:x:501:501::/data:/bin/bash (홈 디렉터리 수정 /home/test -> /data)					
조치 시 영향	일반적인 경우 영향 없음				

UNIX 서버

취약점 항목	2.20. 숨겨진 파일 및 디렉터리 검색 및 제거				
대상 OS	SunOS, LINUX, AIX, HP-UX	위험도	하	Code	U-35
취약점 개요	불법적으로 생성되었거나 숨겨진 의심스러운 파일로부터 침입자는 정보 습득이 가능하며, 파일을 임의로 변경할 수 있음. [...]으로 시작하는 숨겨진 파일 존재 여부 확인 후 불법적이거나 의심스러운 파일을 삭제함.				
보안대책					
판단기준	양호: 디렉터리 내 숨겨진 파일을 확인하여, 불필요한 파일 삭제를 완료한 경우				
	취약: 디렉터리 내 숨겨진 파일을 확인하지 않고, 불필요한 파일을 방치한 경우				
조치방법	ls -al 명령어로 숨겨진 파일 존재 파악 후 불법적이거나 의심스러운 파일을 삭제함				
보안설정방법					
OS별 점검 파일 위치 및 점검 방법					
SunOS, LINUX, AIX, HP-UX,		특정 디렉터리 내 불필요한 파일 점검 #ls -al [디렉터리명]			
특정 디렉터리 내 숨겨진 파일을 확인한 후 불필요한 경우 파일 삭제를 권고함					
■ SunOS, LINUX, AIX, HP-UX					
1. 숨겨진 파일 목록에서 불필요한 파일 삭제					
2. 마지막으로 변경된 시간에 따라, 최근 작업한 파일 확인 시 [-t] 플래그 사용					
조치 시 영향	일반적인 경우 영향 없음				

UNIX 서버

3. 서비스 관리

취약점 항목		3.1. Finger 서비스 비활성화			
대상 OS	SunOS, LINUX, AIX, HP-UX	위험도	상	Code	U-36
취약점 개요	*Finger(사용자정보 확인 서비스)를 통해서 네트워크 외부에서 해당 시스템에 등록된 사용자 정보를 확인할 수 있으므로, 사용하지 않는다면 해당 서비스를 중지하여야 함.				
	*Finger(사용자정보 확인 서비스): who 명령어가 현재 사용 중인 사용자들에 대한 간단한 정보만을 보여주는 데 반해 finger 명령은 옵션에 따른 시스템에 등록된 사용자뿐만 아니라 네트워크를 통하여 연결되어 있는 다른 시스템에 등록된 사용자들에 대한 자세한 정보를 보여줌.				
보안대책					
판단기준	양호: Finger 서비스가 비활성화 되어 있는 경우				
	취약: Finger 서비스가 활성화 되어 있는 경우				
조치방법	Finger 서비스 비활성화				
보안설정방법					
OS별 점검 파일 위치 및 점검 방법					
LINUX, AIX, HP-UX, SunOS 5.9 이하 버전		#cat /etc/inetd.conf #finger stream tcp nowait bin /usr/sbin/fingerd fingerd 주석처리 확인			
SunOS 5.10 이상 버전		#inetadm grep "finger"			
LINUX (xinetd일 경우)		#ls -alL /etc/xinetd.d/* egrep "echo finger"			
위에 제시된 파일 내 "finger" 서비스가 활성화된 경우 아래의 보안설정방법에 따라 서비스 중지					
■ LINUX, AIX, HP-UX, SunOS 5.9 이하 버전					
1. "/etc/inetd.conf" 파일에서 finger 서비스 라인 #처리(주석처리) (수정 전) finger stream tcp nowait bin /usr/sbin/fingerd fingerd (수정 후) #finger stream tcp nowait bin /usr/sbin/fingerd fingerd					
2. inetd 서비스 재시작 #ps -ef grep inetd root 141 1 0 15:03:22 ? 0:01 /usr/sbin/inetd -s #kill -HUP [PID]					
■ SunOS 5.10 이상 버전					
inetadm -d "중지하고자 하는 데몬" 명령으로 서비스 데몬 중지 #inetadm -d svc:/network/finger:default					
■ LINUX (xinetd일 경우)					
1. vi 편집기를 이용하여 "/etc/xinetd.d/finger" 파일을 연 후					

UNIX 서버

2. 아래와 같이 설정 (Disable = yes 설정)

```

service finger
{
    socket_type      = stream
    wait             = no
    user             = nobody
    server           = /usr/sbin/in.fingerd
    disable          = yes
}

```

3. xinetd 서비스 재시작

```
#service xinetd restart
```

조치 시 영향	일반적으로 영향 없음
----------------	-------------

UNIX 서버

취약점 항목		3.2. Anonymous FTP 비활성화			
대상 OS	SunOS, LINUX, AIX, HP-UX	위험도	상	Code	U-37
취약점 개요	*Anonymous FTP(익명 FTP)를 사용할 경우 악의적인 사용자가 시스템에 관한 정보를 획득할 수 있으며 디렉터리에 쓰기 권한이 설정되어 있을 경우 local exploit을 사용하여 다양한 공격이 가능하게 되므로 반드시 필요한 사용자만 접속 할 수 있도록 설정하여 권한 없는 사용자의 FTP 사용을 제한하여야 함.				
	*Anonymous FTP(익명 FTP): 파일 전송을 위해서는 원칙적으로 상대방 컴퓨터를 사용할 수 있는 계정이 필요하나 누구든지 계정 없이도 anonymous 또는, ftp라는 로그인 명과 임의의 비밀번호를 사용하여 FTP를 실행할 수 있음.				
보안대책					
판단기준	양호: Anonymous FTP (익명 ftp) 접속을 차단한 경우				
	취약: Anonymous FTP (익명 ftp) 접속을 차단하지 않은 경우				
조치방법	Anonymous FTP를 사용하지 않는 경우 Anonymous FTP 접속 차단 설정 적용				
보안설정방법					
OS별 점검 파일 위치 및 점검 방법					
SunOS, LINUX, AIX, HP-UX		/etc/passwd 파일에 ftp 계정 존재 여부 확인 #cat /etc/passwd grep "ftp"			
"passwd" 파일 내 ftp 계정이 존재하는 경우 아래의 보안설정방법에 따라 서비스 접속 제한					
■ SunOS, LINUX, AIX, HP-UX					
1. 일반 FTP - Anonymous FTP 접속 제한 설정 방법					
"/etc/passwd" 파일에서 ftp 또는, anonymous 계정 삭제					
▪ SunOS, LINUX, HP-UX 설정: #userdel ftp					
▪ AIX 설정: #rmuser ftp					
2. ProFTP - Anonymous FTP 접속 제한 설정 방법					
"/etc/passwd" 파일에서 ftp 계정 삭제					
▪ SunOS, LINUX, HP-UX 설정: #userdel ftp					
▪ AIX 설정: #rmuser ftp					
3. vsFTP - Anonymous FTP 접속 제한 설정 방법					
vsFTP 설정파일("/etc/vsftpd/vsftpd.conf" 또는, "/etc/vsftpd.conf")에서 anonymous_enable=NO 설정					
조치 시 영향	Anonymous FTP를 사용하지 않을 경우 영향 없음				

UNIX 서버

취약점 항목		3.3. r 계열 서비스 비활성화			
대상 OS	SunOS, LINUX, AIX, HP-UX	위험도	상	Code	U-38
취약점 개요	*r'command 사용을 통한 원격 접속은 *NET Backup이나 다른 용도로 사용되기도 하나, 보안상 매우 취약하여 서비스 포트가 열려있는 경우 중요 정보 유출 및 시스템 장애 발생 등 침해사고의 위험이 있음.				
	*r'command: 인증 없이 관리자의 원격접속을 가능하게 하는 명령어들로 rsh(remsh), rlogin, rexec 등이 있음.				
	*NET Backup: 이기종 운영체제 간 백업을 지원하는 Symantec 사의 백업 및 복구 툴을 말함.				
보안대책					
점검기준	양호: r 계열 서비스가 비활성화 되어 있는 경우				
	취약: r 계열 서비스가 활성화 되어 있는 경우				
조치방법	NET Backup등 특별한 용도로 사용하지 않는다면 아래의 서비스 중지				
보안설정방법					
OS별 점검 파일 위치 및 점검 방법					
SunOS	r'command 서비스 활성화 여부 확인 #svcs -a grep rlogin				
AIX	#cat /etc/inetd.conf grep rlogin (# 처리 되어 있으면 비활성화) #cat /etc/inetd.conf grep rsh (# 처리 되어 있으면 비활성화)				
HP-UX,	# vi /etc/inetd.conf r로 시작하는 필드 존재 시 취약				
SunOS 5.10 이상 버전	#inetadm egrep "shell rlogin rexec" r'command 관련 데몬 확인				
LINUX (xinetd일 경우)	rsh, rlogin, rexec (shell, login, exec) 서비스 구동 확인 #ls -alL /etc/xinetd.d/* egrep "rsh rlogin rexec" egrep -v "grep klogin kshell kexec"				

위에 제시된 파일 내 "r 계열" 서비스가 활성화된 경우 아래의 보안설정방법에 따라 서비스 중지

■ SunOS

1. r 계열 서비스 활성화 여부 확인 후 비활성화 조치

#svcs -a |grep rlogin

#svcadm disable svc:/network/login:rlogin

■ AIX

1. r 계열 서비스 활성화 여부 확인

#cat /etc/inetd.conf |grep rlogin (# 처리 되어 있으면 비활성화)

#cat /etc/inetd.conf |grep rsh (# 처리 되어 있으면 비활성화)

UNIX 서버

2. /etc/hosts.equiv 파일은 TRUSTED 시스템을 등록
3. .rhosts 파일은 사용자 별로 'r'command를 통해 접근이 가능하도록 설정할 수 있음(\$HOME/.rhosts)

■ HP-UX

1. r 계열 서비스 활성화 여부 확인
vi /etc/inetd.conf
2. r로 시작하는 필드 주석처리 후 재가동
inetd -c

■ SunOS 5.10 이상 버전

1. r'command 관련 데몬 확인

- svc:/network/login:rlogin
- svc:/network/rexec:default
- svc:/network/shell:kshell

2. inetadm -d “중지하고자 하는 데몬” 명령으로 데몬 중지
#inetadm -d svc:/network/login:rlogin
#inetadm -d svc:/network/rexec:default
#inetadm -d svc:/network/shell:kshell

■ LINUX (xinetd일 경우)

1. vi 편집기를 이용하여 “/etc/xinetd.d/” 디렉터리 내 rlogin, rsh, rexec 파일을 연 후
2. 아래와 같이 설정 (Disable = yes 설정)

```

• /etc/xinetd.d/rlogin 파일
• /etc/xinetd.d/rsh 파일
• /etc/xinetd.d/rexec 파일

service    rlogin
{
    socket_type      = stream
    wait             = no
    user             = nobody
    log_on_success   += USERID
    log_on_failure   += USERID
    server           = /usr/sbin/in.fingerd
    disable          = yes
}

```

3. xinetd 서비스 재시작
#service xinetd restart

조치 시 영향

rlogin, rshell, rexec 서비스는 backup 등의 용도로 종종 사용되며 /etc/hosts.equiv 또는, 각 홈 디렉터리 밑에 있는 .rhosts 파일에 설정 유무를 확인하여 해당 파일이 존재하지 않거나 해당 파일 내에 설정이 없다면 사용하지 않는 것으로 파악

UNIX 서버

취약점 항목	3.4. cron 파일 소유자 및 권한 설정				
대상 OS	SunOS, LINUX, AIX, HP-UX	위험도	상	Code	U-39
취약점 개요	*Cron 시스템은 cron.allow 파일과 cron.deny 파일을 통하여 명령어 사용자를 제한할 수 있으며 보안상 해당 파일에 대한 접근제한이 필요함. 만약 cron 접근제한 파일의 권한이 잘못되어 있을 경우 권한을 획득한 사용자가 악의적인 목적으로 임의의 계정을 등록하여 불법적인 예약 파일 실행으로 시스템 피해를 일으킬 수 있음.				
	*Cron 시스템: 특정 작업을 정해진 시간에 주기적이고 반복적으로 실행하기 위한 데몬과 그 설정들을 말함.				
보안대책					
판단기준	양호: cron 접근제어 파일 소유자가 root이고, 권한이 640 이하인 경우				
	취약: cron 접근제어 파일 소유자가 root가 아니거나, 권한이 640 이하가 아닌 경우				
조치방법	"cron.allow", "cron.deny" 파일 소유자 및 권한 변경 (소유자 root, 권한 640 이하)				
보안설정방법					
OS별 점검 방법					
SunOS, LINUX, AIX, HP-UX,	Cron 관련 파일 권한 확인 #ls -al <cron 접근제어 파일 경로> rw-r----- root <cron 접근제어 파일>				
OS별 점검 파일 위치					
LINUX, AIX, HP-UX	/var/spool/cron/crontabs/*				
SunOS	/etc/crontab, /etc/cron.daily/*, /etc/cron.hourly/*, /etc/cron.monthly/*, /etc/cron.weekly/*, /var/spool/cron/*				
"cron" 접근제어 설정이 적절하지 않은 경우 아래의 보안설정방법에 따라 설정을 변경함					
■ SunOS					
1. "/etc/cron.d/cron.allow" 및 "/etc/cron.d/cron.deny" 파일의 소유자 및 권한 확인					
#ls -l /etc/cron.d/cron.allow					
#ls -l /etc/cron.d/cron.deny					
2. "/etc/cron.d/cron.allow" 및 "/etc/cron.d/cron.deny" 파일의 소유자 및 권한 변경					
#chown root /etc/cron.d/cron.allow					
#chmod 640 /etc/cron.d/cron.allow					
#chown root /etc/cron.d/cron.deny					
#chmod 640 /etc/cron.d/cron.deny					
■ LINUX					
1. "/etc/cron.allow" 및 "/etc/cron.deny" 파일의 소유자 및 권한 확인					

UNIX 서버

```
#ls -l /etc/cron.allow
```

```
#ls -l /etc/cron.deny
```

2. "/etc/cron.allow" 및 "/etc/cron.deny" 파일의 소유자 및 권한 변경

```
#chown root /etc/cron.allow
```

```
#chmod 640 /etc/cron.allow
```

```
#chown root /etc/cron.deny
```

```
#chmod 640 /etc/cron.deny
```

■ AIX, HP-UX

1. "/var/adm/cron/cron.allow" 및 "/var/adm/cron/cron.deny" 파일의 소유자 및 권한 확인

```
#ls -l /var/adm/cron/cron.allow
```

```
#ls -l /var/adm/cron/cron.deny
```

2. "/var/adm/cron/cron.allow" 및 "/var/adm/cron/cron.deny" 파일의 소유자 및 권한 변경

```
#chown root /var/adm/cron/cron.allow
```

```
#chmod 640 /var/adm/cron/cron.allow
```

```
#chown root /var/adm/cron/cron.deny
```

```
#chmod 640 /var/adm/cron/cron.deny
```

조치 시 영향	일반적인 경우 영향 없음
----------------	---------------

UNIX 서버

취약점 항목		3.5. DoS 공격에 취약한 서비스 비활성화			
대상 OS	SunOS, LINUX, AIX, HP-UX	위험도	상	Code	U-40
취약점 개요	*Dos(서비스 거부 공격)에 취약한 echo, discard, daytime, chargen 서비스는 취약점이 많이 발표된 불필요한 서비스들로 해당 서비스 사용을 중지하여야 함. 만약 해당 서비스가 활성화되어 있는 경우 시스템 정보 유출 및 Dos(서비스 거부 공격)의 대상이 될 수 있음.				
	*Dos(Denial of Service attack): 시스템을 악의적으로 공격해 해당 시스템의 자원을 부족하게 하여 원래 의도된 용도로 사용하지 못하게 하는 공격임. 특정 서버에게 수많은 접속 시도를 만들어 다른 이용자가 정상적으로 서비스 이용을 하지 못하게 하거나, 서버의 TCP 연결을 바닥내는 등의 공격이 이 범위에 포함됨.				
보안대책					
점검기준	양호: Dos 공격에 취약한 echo, discard, daytime, chargen 서비스가 비활성화 된 경우				
	취약: Dos 공격에 취약한 echo, discard, daytime, chargen 서비스 활성화 된 경우				
조치방법	"cron.allow", "cron.deny" 파일 소유자 및 권한 변경 (소유자 root, 권한 640 이하)				
보안설정방법					
OS별 점검 파일 위치 및 점검 방법					
SunOS	#svcs -a grep echo #svcs -a grep daytime #svcs -a grep discard #svcs -a grep chargen echo, discard, daytime, chargen 서비스 활성 여부 확인				
AIX, HP-UX	# vi /etc/inetd.conf echo, discard, daytime, chargen 필드 주석처리 확인				
SunOS 5.10 이상 버전	#inetadm grep enabled egrep "echo discard daytime chargen" 명령으로 기타 서비스 데몬 확인				

아래 제시된 DoS 공격에 취약한 서비스가 활성화된 경우 아래의 보안설정방법에 따라 서비스 중지

DoS 공격에 취약한 서비스	
echo(7)	클라이언트에서 보내는 메시지를 단순히 재전송
discard(9)	수신되는 임의 사용자의 데이터를 폐기하는 서비스
daytime(13)	daytime은 클라이언트의 질의에 응답하여 아스키 형태로 현재 시간과 날짜를 출력하는 데몬
chargen(19)	임의 길이의 문자열을 반환하는 서비스

UNIX 서버

■ SunOS

1. echo 서비스 비활성화 설정

```
#svcs -a |grep echo
#svcadm disable svc:/network/echo:dgram
#svcadm disable svc:/network/echo:stream
```

2. discard 서비스 비활성화 설정

```
#svcs -a |grep daytime
#svcadm disable svc:/network/daytime:dgram
#svcadm disable svc:/network/daytime:stream
```

3. daytime 서비스 비활성화 설정

```
#svcs -a |grep discard
#svcadm disable svc:/network/discard:dgram
#svcadm disable svc:/network/discard:stream
```

4. chargen 서비스 비활성화 설정

```
#svcs -a |grep chargen
#svcadm disable svc:/network/chargen:dgram
#svcadm disable svc:/network/chargen:stream
```

■ AIX

1. vi편집기를 이용하여 echo, discard, daytime, chargen 필드 주석처리

```
#vi /etc/inetd.conf
#echo stream tcp nowait root internal
#discard stream tcp nowait root internal
#chargen stream tcp nowait root internal
#daytime stream tcp nowait root internal
```

■ HP-UX

1. vi편집기를 이용하여 echo, discard, daytime, chargen 필드 주석처리

```
# vi /etc/inetd.conf
```

2. 필드 주석처리 후 재가동

```
# inetd -c
```

■ SunOS 5.10 이상 버전

1. 기타 서비스 데몬 확인

- | | |
|-------------------------------|-------------------------------|
| • svc:/network/echo:dgram | • svc:/network/daytime:dgram |
| • svc:/network/echo:stream | • svc:/network/daytime:stream |
| • svc:/network/discard:dgram | • svc:/network/chargen:dgram |
| • svc:/network/discard:stream | • svc:/network/chargen:stream |

UNIX 서버

2. inetadm -d “중지하고자 하는 데몬” 명령으로 서비스 데몬 중지

```
#inetadm -d svc:/network/echo:stream
```

■ LINUX (xinetd일 경우)

1. vi 편집기를 이용하여 “/etc/xinetd.d/” 디렉터리 내 echo, discard, daytime, chargen 파일을 연 후
2. 아래와 같이 설정 (Disable = yes 설정)

- /etc/xinetd.d/echo 파일
- /etc/xinetd.d/discard 파일
- /etc/xinetd.d/daytime 파일
- /etc/xinetd.d/chargen 파일

```
service echo
```

```
{
    disable          = yes
    id               = echo-stream
    type             = INTERNAL
    wait             = no
    socket_type      = stream
}
```

3. xinetd 서비스 재시작

```
#service xinetd restart
```

조치 시 영향	일반적으로 사용하지 않는 서비스들임
----------------	---------------------

UNIX 서버

취약점 항목		3.6. NFS 서비스 비활성화			
대상 OS	SunOS, LINUX, AIX, HP-UX	위험도	상	Code	U-41
취약점 개요	*NFS(Network File System) 서비스는 root 권한 획득을 가능하게 하는 등 침해사고 위험성이 높으므로 사용하지 않는 경우 중지함.				
	*NFS(Network File System):원격 컴퓨터의 파일시스템을 로컬 시스템에 마운트하여 마치 로컬 파일시스템처럼 사용할 수 있는 프로그램임.				
보안대책					
판단기준	양호: NFS 서비스 관련 데몬이 비활성화 되어 있는 경우				
	취약: NFS 서비스 관련 데몬이 활성화 되어 있는 경우				
조치방법	사용하지 않는다면 NFS 서비스 중지 아래의 방법으로 NFS 서비스를 제거한 후 시스템 부팅 시, 스크립트 실행 방지 가능 1. /etc/dfs/dfstab의 모든 공유 제거 2. NFS 데몬(nfsd, statd, mountd) 중지 3. 시동 스크립트 삭제 또는, 스크립트 이름 변경				
보안설정방법					
OS별 점검 파일 위치 및 점검 방법					
LINUX, AIX, HP-UX, SunOS 5.9 이하 버전	NFS 서비스 데몬 확인 (NFS 동작 SID 확인) #ps -ef grep nfsd root 3809 3721 0 08:44:40 ? 0:00 /usr/lib/nfs/nfsd				
SunOS 5.10 이상 버전	#inetadm egrep "nfs statd lockd"				
불필요한 "NTFS" 서비스가 활성화된 경우 아래의 보안설정방법에 따라 서비스 데몬 중지					
■ LINUX, AIX, HP-UX, SunOS 5.9 이하 버전					
NFS 서비스 데몬 중지 #kill -9 [PID]					
■ SunOS 5.10 이상 버전 설정 방법					
1. NFS 서비스 데몬 확인					
svc:/network/nfs/server:default					
2. inetadm -d "중지하고자 하는 데몬" 명령으로 서비스 데몬 중지 #inetadm -d svc:/network/nfs/server:default					
조치 시 영향	showmount, share, exportfs 등의 명령어를 사용하여 로컬 서버에 마운트 되어 있는 디렉터리 확인 및 NFS 설정파일에 공유디렉터리 설정 여부 확인 후 해당 디렉터리가 존재하지 않을 경우 서비스 중지 가능				

UNIX 서버

취약점 항목		3.7. NFS 접근통제			
대상 OS	SunOS, LINUX, AIX, HP-UX	위험도	상	Code	U-42
취약점 개요	*NFS(Network File System) 사용 시 허가된 사용자만 접속할 수 있도록 접근제한 설정을 하여야 함. 접근제한 설정이 적절하게 이루어지지 않을 경우 비인가자의 root 권한 획득이 가능하며, 해당 공유 시스템에 원격으로 마운트하여 중요 파일을 변조하거나 유출할 위험이 있음.				
	*NFS(Network File System): 원격 컴퓨터의 파일시스템을 로컬 시스템에 마운트하여 마치 로컬 파일시스템처럼 사용할 수 있는 프로그램임.				
보안대책					
판단기준	양호: NFS 서비스를 사용하지 않거나, 사용 시 everyone 공유를 제한한 경우				
	취약: NFS 서비스를 사용하고 있고, everyone 공유를 제한하지 않은 경우				
조치방법	사용하지 않는다면 NFS 서비스 중지, 사용할 경우 NFS 설정파일에 everyone 공유 설정 제거				
보안설정방법					
< 서비스 필요 시 >					
불가피하게 NFS 서비스를 사용하여야 하는 경우 NFS 접근제어 파일에 꼭 필요한 공유 디렉터리만 나열하고, everyone으로 시스템이 마운트 되지 않도록 설정					
OS 종류별 NFS 접근제어 파일					
SunOS, HP-UX의 경우		"/etc/dfs/dfstab, /etc/dfs/sharetab 파일			
LINUX, AIX, HP-UX의 경우		"/etc/exports" 파일			
■ /etc/dfs/dfstab 설정 예문					
rw=client, ro=client 형식으로 접속 허용 client 지정					
• 사용자의 읽기, 쓰기 권한 접속 허용: share -F nfs -o rw, ro /export/home/test					
• 사용자의 권한 접속 제한: share -F nfs -o rw=client1:client2, ro=client1:client2 /export/home/test					
※ 읽기(ro), 쓰기(rw) 권한에 각각 사용자를 설정하여야 읽기, 쓰기 권한 모두 제한 가능					
■ /etc/exports 설정 예문					
1. everyone으로 시스템 마운트 금지					
#showmount -e hostname 명령어로 확인					
2. /etc/exports 파일에 접근 가능한 호스트명 추가					
(예) /stand host1 host2					
3. NFS 서비스 재구동					
#/etc/exportfs -u					
#/etc/exportfs -a					

UNIX 서버

< 서비스 불필요 시 >

OS별 점검 파일 위치 및 점검 방법	
LINUX, AIX, HP-UX, SunOS 5.9 이하 버전	NFS 서비스 데몬 확인 (NFS 동작 SID 확인) #ps -ef grep nfsd <i>root 3809 3721 0 08:44:40 ? 0:00 /usr/lib/nfs/nfsd</i>
SunOS 5.10 이상 버전	#inetadm egrep "nfs statd lockd"

불필요한 "NFS" 서비스가 활성화된 경우 아래의 보안설정방법에 따라 서비스 데몬 중지

■ LINUX, AIX, HP-UX, SunOS 5.9 이하 버전

NFS 서비스 데몬 중지

#kill -9 [PID]

■ SunOS 5.10 이상 버전

1. NFS 서비스 데몬 확인

```
svc:/network/nfs/server:default
```

2. inetadm -d "중지하고자 하는 데몬" 명령으로 서비스 데몬 중지

```
#inetadm -d svc:/network/nfs/server:default
```

조치 시 영향

showmount, share, exportfs 등의 명령어를 사용하여 로컬 서버에 마운트 되어 있는 디렉터리 확인 및 NFS 설정파일에 공유디렉터리 설정 여부 확인 후 해당 디렉터리가 존재하지 않을 경우 서비스 중지 가능

UNIX 서버

취약점 항목	3.8. automountd 제거										
대상 OS	SunOS, LINUX, AIX, HP-UX	위험도	상	Code	U-43						
취약점 개요	*automountd 데몬에는 로컬 공격자가 데몬에 *RPC(Remote Procedure Call)를 보낼 수 있는 취약점이 존재하여 이를 통해 파일 시스템의 마운트 옵션을 변경하여 root 권한을 획득할 수 있으며, 로컬 공격자가 automountd 프로세스 권한으로 임의의 명령을 실행할 수 있음.										
	*automountd: 클라이언트에서 자동으로 서버에 마운트를 시키고 일정 시간 사용하지 않으면 unmount 시켜 주는 기능을 말함.										
	*RPC(Remote Procedure Call): 분산 환경에서 서버 응용프로그램에 접근하여 특정 작업을 요구하는 Call을 말함.										
보안대책											
판단기준	양호: automountd 서비스가 비활성화 되어 있는 경우										
	취약: automountd 서비스가 활성화 되어 있는 경우										
조치방법	automountd 서비스 비활성화										
보안설정방법											
<table><tr><th colspan="2">OS별 점검 파일 위치 및 점검 방법</th></tr><tr><td>LINUX, AIX, HP-UX, SunOS 5.9 이하 버전</td><td>automountd 서비스 데몬 확인 (automountd 동작 SID 확인) #ps -ef grep automount root 1131 1 0 Jun 15 ? 32:11 /usr/sbin/automountd</td></tr><tr><td>SunOS 5.10 이상 버전</td><td>automountd 서비스 데몬 확인 #svcs -a egrep "autofs"</td></tr></table>						OS별 점검 파일 위치 및 점검 방법		LINUX, AIX, HP-UX, SunOS 5.9 이하 버전	automountd 서비스 데몬 확인 (automountd 동작 SID 확인) #ps -ef grep automount root 1131 1 0 Jun 15 ? 32:11 /usr/sbin/automountd	SunOS 5.10 이상 버전	automountd 서비스 데몬 확인 #svcs -a egrep "autofs"
OS별 점검 파일 위치 및 점검 방법											
LINUX, AIX, HP-UX, SunOS 5.9 이하 버전	automountd 서비스 데몬 확인 (automountd 동작 SID 확인) #ps -ef grep automount root 1131 1 0 Jun 15 ? 32:11 /usr/sbin/automountd										
SunOS 5.10 이상 버전	automountd 서비스 데몬 확인 #svcs -a egrep "autofs"										
"automountd" 서비스가 활성화된 경우 아래의 보안설정방법에 따라 서비스 데몬 중지											
■ LINUX, AIX, HP-UX, SunOS 5.9 이하 버전 automountd 서비스 데몬 중지 #kill -9 [PID]											
■ SunOS 5.10 이상 버전 1. autofs 서비스 데몬 확인 svc:/system/filesystem/autofs:default 2. svcadm disable "중지하고자 하는 데몬" 명령으로 서비스 데몬 중지 #svcadm disable svc:/system/filesystem/autofs:default											
조치 시 영향	NFS 및 *삼바(Samba) 서비스에서 사용 시 automountd 사용 여부 확인이 필요하며, 적용 시 CDROM의 자동 마운트는 이뤄지지 않음 (/etc/auto.*, /etc/auto_* 파일을 확인하여 필요 여부 확인)										
	*삼바(Samba): 서로 다른 운영체제(OS) 간의 자원 공유를 위해 이용하는 서버로 같은 네트워크 내 연결된 PC는 서로 운영체제가 달라도 네트워크로 파일을 주고받을 수 있고 자원을 공유할 수 있음										

UNIX 서버

취약점 항목	3.9. RPC 서비스 확인												
대상 OS	SunOS, LINUX, AIX, HP-UX	위험도	상	Code	U-44								
취약점 개요	*RPC (Remote Procedure Call) 서비스는 분산처리 환경에서 개발을 하는 데 있어 많은 이점을 제공하지만, 아래와 같은 서비스들은 버퍼 오버플로우(Buffer Overflow) 취약성이 다수 존재하여 root 권한 획득 및 침해사고 발생 위험이 있으므로 서비스를 중지하여야 함. rpc.cmsd, rpc.ttdbserverd, sadmind, rusersd, walld, sprayd, rstatd, rpc.nisd, rexd, rpc.pcnfsd, rpc.statd, rpc.yppupdated, rpc.rquotad, kcms_server, cachesfd *RPC(Remote Procedure Call): 분산 환경에서 서버 응용프로그램에 접근하여 특정 작업을 요구하는 Call을 말함.												
	보안대책												
판단기준	양호: 불필요한 RPC 서비스가 비활성화 되어 있는 경우 취약: 불필요한 RPC 서비스가 활성화 되어 있는 경우												
조치방법	일반적으로 사용하지 않는 RPC 서비스들을 inetd.conf 파일에서 주석 처리한 후 inetd 재구동 (진단 보고서에 발견된 RPC 서비스 조치)												
보안설정방법													
<table><tr><th colspan="2">OS별 점검 파일 위치 및 점검 방법</th></tr><tr><td>LINUX, AIX, HP-UX, SunOS 5.9 이하 버전</td><td>불필요한 RPC 서비스 비활성화 여부 확인 #cat /etc/inetd.conf</td></tr><tr><td>LINUX (xinetd)</td><td>"/etc/xinetd.d" 디렉터리 내 서비스별 파일 비활성화 여부 확인 #vi /etc/xinetd.d/[서비스별 파일명]</td></tr><tr><td>SunOS 5.10 이상 버전</td><td>RPC 서비스 관련 데몬 확인 #inetadm grep rpc grep enabled egrep "ttldbserver rex rstat rusers spray wall rquota"</td></tr></table>						OS별 점검 파일 위치 및 점검 방법		LINUX, AIX, HP-UX, SunOS 5.9 이하 버전	불필요한 RPC 서비스 비활성화 여부 확인 #cat /etc/inetd.conf	LINUX (xinetd)	"/etc/xinetd.d" 디렉터리 내 서비스별 파일 비활성화 여부 확인 #vi /etc/xinetd.d/[서비스별 파일명]	SunOS 5.10 이상 버전	RPC 서비스 관련 데몬 확인 #inetadm grep rpc grep enabled egrep "ttldbserver rex rstat rusers spray wall rquota"
OS별 점검 파일 위치 및 점검 방법													
LINUX, AIX, HP-UX, SunOS 5.9 이하 버전	불필요한 RPC 서비스 비활성화 여부 확인 #cat /etc/inetd.conf												
LINUX (xinetd)	"/etc/xinetd.d" 디렉터리 내 서비스별 파일 비활성화 여부 확인 #vi /etc/xinetd.d/[서비스별 파일명]												
SunOS 5.10 이상 버전	RPC 서비스 관련 데몬 확인 #inetadm grep rpc grep enabled egrep "ttldbserver rex rstat rusers spray wall rquota"												
불필요한 "RPC" 서비스가 활성화된 경우 아래의 보안설정방법에 따라 서비스 데몬 중지													
■ LINUX, AIX, HP-UX, SunOS 5.9 이하 버전													
1. "/etc/inetd.conf" 파일에서 해당 라인 #처리(주석처리) (수정 전) rpc.cmsd/2-4 dgram rpc/udp wait root /usr/dt/bin/rpc.cmsd rpc.cmsd (수정 후) #rpc.cmsd/2-4 dgram rpc/udp wait root /usr/dt/bin/rpc.cmsd rpc.cmsd													
2. inetd 서비스 재시작 #ps -ef grep inetd root 141 1 0 15:03:22 ? 0:01 /usr/sbin/inetd -s #kill -HUP 141													

UNIX 서버

■ LINUX (xinetd일 경우)

1. vi 편집기를 이용하여 "/etc/xinetd.d/" 디렉터리 내의 불필요한 RPC 서비스 파일을 연 후
2. 아래와 같이 설정 (Disable = yes 설정)

```
service finger
{
    disable                = yes
    socket_type            = stream
    wait                   = no
    - 이하 생략 -
}
```

3. xinetd 서비스 재시작

```
#service xinetd restart
```

■ SunOS 5.10 이상 버전

1. 불필요한 rpc 서비스 관련 데몬 확인

```
• svc:/network/rpc/cde-ttdbserver:tcp      • svc:/network/rpc/spray:default
• svc:/network/rpc/rex:default             • svc:/network/rpc/wall:default
• svc:/network/rpc/rstat:default           • svc:/network/fs/rquota:default
• svc:/network/rpc/rusers:default          - 이하 생략 -
```

2. svcadm disable "중지하고자 하는 데몬" 명령으로 서비스 데몬 중지

```
#inetadm -d svc:/network/rpc/rusers:default
```

UNIX 서버

불필요한 RPC 서비스	
rpc.cmsd	데이터베이스 관리 프로그램으로 Open Windows의 Calendar Manager와 CDE의 Calendar 프로그램에서 사용
rusersd	rusers 명령의 조회에 응답
rstatd	커널에서 얻은 성능 통계 리턴
rpc.ttdbserverd	시스템 장애 시 NFS에서 파일 복구를 위해 제공하는 lockd 프로그램 지원
kcms_server	kodak color management 관련된 api 와 라이브러리들은 데스크탑의 디지털 이미지들의 컬러 퍼포먼스를 컨트롤할 수 있는 Profile를 만들거나 관리하기 위해 사용
rpc.ttdbserverd	RPC 기반의 ToolTalk 데이터베이스 서버 프로그램
Walld	다른 사용자들에게 메시지 발송
rpc.nids	NIS+ server Daemon
rpc.yppupdated	Network Information Services(NIS) 맵 정보 갱신
cachefs	Cache 파일 시스템 데몬
sadmind	remote로부터의 시스템 관리
sprayd	지정된 수의 패킷을 호스트에 전송하고 성능 통계를 보고하는 spray 명령에 의해 전송된 패킷 수신
rpc.pcnfsd	PC-NFS (개인용 컴퓨터 네트워크 파일 시스템) 클라이언트에서의 서비스 요청 처리
rex	원격 시스템용 프로그램 실행
rpc.rquotad	리모트 머신에 NFS mount 되고 있는 파일 시스템에 대해 사용자에게 대한 로컬 머신에서의 할당 제한치를 반환
조치 시 영향	일반적인 경우 영향 없음

UNIX 서버

취약점 항목	3.10. NIS, NIS+ 점검				
대상 OS	SunOS, LINUX, AIX, HP-UX	위험도	상	Code	U-45
취약점 개요	*NIS(Network Information Service)는 중요한 시스템 데이터베이스 파일들을 네트워크를 통하여 공유하며, NIS+는 보안 및 편의 기능들을 추가한 그 후의 버전임. 보안상 취약한 서비스인 NIS, NIS+를 사용하는 경우 root 권한 획득이 가능하므로 사용하지 않는 것이 가장 바람직하나 만약 NIS를 사용해야 하는 경우 사용자 정보보안에 많은 문제점을 내포하고 있는 NIS보다 NIS+를 사용하는 것을 권장함. *NIS(Network Information Service) 주 서버는 정보표를 소유하여 NIS 대응 파일들로 변환하고, 이 대응 파일들이 네트워크를 통해 제공됨으로써 모든 컴퓨터에 정보가 갱신되도록 함. 네트워크를 통한 공유로부터 관리자와 사용자들에게 일관성 있는 시스템 환경을 제공함.				
보안대책					
판단기준	양호: NIS 서비스가 비활성화 되어 있거나, 필요 시 NIS+를 사용하는 경우 취약: NIS 서비스가 활성화 되어 있는 경우				
조치방법	NIS 관련 서비스 비활성화				
보안설정방법					
OS별 점검 파일 위치 및 점검 방법					
LINUX, AIX, HP-UX, SunOS 5.9 이하 버전	NIS, NIS+ 서비스 구동 확인 <pre>#ps -ef egrep "ypserv ypbind ypxfrd rpc.yppasswdd rpc.yupdated" grep -v "grep" root 3809 3721 0 08:44:40 ? 0:00 /usr/lib/nis/ypserv</pre>				
SunOS 5.10 이상 버전	서비스 데몬 구동 여부 확인 <pre>#svcs -a grep nis</pre>				
불필요한 "NIS" 서비스가 활성화된 경우 아래의 보안설정방법에 따라 서비스 데몬 중지					
NIS 관련 서비스 데몬					
ypserv	master와 slave 서버에서 실행되며 클라이언트로부터의 ypbind 요청에 응답				
ypbind	모든 NIS 시스템에서 실행되며 클라이언트와 서버를 바인딩하고 초기화함				
rpc.yppasswdd	사용자들이 패스워드를 변경하기 위해 사용				
ypxfrd	NIS 마스터 서버에서만 실행되며 고속으로 NIS 맵 전송				
rpc.yupdated	NIS 마스터 서버에서만 실행되며 고속으로 암호화하여 NIS 맵 전송				

UNIX 서버

■ LINUX, AIX, HP-UX, SunOS 5.9 이하 버전

NFS 서비스 데몬 중지

```
#kill -9 [PID]
```

■ SunOS 5.10 이상 버전

1. NIS 관련 서비스 데몬 확인

online	16:44:06	svc:/network/nis/client:default
online	16:44:07	svc:/network/nis/passwd:default
online	16:44:07	svc:/network/nis/server:default
online	16:44:07	svc:/network/nis/update:default
online	16:44:07	svc:/network/nis/xfr:default

2. svcadm disable “중지하고자 하는 데몬” 명령으로 서비스 데몬 중지

```
#svcadm disable svc:/network/nis/server:default
#svcadm disable svc:/network/nis/client:default
#svcadm disable svc:/network/nis/passwd:default
#svcadm disable svc:/network/nis/update:default
#svcadm disable svc:/network/nis/xfr:default
```

조치 시 영향	일반적으로 영향 없음
---------	-------------

UNIX 서버

취약점 항목	3.11. tftp, talk 서비스 비활성화				
대상 OS	SunOS, LINUX, AIX, HP-UX	위험도	상	Code	U-46
취약점 개요	운영체제는 ftp, tftp, telnet, talk 등의 서비스를 포함하고 있으므로 시스템 운영에 필요하지 않는 불필요한 서비스를 제거하여 보안성을 높일 수 있고 해당 불필요한 서비스 취약점 발견으로 인한 피해를 최소화할 수 있음.				
보안대책					
판단기준	양호: tftp, talk, ntalk 서비스가 비활성화 되어 있는 경우				
	취약: tftp, talk, ntalk 서비스가 활성화 되어 있는 경우				
조치방법	시스템 운영에 불필요한 서비스(tftp, talk, ntalk) 비활성화				
보안설정방법					

OS별 점검 파일 위치 및 점검 방법	
LINUX, AIX, HP-UX, SunOS 5.9 이하 버전	불필요한 서비스 데몬 확인 #ps -ef egrep "tftp talk" <i>root 3809 3721 0 08:44:40 ? 0:00 /usr/sbin/in.tftpd</i>
LINUX (xinetd)	tftp, talk, ntalk 서비스 활성화 여부 확인 #vi /etc/xinetd.d/tftp #vi /etc/xinetd.d/talk #vi /etc/xinetd.d/ntalk
SunOS 5.10 이상 버전	서비스 데몬 확인 #inetadm egrep "tftp talk"

불필요한 "tftp, talk, ntalk" 서비스가 활성화된 경우 아래의 보안설정방법에 따라 서비스 데몬 중지

불필요한 서비스 데몬	
tftp(69)	파일 전송을 위한 프로토콜. tftp 프로토콜은 OS에서는 부팅 디스켓이 없는 워크스테이션이나 네트워크 인식 프린터를 위한 설정파일의 다운로드, 설치 프로세스의 시작을 위해 사용
talk(517)	사용자가 시스템에 원격으로 연결하여 다른 시스템에 로그인하고 있는 사용자와 대화 세션을 시작할 수 있음
ntalk(518)	서로 다른 시스템 간에 채팅을 가능하게 하는 서비스

■ LINUX, AIX, HP-UX, SunOS 5.9 이하 버전

불필요한 서비스 데몬 중지

```
#kill -9 [PID]
```


UNIX 서버

■ LINUX (xinetd일 경우)

1. vi 편집기를 이용하여 "/etc/xinetd.d/" 디렉터리 내 tftp, talk, ntalk 파일을 연 후
2. 아래와 같이 설정 (Disable = yes 설정)

```

• /etc/xinetd.d/tftp 파일
• /etc/xinetd.d/talk 파일
• /etc/xinetd.d/ntalk 파일

service tftp
{
    socket_type          = dgram
    protocol             = udp
    wait                = yes
    user                 = root
    server                = /usr/sbin/in.tftpd
    server_args           = -s /tftpboot
    disable               = yes
}

```

3. xinetd 서비스 재시작

```
#service xinetd restart
```

■ SunOS 5.10 이상 버전

1. 불필요한 서비스 데몬 확인

```

svc:/network/tftp:default
svc:/network/talk:default
svc:/network/ntalk:default

```

2. inetadm -d "중지하고자 하는 데몬" 명령으로 서비스 데몬 중지

```

#inetadm -d svc:/network/tftp:default
#inetadm -d svc:/network/talk:default
#inetadm -d svc:/network/ntalk:default

```

조치 시 영향	일반적으로 영향 없음
----------------	-------------

UNIX 서버

취약점 항목		3.12. Sendmail 버전 점검			
대상 OS	SunOS, LINUX, AIX, HP-UX	위험도	상	Code	U-47
취약점 개요	Sendmail은 널리 쓰이는 만큼 많은 취약점이 알려져 있어 공격에 목표가 되기 쉬우므로 서버에서 Sendmail을 사용하는 목적을 검토하여 사용할 필요가 없는 경우, 서비스를 제거하는 것이 바람직함. 만일 운영할 필요가 있다면 취약점이 없는 Sendmail 버전을 유지하고 취약점에 대한 패치가 발표되었을 시 빠른 시기에 이를 적용하도록 함. 그렇지 않을 경우 버퍼 오버플로우(Buffer Overflow)의 공격에 의한 시스템 권한 획득 및 주요 정보 유출 가능성이 있음.				
보안대책					
판단기준	양호: Sendmail 버전이 8.13.8 이상인 경우				
	취약: Sendmail 버전이 8.13.8 이상이 아닌 경우				
조치방법	Sendmail 서비스를 사용하지 않을 경우 서비스 중지, 재부팅 후 다시 시작하지 않도록 시작 스크립트 변경, 사용할 경우 패치 관리 정책을 수립하여 주기적으로 패치 적용 ※ Sendmail 서비스의 경우 8.13.8 이하 대부분의 버전에서 취약점이 보고되고 있기 때문에 O/S 관리자, 서비스 개발자가 패치 적용에 따른 서비스 영향 정도를 정확히 파악하고 주기적인 패치 적용 정책을 수립하여 적용함				
보안설정방법					
OS별 점검 파일 위치 및 점검 방법					
SunOS, LINUX, AIX, HP-UX		1. Sendmail 서비스 실행 여부 점검 #ps -ef grep sendmail 2. Sendmail 버전 점검 #telnet localhost 25			
"Sendmail" 서비스가 활성화된 경우 아래의 보안설정방법에 따라 서비스 중지 또는, 버전 업그레이드					
■ SunOS, LINUX, AIX, HP-UX Sendmail 서비스 실행 여부 및 버전 점검 후, http://www.sendmail.org/ 또는, 각 OS 벤더사의 보안 패치 설치					
조치 시 영향	패치를 적용할 경우 시스템 및 서비스의 영향 정도를 충분히 고려하여야 함				

UNIX 서버

취약점 항목		3.13. 스팸 메일 릴레이 제한			
대상 OS	SunOS, LINUX, AIX, HP-UX	위험도	상	Code	U-48
취약점 개요	*SMTP(Simple Mail Transfer Protocol) 서버의 릴레이 기능을 제한하지 않을 경우 스팸 메일 서버로 악용되거나, 서버의 부하가 증가할 수 있음. 따라서 인증된 사용자에게 메일을 보낼 수 있도록 설정하거나 불필요 시 SMTP 서비스를 중지하여야 함.				
	*SMTP(Simple Mail Transfer Protocol) 서버: 인터넷상에서 전자우편(E-mail)을 전송할 때 이용하게 되는 표준 통신 규약을 SMTP라고 하며, SMTP에 의해 전자 메일을 발신하는 서버(server)를 SMTP 서버라고 함.				
보안대책					
판단기준	양호: SMTP 서비스를 사용하지 않거나 릴레이 제한이 설정되어 있는 경우				
	취약: SMTP 서비스를 사용하며 릴레이 제한이 설정되어 있지 않은 경우				
조치방법	Sendmail 서비스를 사용하지 않을 경우 서비스 중지 사용할 경우 릴레이 방지 설정 또는, 릴레이 대상 접근 제어				
보안설정방법					
OS별 점검 파일 위치 및 점검 방법					
SunOS, LINUX, HP-UX	SMTP 서비스 사용 여부 및 릴레이 제한 옵션 확인 #ps -ef grep sendmail grep -v "grep" #cat /etc/mail/sendmail.cf grep "R\$W*" grep "Relaying denied" R\$* \$error \$@ 5.7.1 \$: "550 Relaying denied"				
AIX	#ps -ef grep sendmail grep -v "grep" #cat /etc/sendmail.cf grep "R\$W*" grep "Relaying denied" R\$* \$error \$@ 5.7.1 \$: "550 Relaying denied"				
"SMTP" 서비스가 실행중이며, 위에 제시한 설정이 적용되지 않은 경우 아래의 보안설정방법에 따라 설정을 변경함					
OS 종류별 sendmail.cf 설정파일 위치					
AIX의 경우	"/etc/sendmail.cf" 파일				
SunOS, LINUX, HP-UX의 경우	"/etc/mail/sendmail.cf" 파일				
■ SunOS, LINUX, HP-UX					
1. vi 편집기를 이용하여 sendmail.cf 설정파일을 연 후					
2. 아래와 같이 주석 제거					
(수정 전) #R\$* \$error \$@ 5.7.1 \$: "550 Relaying denied"					
(수정 후) R\$* \$error \$@ 5.7.1 \$: "550 Relaying denied"					
3. 특정 IP, domain, Email Address 및 네트워크에 대한 sendmail 접근 제한 확인					
#cat /etc/mail/access					

UNIX 서버

■ AIX

1. vi 편집기를 이용하여 sendmail.cf 설정파일을 연 후
2. 아래와 같이 주석 제거
 (수정 전) #R\$* \$#error \$@ 5.7.1 \$: "550 Relaying denied"
 (수정 후) R\$* \$#error \$@ 5.7.1 \$: "550 Relaying denied"
3. 특정 IP, domain, Email Address 및 네트워크에 대한 sendmail 접근 제한 확인
 #cat /etc/sendmail.cf

조치 시 영향	릴레이를 허용할 대상에 대한 정보를 입력한다면 영향 없음
----------------	---------------------------------

UNIX 서버

취약점 항목		3.14. 일반사용자의 Sendmail 실행 방지			
대상 OS	SunOS, LINUX, AIX, HP-UX	위험도	상	Code	U-49
취약점 개요	SMTP 서비스 사용 시 일반 사용자의 q 옵션을 사용한 Sendmail 실행을 방지하여 메일류 내용과 sendmail 설정을 보거나, 메일류를 강제로 drop 시킬 수 있는 기능을 막아야 함. 그렇지 않을 경우 비인가자에 의한 SMTP 서비스 오류 발생이 가능함. *SMTP(Simple Mail Transfer Protocol): 인터넷상에서 전자우편(E-mail)을 전송할 때 이용하게 되는 표준 통신 규약을 말함.				
보안대책					
판단기준	양호: SMTP 서비스 미사용 또는, 일반 사용자의 Sendmail 실행 방지가 설정된 경우 취약: SMTP 서비스 사용 및 일반 사용자의 Sendmail 실행 방지가 설정되어 있지 않은 경우				
조치방법	Sendmail 서비스를 사용하지 않을 경우 서비스 중지 Sendmail 서비스를 사용 시 sendmail.cf 설정파일에 restrictqrun 옵션 추가 설정				
보안설정방법					
OS별 점검 파일 위치 및 점검 방법					
SunOS, LINUX, HP-UX	SMTP 서비스 사용 여부 및 restrictqrun 옵션 확인 <pre>#ps -ef grep sendmail grep -v "grep"</pre> <pre>#grep -v '^ *#' /etc/mail/sendmail.cf grep PrivacyOptions</pre>				
AIX	<pre>#ps -ef grep sendmail grep -v "grep"</pre> <pre>#grep -v '^ *#' /etc/sendmail.cf grep PrivacyOptions</pre>				
"SMTP" 서비스가 실행중이며, 위에 제시한 설정이 적용되지 않은 경우 아래의 보안설정방법에 따라 설정을 변경함					
OS 종류별 sendmail.cf 설정파일 위치					
AIX의 경우	"/etc/sendmail.cf" 파일				
SunOS, LINUX, HP-UX의 경우	"/etc/mail/sendmail.cf" 파일				
■ SunOS, LINUX, AIX, HP-UX					
1. vi 편집기를 이용하여 sendmail.cf 설정파일을 연 후 2. O PrivacyOptions= 설정 부분에 restrictqrun 옵션 추가 (수정 전) O PrivacyOptions=authwarnings, novrfy, noexpn (수정 후) O PrivacyOptions=authwarnings, novrfy, noexpn, restrictqrun 3. Sendmail 서비스 재시작					
조치 시 영향	옵션 적용 시에는 일반적으로 영향 없음				

UNIX 서버

취약점 항목		3.15.DNS 보안 버전 패치							
대상 OS	SunOS, LINUX, AIX, HP-UX	위험도	상	Code	U-50				
취약점 개요	*BIND(Berkeley Internet Name Domain)는 BIND 9.5.0 버전이 나왔으며 이하 버전에서는 많은 취약점이 존재함. BIND 8.x는 BIND의 distribution을 Sendmail의 버전과 일치시키기 위해 사용하는 새로운 버전 번호로 BIND 4의 Production version에 비하여 안정성, 성능, 보안성 등이 향상되었으나, BIND 8.3.4 이하 버전에서는 서비스거부 공격, 버퍼 오버플로우(Buffer Overflow) 및 DNS 서버 원격 침입 등의 취약성이 존재함. *BIND(Berkeley Internet Name Domain): BIND는 BSD 기반의 유닉스 시스템을 위해 설계된 DNS로 서버와 resolver 라이브러리로 구성되어 있음. 네임서버는 클라이언트들이 이름 자원들이나 객체들에 접근하여, 네트워크 내의 다른 객체들과 함께 정보를 공유할 수 있게 해주는 네트워크 서비스로 사실상 컴퓨터 네트워크 내의 객체들을 위한 분산 데이터베이스 시스템임.								
	보안대책								
판단기준	양호: DNS 서비스를 사용하지 않거나 주기적으로 패치를 관리하고 있는 경우 취약: DNS 서비스를 사용하며 주기적으로 패치를 관리하고 있지 않는 경우 [취약점이 존재하지 않는 버전] 8.4.6, 8.4.7, 9.2.8-P1, 9.3.4-P1, 9.4.1-P1, 9.5.0a6								
	DNS 서비스를 사용하지 않을 경우 서비스 중지, 사용할 경우 패치 관리 정책을 수립하여 주기적으로 패치 적용 ※ DNS 서비스의 경우 대부분의 버전에서 취약점이 보고되고 있기 때문에 O/S 관리자, 서비스 개발자가 패치 적용에 따른 서비스 영향 정도를 정확히 파악하여 주기적인 패치 적용 정책 수립 후 적용								
보안설정방법									
<table><tr><th colspan="2">OS별 점검 파일 위치 및 점검 방법</th></tr><tr><td>SunOS, LINUX, AIX, HP-UX</td><td>DNS 서비스 사용 및 BIND 버전 확인 #ps -ef grep named named -v</td></tr></table>						OS별 점검 파일 위치 및 점검 방법		SunOS, LINUX, AIX, HP-UX	DNS 서비스 사용 및 BIND 버전 확인 #ps -ef grep named named -v
OS별 점검 파일 위치 및 점검 방법									
SunOS, LINUX, AIX, HP-UX	DNS 서비스 사용 및 BIND 버전 확인 #ps -ef grep named named -v								
"DNS" 서비스를 사용하지 않는 경우 서비스 중지									
"DNS" 서비스 사용 시 BIND 버전 확인 후 아래의 보안설정방법에 따라 최신 버전으로 업데이트									
■ SunOS, LINUX, AIX, HP-UX									
1. BIND는 거의 모든 버전이 취약한 상태로서 최신 버전으로 업데이트가 요구됨									
2. 다음은 구체적인 BIND 취약점들이며, 취약점 관련 버전을 사용하는 시스템에서는 버전 업그레이드를 하여야 함									
• Inverse Query 취약점 (Buffer Overflow) : BIND 4.9.7이전 버전과 BIND 8.1.2 이전 버전									
• NXT버그 (buffer overflow) : BIND 8.2, 8.2 p1, 8.2.1버전									
• solinger버그 (Denial of Service) : BIND 8.1 이상버전									

UNIX 서버

- fdmax 버그 (Denial of Service) : BIND 8.1 이상버전
- Remote Execution of Code(Buffer Overflow):
BIND 4.9.5 to 4.9.10, 8.1, 8.2 to 8.2.6, 8.3.0 to 8.3.3 버전
- Multiple Denial of Service: BIND 8.3.0 - 8.3.3, 8.2 - 8.2.6 버전
- LIBRESOLV: buffer overrun(Buffer Overflow) : BIND 4.9.2 to 4.9.10 버전
- OpenSSL (buffer overflow) : BIND 9.1, BIND 9.2 if built with OpenSSL
(configure --with-openssl)
- libbind (buffer overflow) : BIND 4.9.11, 8.2.7, 8.3.4, 9.2.2 이외의 모든 버전
- DoS internal consistency check (Denial of Service) : BIND 9 ~ 9.2.0 버전
- tsig bug (Access possible) : BIND 8.2 ~ 8.2.3 버전
- complain bug (Stack corruption, possible remote access) : BIND 4.9.x 거의 모든 버전
- zxfr bug (Denial of service) : BIND 8.2.2, 8.2.2 patchlevels 1 through 6 버전
- sigdiv0 bug (Denial of service) : BIND 8.2, 8.2 patchlevel 1, 8.2.2 버전
- srv bug(Denial of service): BIND 8.2, 8.2 patchlevel 1, 8.2.1, 8.2.2, 8.2.2 patchlevels 1-6 버전
- nxd bug (Access possible) : BIND 8.2, 8.2 patchlevel 1, 8.2.1 버전
- BIND 4.9.8 이전 버전, 8.2.3 이전 버전과 관련된 취약점
 - TSIG 핸들링 버퍼오버플로우 취약점
 - nslookupComplain() 버퍼오버플로우 취약점
 - nslookupComplain() input validation 취약점
 - information leak 취약점
 - sig bug Denial of service 취약점
 - naptr bug Denial of service 취약점
 - maxdname bug Denial of service 취약점

※ BIND Vulnerability matrix : <http://www.isc.org/sw/bind/bind-security.php#matrix>

조치 시 영향	패치를 적용 시 시스템 및 서비스 영향 정도를 충분히 고려하여야 함
----------------	---------------------------------------

UNIX 서버

취약점 항목		3.16. DNS Zone Transfer 설정							
대상 OS	SunOS, LINUX, AIX, HP-UX	위험도	상	Code	U-51				
취약점 개요	DNS Zone Transfer는 Primary Name Server와 Secondary Name Server 간에 Zone 정보를 일관성 있게 유지하기 위하여 사용하는 기능으로 Secondary Name Server로만 Zone 정보를 전송하도록 제한하여야 함. 만약 허가되지 않는 사용자에게 Zone Transfer를 허용할 경우 공격자는 전송받은 Zone 정보를 이용하여 호스트 정보, 시스템 정보, 네트워크 구성 형태 등의 많은 정보를 파악할 수 있음.								
보안대책									
판단기준	양호: DNS 서비스 미사용 또는, Zone Transfer를 허가된 사용자에게만 허용한 경우								
	취약: DNS 서비스를 사용하며 Zone Transfer를 모든 사용자에게 허용한 경우								
조치방법	DNS 서비스를 사용하지 않을 경우 서비스 중지, 사용한다면 DNS설정을 통해 내부 Zone 파일을 임의의 외부 서버에서 전송 받지 못하게 하고, 아무나 쿼리 응답을 받을 수 없도록 수정								
보안설정방법									
< DNS 서비스를 사용할 경우 > <table><tr><th colspan="2">OS별 점검 파일 위치 및 점검 방법</th></tr><tr><td>SunOS, LINUX, AIX, HP-UX</td><td>DNS 서비스 사용 시 /etc/named.conf 파일의 allow-transfer 및 xfrnets 확인 #ps -ef grep named grep -v "grep" #cat /etc/named.conf grep 'allow-transfer' #cat /etc/named.boot grep "xfrnets"</td></tr></table> “DNS” 서비스 사용 시 위에 제시된 파일의 DNS 설정을 아래의 보안설정방법에 따라 수정함 ■ BIND8 DNS 설정(named.conf) 수정 예 <pre>options { allow-transfer {존 파일 전송을 허용하고자 하는 IP}; };</pre> ■ BIND4.9 DNS 설정(named.boot) 수정 예 <pre>options xfrnets 허용하고자 하는 IP</pre> < DNS 서비스를 사용하지 않는 경우 >						OS별 점검 파일 위치 및 점검 방법		SunOS, LINUX, AIX, HP-UX	DNS 서비스 사용 시 /etc/named.conf 파일의 allow-transfer 및 xfrnets 확인 #ps -ef grep named grep -v "grep" #cat /etc/named.conf grep 'allow-transfer' #cat /etc/named.boot grep "xfrnets"
OS별 점검 파일 위치 및 점검 방법									
SunOS, LINUX, AIX, HP-UX	DNS 서비스 사용 시 /etc/named.conf 파일의 allow-transfer 및 xfrnets 확인 #ps -ef grep named grep -v "grep" #cat /etc/named.conf grep 'allow-transfer' #cat /etc/named.boot grep "xfrnets"								

UNIX 서버

OS별 점검 파일 위치 및 점검 방법

LINUX, AIX, HP-UX, SunOS 5.9 이하 버전	DNS 서비스 데몬 확인 (DNS 동작 SID 확인) #ps -ef grep named <i>root 3809 3721 0 08:44:40 ? 0:00 /usr/sbin/in.named</i>
SunOS 5.10 이상 버전	#svcs -a egrep "dns"

"DNS" 서비스를 사용하지 않는 경우 서비스 데몬 중지

■ LINUX, AIX, HP-UX, SunOS 5.9 이하 버전

DNS 서비스 데몬 중지

#kill -9 [PID]

■ SunOS 5.10 이상 버전

1. DNS 서비스 데몬 확인

```
enabled      16:22:31 svc:/network/dns/server:default
```

2. svcadm disable "중지하고자 하는 데몬" 명령으로 서비스 데몬 중지

```
#svcadm disable svc:/network/dns/server:default
```

조치 시 영향	Zone 파일 전송을 허용할 대상을 정상적으로 등록할 경우 일반적으로 영향 없음
----------------	--

UNIX 서버

취약점 항목		3.17. Apache 디렉터리 리스팅 제거			
대상 OS	SunOS, LINUX, AIX, HP-UX	위험도	상	Code	U-52
취약점 개요	디렉터리 검색은 디렉터리 요청 시 해당 디렉터리에 기본 문서가 존재하지 않을 경우 디렉터리 내 모든 파일의 목록을 보여주는 기능임. 디렉터리 검색 기능이 활성화되어 있는 경우 외부에서 디렉터리 내의 모든 파일에 대한 접근이 가능하여 WEB 서버 구조 노출뿐만 아니라 백업 파일이나 소스파일 등 공개되어서는 안 되는 중요 파일 노출이 가능함.				
보안대책					
판단기준	양호: 디렉터리 검색 기능을 사용하지 않는 경우				
	취약: 디렉터리 검색 기능을 사용하는 경우				
조치방법	디렉터리 검색 기능 제거 (/[Apache_home]/conf/httpd.conf 파일에 설정된 모든 디렉터리의 Options 지시자에서 Indexes 옵션 제거)				
보안설정방법					
OS별 점검 파일 위치 및 점검 방법					
SunOS, LINUX, AIX, HP-UX	Indexes 옵션 사용 여부 확인 #vi /[Apache_home]/conf/httpd.conf Options Indexes FollowSymLinks				
위에 제시한 파일에 "Indexes" 옵션이 설정된 경우 아래의 보안설정방법에 따라 옵션 설정 변경					
■ SunOS, LINUX, AIX, HP-UX					
1. vi 편집기를 이용하여 /[Apache_home]/conf/httpd.conf 파일을 연 후 #vi /[Apache_home]/conf/httpd.conf					
2. 설정된 모든 디렉터리의 Options 지시자에서 Indexes 옵션 제거 (수정 전) Option 지시자에 Indexes 옵션이 설정되어 있음					
<Directory /> Options Indexes FollowSymLinks AllowOverride None Order allow, deny Allow from all </Directory>					

UNIX 서버

(수정 후) Option 지시자에 Indexes 옵션 제거 후 저장

```
<Directory />
    Options FollowSymLinks
    AllowOverride None
    Order allow, deny
    Allow from all

</Directory>
```

조치 시 영향	일반적인 경우 영향 없음
----------------	---------------

UNIX 서버

취약점 항목		3.18. Apache 웹 프로세스 권한 제한			
대상 OS	SunOS, LINUX, AIX, HP-UX	위험도	상	Code	U-53
취약점 개요	UNIX 시스템의 경우 Web 서버 데몬이 root 권한으로 운영될 경우 Web Application의 취약점 또는, 버퍼 오버플로우(Buffer Overflow)로 인하여 root 권한을 획득할 수 있으므로 서버 데몬이 root 권한으로 운영되지 않도록 관리하여야 함.				
보안대책					
판단기준	양호: Apache 데몬이 root 권한으로 구동되지 않는 경우				
	취약: Apache 데몬이 root 권한으로 구동되는 경우				
조치방법	Apache 데몬을 root 가 아닌 별도 계정으로 구동				
보안설정방법					
OS별 점검 파일 위치 및 점검 방법					
SunOS, LINUX, AIX, HP-UX	Apache 데몬 구동 권한(User 및 Group) 확인 #vi /[Apache_home]/conf/httpd.conf User [root가 아닌 별도 계정명] Group [root가 아닌 별도 계정명]				
위에 제시한 설정이 적용되지 않은 경우 아래의 보안설정방법에 따라 설정을 변경함					
■ SunOS, LINUX, AIX, HP-UX					
1. 데몬 User & Group 변경					
User & Group 부분에 root가 아닌 별도 계정으로 변경					
User [root가 아닌 별도 계정명] Group [root가 아닌 별도 계정명]					
3. Apache 서비스 재시작					
조치 시 영향	일반적인 경우 영향 없음				

UNIX 서버

취약점 항목		3.19. Apache 상위 디렉터리 접근 금지			
대상 OS	SunOS, LINUX, AIX, HP-UX	위험도	상	Code	U-54
취약점 개요	상위경로로 이동하는 것이 가능할 경우 하위경로에 접속하여 상위경로로 이동함으로써 해킹을 당할 위험이 있으며, 유니코드 버그(Unicode Bug) 및 서비스 거부 공격에 취약해지기 쉬우므로 "." 와 같은 상위경로로 이동이 가능한 문자사용이 불가능하도록 설정할 것을 권장함. Apache는 특정 디렉터리 내에 존재하는 파일들을 호출할 때 사용자 인증을 수행하도록 설정할 수 있음. 따라서 해당 설정을 이용하여 중요 파일 및 데이터 접근은 허가된 사용자만 가능하도록 제한함.				
보안대책					
판단기준	양호: 상위 디렉터리에 이동제한을 설정한 경우 취약: 상위 디렉터리에 이동제한을 설정하지 않은 경우				
조치방법	1. 사용자 인증을 하기 위해서 각 디렉터리 별로 httpd.conf 파일 내 AllowOverride 지시자의 옵션 설정을 변경 (None에서 AuthConfig 또는, All로 변경) 2. 사용자 인증을 설정할 디렉터리에 .htaccess 파일 생성 3. 사용자 인증 계정 생성: htpasswd -c <인증 파일> <사용자 계정>				
보안설정방법					
OS별 점검 파일 위치 및 점검 방법					
SunOS, LINUX, AIX, HP-UX	AllowOverride 지시자 Authconfig 옵션 확인 #vi /[Apache_home]/conf/httpd.conf AllowOverride None				
"AllowOverride" 옵션이 "None"으로 설정된 경우 아래의 보안설정방법에 따라 옵션 설정 변경					
■ SunOS, LINUX, AIX, HP-UX					
1. vi 편집기를 이용하여 /[Apache_home]/conf/httpd.conf 파일을 연 후 #vi /[Apache_home]/conf/httpd.conf					
2. 설정된 모든 디렉터리의 AllowOverride 지시자에서 AuthConfig 옵션 설정 (수정 전) AllowOverride 지시자에 None 옵션이 설정되어 있음					
<Directory "/usr/local/apache2/htdocs"> AllowOverride None Allow from all </Directory>					
(수정 후) AllowOverride 지시자에 AuthConfig 옵션이 설정되어 있음					

UNIX 서버

```
<Directory "/usr/local/apache2/htdocs">
```

```
    AllowOverride AuthConfig
```

```
    Allow from all
```

```
</Directory>
```

3. 사용자 인증을 설정할 디렉터리에 .htaccess 파일 생성 (아래 내용 삽입)

```
AuthName "디렉터리 사용자 인증"
```

```
AuthType Basic
```

```
AuthUserFile /usr/local/apache/test/.auth
```

```
Require valid-user
```

지시자	설명
AuthName	인증 영역 (웹 브라우저의 인증 창에 표시되는 문구)
AuthType	인증 형태 (Basic 또는, Digest)
AuthUserFile	사용자 정보(아이디 및 패스워드) 저장 파일 위치
AuthGroupFile	그룹 파일의 위치 (옵션)
Require	접근을 허용할 사용자 또는, 그룹 정의

4. 사용자 인증에 사용할 아이디 및 패스워드 생성

```
#htpasswd -c /usr/local/apache/test/.auth test
```

```
New password:
```

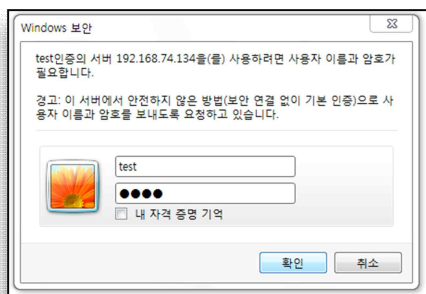
```
Re-type new password:
```

```
Adding password for user test
```

```
[root@localhost apache]#
```

5. 변경된 설정 내용을 적용하기 위하여 Apache 데몬 재시작

6. 사용자 인증을 설정한 디렉터리 내 파일 호출 화면



조치 시 영향

해당 설정이 적용된 디렉터리 내 파일들은 아이디/패스워드 인증절차 없이는 접속이 불가능하며, 대외 서비스인 경우 해당 디렉터리에 대한 외부자의 접근 필요성을 검토 후 적용하여야 함

UNIX 서버

취약점 항목		3.20. Apache 불필요한 파일 제거			
대상 OS	SunOS, LINUX, AIX, HP-UX	위험도	상	Code	U-55
취약점 개요	웹 서버 설치 시 기본으로 생성되는 매뉴얼 파일은 외부 침입자에게 시스템 정보 및 웹 서버 정보를 제공할 수 있으므로 제거하여야 함.				
보안대책					
판단기준	양호: 매뉴얼 파일 및 디렉터리가 제거되어 있는 경우				
	취약: 매뉴얼 파일 및 디렉터리가 제거되지 않은 경우				
조치방법	매뉴얼 파일 및 디렉터리 제거 ("/[Apache_home]/htdocs/manual", "/[Apache_home]/manual" 파일 제거)				
보안설정방법					
OS별 점검 파일 위치 및 점검 방법					
SunOS, LINUX, AIX, HP-UX		매뉴얼 및 디렉터리 존재 여부 확인 #ls -ld /[Apache_home]/htdocs/manual #ls -ld /[Apache_home]/manual			
위에 제시한 매뉴얼 파일 및 디렉터리가 존재하는 경우 아래의 보안설정방법에 따라 매뉴얼 파일 및 디렉터리 제거 또는, 설정을 변경함					
■ SunOS, LINUX, AIX, HP-UX					
1. #ls 명령어로 확인된 매뉴얼 디렉터리 및 파일 제거 #rm -rf /[Apache_home]/htdocs/manual #rm -rf /[Apache_home]/manual					
2. #ls 명령어로 정상적인 제거 확인 #ls -ld /[Apache_home]/htdocs/manual #ls -ld /[Apache_home]/manual					
조치 시 영향	일반적인 경우 영향 없음				

UNIX 서버

취약점 항목		3.21. Apache 링크 사용금지			
대상 OS	SunOS, LINUX, AIX, HP-UX	위험도	상	Code	U-56
취약점 개요	일부 서버는 *심볼릭 링크(Symbolic link)를 이용하여 기존의 웹 문서 이외의 파일시스템 접근이 가능하도록 하고 있음. 이러한 방법은 편의성을 제공하는 반면, 일반 사용자들도 시스템 중요 파일에 접근할 수 있게 하는 보안 문제를 발생시킴. 가령 시스템 자체의 root 디렉터리(/)에 링크를 걸게 되면 웹 서버 구동 사용자 권한(nobody)으로 모든 파일 시스템의 파일에 접근할 수 있게 되어 "/etc/passwd" 파일과 같은 민감한 파일을 누구나 열람할 수 있게 됨.				
	*심볼릭 링크(Symbolic link, 소프트 링크): 윈도우 운영체제의 바로가기 아이콘과 비슷함. 링크 생성 시 파일 내용은 존재하지 않으나 사용자가 파일을 요청하면 링크가 가리키고 있는 원본 데이터에서 데이터를 가져와서 전달함. 직접 원본을 가리키지 않고 원본 데이터를 가리키는 포인터를 참조함으로써 원본데이터가 삭제, 이동, 수정이 되면 사용 불가함.				
보안대책					
판단기준	양호: 심볼릭 링크, aliases 사용을 제한한 경우				
	취약: 심볼릭 링크, aliases 사용을 제한하지 않은 경우				
조치방법	심볼릭 링크, aliases 사용 제한 (/[Apache_home]/conf/httpd.conf 파일에 설정된 모든 디렉터리의 Options 지시자에서 심볼릭 링크를 가능하게 하는 FollowSymLinks 옵션 제거)				
보안설정방법					
OS별 점검 파일 위치 및 점검 방법					
SunOS, LINUX, AIX, HP-UX	Options 지시자 FollowSymLinks 옵션 제거 여부 확인 #vi /[Apache_home]/conf/httpd.conf Options Indexes FollowSymLinks				

위에 제시한 옵션이 적용되어 있는 경우 아래의 보안설정방법에 따라 옵션을 제거함

■ SunOS, LINUX, AIX, HP-UX

1. vi 편집기를 이용하여 /[Apache_home]/conf/httpd.conf 파일을 연 후
#vi /[Apache_home]/conf/httpd.conf

2. 설정된 모든 디렉터리의 Options 지시자에서 FollowSymLinks 옵션 제거
(수정 전) Options 지시자에 FollowSymLinks 옵션이 설정되어 있음

<Directory />

Options Indexes FollowSymLinks
AllowOverride None
Order allow, deny
Allow from all

</Directory>

UNIX 서버

(수정 전) Options 지시자에 FollowSymLinks 옵션 제거 후 저장

```
<Directory />
    Options Indexes
    AllowOverride None
    Order allow, deny
    Allow from all
</Directory>
```

조치 시 영향	일반적인 경우 영향 없음
----------------	---------------

UNIX 서버

취약점 항목	3.22. Apache 파일 업로드 및 다운로드 제한				
대상 OS	SunOS, LINUX, AIX, HP-UX	위험도	상	Code	U-57
취약점 개요	불필요한 파일 업로드, 다운로드 시에 대량의 업로드, 다운로드에 의한 서비스 불능상태가 발생할 수 있음. 따라서 불필요한 업로드와 다운로드는 허용하지 않으며, 웹 서버에 의해 처리되지 못하게 하고, 자동이나 수동으로 파일의 보안성 검토를 수행함.				
보안대책					
판단기준	양호: 파일 업로드 및 다운로드를 제한한 경우				
	취약: 파일 업로드 및 다운로드를 제한하지 않은 경우				
조치방법	파일 업로드 및 다운로드 용량 제한 (/[Apache_home]/conf/httpd.conf 파일에 설정된 모든 디렉터리의 LimitRequestBody 지시자에 파일 사이즈 용량 제한 설정				
보안설정방법					
OS별 점검 파일 위치 및 점검 방법					
SunOS, LINUX, AIX, HP-UX	LimitRequestBody 파일 사이즈 용량 제한 설정 여부 확인 #vi /[Apache_home]/conf/httpd.conf LimitRequestBody 5000000 (※ 업로드 및 다운로드 파일이 5M를 넘지 않도록 설정 권고함)				
위에 제시한 설정이 적용되지 않은 경우 아래의 보안설정방법에 따라 설정을 변경함					
■ SunOS, LINUX, AIX, HP-UX					
1. vi 편집기를 이용하여 /[Apache_home]/conf/httpd.conf 파일을 연 후 #vi /[Apache_home]/conf/httpd.conf					
2. 설정된 모든 디렉터리의 LimitRequestBody 지시자에서 파일 사이즈 용량 제한 설정					
<Directory /> LimitRequestBody 5000000 (※ "/" 는 모든 파일 사이즈를 5M로 제한하는 설정) </Directory>					
조치 시 영향	일반적인 경우 영향 없음				

UNIX 서버

취약점 항목		3.23. Apache 웹 서비스 영역의 분리			
대상 OS	SunOS, LINUX, AIX, HP-UX	위험도	상	Code	U-58
취약점 개요	Apache 설치 시 htdocs 디렉터리를 DocumentRoot로 사용하고 있는데 htdocs 디렉터리는 공개되어서는 안 될(또는, 공개될 필요가 없는) Apache 문서뿐만 아니라 공격에 이용될 수 있는 시스템 관련 정보도 포함하고 있으므로 이를 변경하여야 함. 또한, 대량의 업로드와 다운로드 시 서비스 불능 상태가 발생할 수 있음.				
보안대책					
판단기준	양호: DocumentRoot를 별도의 디렉터리로 지정한 경우				
	취약: DocumentRoot를 기본 디렉터리로 지정한 경우				
조치방법	DocumentRoot "/usr/local/apache/htdocs"-> DocumentRoot "별도 디렉터리" 로 변경				
보안설정방법					
OS별 점검 파일 위치 및 점검 방법					
SunOS, LINUX, AIX, HP-UX	DocumentRoot의 별도 디렉터리 지정 여부 확인 #vi /[Apache_home]/conf/httpd.conf DocumentRoot "/usr/local/apache/htdocs"				
DocumentRoot가 "/usr/local/apache/htdocs"가 아닌 별도의 디렉터리로 지정되지 않은 경우 아래의 보안설정방법에 따라 설정을 변경함					
■ SunOS, LINUX, AIX, HP-UX					
1. vi 편집기를 이용하여 /[Apache_home]/conf/httpd.conf 파일을 연 후 #vi /[Apache_home]/conf/httpd.conf					
2. DocumentRoot 설정 부분에 "/usr/local/apache/htdocs"가 아닌 별도의 디렉터리로 변경					
DocumentRoot "디렉터리"					
조치 시 영향	일반적인 경우 영향 없음				

UNIX 서버

취약점 항목		3.24. ssh 원격접속 허용			
대상 OS	SunOS, LINUX, AIX, HP-UX	위험도	중	Code	U-59
취약점 개요	Telnet, FTP 등은 암호화되지 않은 상태로 데이터를 전송하기 때문에 ID/패스워드 및 중요 정보가 외부로 유출될 위험성이 있음. 따라서 원격 접속 시 사용자와 시스템과의 모든 통신을 암호화하는 *SSH(Secure Shell) 서비스를 사용할 것을 권장함.				
	*SSH(Secure Shell): 공개 키 암호 방식을 사용하여 원격지 시스템에 접근, 암호화된 메시지를 전송하는 시스템을 말함. 암호화된 메시지를 전송함으로써 LAN 상에서 다른 시스템에 로그인할 때 스니퍼에 의해서 도청당하는 것을 막을 수 있음.				
보안대책					
판단기준	양호: 원격 접속 시 SSH 프로토콜을 사용하는 경우				
	취약: 원격 접속 시 Telnet, FTP 등 안전하지 않은 프로토콜을 사용하는 경우				
조치방법	Telnet, FTP 등 안전하지 않은 서비스 사용을 중지하고, SSH 설치 및 사용				
보안설정방법					
OS별 점검 파일 위치 및 점검 방법					
SunOS	서비스 데몬 실행 여부 확인 # svcs -a grep ssh				
LINUX	서비스 데몬 실행 여부 확인 # ps -ax grep sshd				
서비스 데몬이 실행중인 경우 각 OS 벤더사로부터 SSH 서비스 설치 방법을 문의한 후 서버에 설치할 것을 권고함					
■ SunOS, LINUX, AIX, HP-UX					
1. 각 OS 벤더사로부터 SSH 서비스 설치 방법을 문의한 후 서버에 설치					
조치 시 영향	일반적인 경우 영향 없음				

UNIX 서버

취약점 항목		3.25. ftp 서비스 확인			
대상 OS	SunOS, LINUX, AIX, HP-UX	위험도	하	Code	U-60
취약점 개요	FTP 서비스는 아이디 및 패스워드가 암호화되지 않은 채로 전송되어 간단한 Sniffer에 의해서도 스니핑이 가능하므로 반드시 필요한 경우를 제외하고는 FTP 서비스 사용을 제한하여야 함.				
보안대책					
판단기준	양호: FTP 서비스가 비활성화 되어 있는 경우				
	취약: FTP 서비스가 활성화 되어 있는 경우				
조치방법	FTP 서비스 중지				
보안설정방법					
FTP 종류별 점검 방법					
SunOS, LINUX, AIX, HP-UX	일반 ftp 서비스 비활성화 여부 확인				
	# vi /etc/inetd.conf				
	proftpd 서비스 데몬 확인 (proftpd 동작 SID 확인)				
	# ps -ef grep proftpd				
	root 3809 3721 0 08:44:40 ? 0:00 /usr/local/proftpd/sbin/proftpd				
	vsftpd 서비스 데몬 확인 (vsftpd 동작 SID 확인)				
	# ps -ef grep vsftpd				
	root 3809 3721 0 08:44:40 ? 0:00 /usr/sbin/vsftpd/etc/vsftpd/vsftpd.conf				
불필요한 "ftp" 서비스 실행 시 아래의 보안설정방법에 따라 서비스 중지					
■ SunOS, LINUX, AIX, HP-UX					
< 일반 FTP 서비스 중지 방법 >					
1. "/etc/inetd.conf" 파일에서 ftp 서비스 라인 #처리(주석처리)					
(수정 전) ftp stream tcp nowait bin /usr/sbin/in.ftpd in.fingerd -a					
(수정 후) #ftp stream tcp nowait bin /usr/sbin/in.ftpd in.fingerd -a					
2. inetd 서비스 재시작					
#ps -ef grep inetd					
root 141 1 0 15:03:22 ? 0:01 /usr/sbin/inetd -s					
#kill -HUP [PID]					
< ProFTP 서비스 중지 방법 >					
proftpd 서비스 데몬 중지					
#kill -9 [PID]					
< vsFTP 서비스 중지 방법 >					
vsftpd 서비스 데몬 중지					
#kill -9 [PID]					
조치 시 영향	일반적인 경우 영향 없음				

UNIX 서버

취약점 항목		3.26. ftp 계정 shell 제한			
대상 OS	SunOS, LINUX, AIX, HP-UX	위험도	중	Code	U-61
취약점 개요	FTP 서비스 설치 시 기본으로 생성되는 ftp 계정은 로그인이 필요하지 않은 기본 계정으로 쉘을 제한하여 해당 계정으로의 시스템 접근을 차단하여야 함. 로그인이 불필요한 기본 계정에 *셸(Shell)을 부여할 경우 공격자에게 해당 계정이 노출되어 시스템 불법 침투가 발생할 수 있음.				
	*셸(Shell): 대화형 사용자 인터페이스로써, 운영체제(OS) 가장 외곽계층에 존재하여 사용자의 명령어를 이해하고 실행함.				
보안대책					
판단기준	양호: ftp 계정에 /bin/false 쉘이 부여되어 있는 경우				
	취약: ftp 계정에 /bin/false 쉘이 부여되지 않은 경우				
조치방법	ftp 계정에 /bin/false 쉘 부여				
보안설정방법					
OS별 점검 파일 위치 및 점검 방법					
SunOS, LINUX, AIX, HP-UX	ftp 계정에 대한 /bin/false 부여 확인 #cat /etc/passwd ftp:x:500:100:Anonymous FTP USER:/var/ftp:/sbin/bash				
"passwd" 파일 내 로그인 쉘 설정이 "/bin/false"가 아닌 경우 아래의 보안설정방법에 따라 설정을 변경함					
■ SunOS, LINUX, AIX, HP-UX					
1. vi 편집기를 이용하여 "/etc/passwd" 파일을 연 후					
2. ftp 계정의 로그인 쉘 부분인 계정 맨 마지막에 /bin/false 부여 및 변경					
(수정 전) ftp:x:500:100:Anonymous FTP USER:/var/ftp:/sbin/bash					
(수정 후) ftp:x:500:100:Anonymous FTP USER:/var/ftp:/bin/false					
조치 시 영향	일반적인 경우 영향 없음				

UNIX 서버

취약점 항목		3.27. Ftpusers 파일 소유자 및 권한 설정			
대상 OS	SunOS, LINUX, AIX, HP-UX	위험도	하	Code	U-62
취약점 개요	FTP 접근제어 설정파일을 관리자가 아닌 일반 사용자들도 접근 및 변경이 가능할 경우 비인가자 FTP 접근을 통해 계정을 등록하고 서버에 접속하여 불법적인 행동을 가능하게 하는 등 침해사고가 발생할 수 있음. FTP 접근제어 설정파일을 일반 사용자들이 수정할 수 없도록 제한하고 있는지 점검함.				
보안대책					
판단기준	양호: ftpusers 파일의 소유자가 root이고, 권한이 640 이하인 경우				
	취약: ftpusers 파일의 소유자가 root가 아니거나, 권한이 640 이하가 아닌 경우				
조치방법	FTP 접근제어 파일의 소유자 및 권한 변경 (소유자 root, 권한 640 이하)				
보안설정방법					
OS별 점검 파일 위치 및 점검 방법					
SunOS, LINUX, AIX, HP-UX	ftpusers 파일에 대한 일반사용자 쓰기권한 확인 #ls -al /etc/ftpusers #ls -al /etc/ftpd/ftpusers rw-r----- root <ftpusers 파일>				
“ftpusers” 파일의 소유자가 root가 아니거나 파일의 권한이 640 이하가 아닌 경우 아래의 보안설정방법에 따라 설정을 변경함					
FTP 종류 별 ftpusers 파일 위치					
기본 FTP	/etc/ftpusers 또는, /etc/ftpd/ftpusers				
ProFTP	/etc/ftpusers 또는, /etc/ftpd/ftpusers				
vsFTP	/etc/vsftpd/ftpusers, /etc/vsftpd/user_list 또는, /etc/vsftpd.ftpusers, /etc/vsftpd.user_list				
■ SunOS, LINUX, AIX, HP-UX					
1. “/etc/ftpusers” 파일의 소유자 및 권한 확인 #ls -l /etc/ftpusers					
2. “/etc/ftpusers” 파일의 소유자 및 권한 변경 (소유자 root, 권한 640) #chown root /etc/ftpusers #chmod 640 /etc/ftpusers					
※ vsFTP를 사용할 경우 FTP 접근제어 파일					
(1) vsftpd.conf 파일에서 userlist_enable=YES인 경우: vsftpd.ftpusers, vsftpd.userlist (ftpusers, user_list 파일에 등록된 모든 계정의 접속이 차단됨)					
(2) vsftpd.conf 파일에서 userlist_enable=NO 또는, 옵션 설정이 없는 경우: vsftpd.ftpusers (ftpusers 파일에 등록된 계정들만 접속이 차단됨)					
조치 시 영향	일반적인 경우 영향 없음				

UNIX 서버

취약점 항목		3.28. Ftpusers 파일 설정			
대상 OS	SunOS, LINUX, AIX, HP-UX	위험도	중	Code	U-63
취약점 개요	FTP 서비스는 아이디 및 패스워드가 암호화되지 않은 채로 전송되어 간단한 스니퍼에 의해서도 아이디 및 패스워드가 노출될 수 있으므로 반드시 필요한 경우를 제외하고는 FTP 서비스 사용을 제한하여야 함. 불가피하게 FTP 서비스를 사용하여야 하는 경우 root 계정의 직접 접속을 제한하여 root 계정의 패스워드 정보가 노출되지 않도록 함.				
보안대책					
판단기준	양호: FTP 서비스가 비활성화 되어 있거나, 활성화 시 root 계정 접속을 차단한 경우 취약: FTP 서비스가 활성화 되어 있고, root 계정 접속을 허용한 경우				
조치방법	FTP 접속 시 root 계정으로 직접 접속 할 수 없도록 설정파일 수정 (접속 차단 계정을 등록하는 ftpusers 파일에 root 계정 추가)				
보안설정방법					
FTP 종류별 점검 방법					
SunOS, LINUX, AIX, HP-UX	아래 파일에서 ftp에 대한 root 계정으로의 접속 가능 여부 확인 #cat /etc/ftpusers #cat /etc/ftpd/ftpusers #root (주석처리) 또는, root 계정 미등록				
	ProFTP #cat /etc/proftpd.con RootLogin on				
	vsFTP #cat /etc/vsftp/ftpusers #cat /etc/vsftpd.ftpusers #root (주석처리) 또는, root 계정 미등록				
root 계정으로 FTP 접속이 가능하도록 위와 같이 설정된 경우 아래의 보안설정방법에 따라 설정을 변경함					
■ SunOS, LINUX, AIX, HP-UX					
< 일반 FTP 서비스 root 계정 접속 제한 방법 >					
1. vi 편집기를 이용하여 ftpusers 파일을 연 후 ("/etc/ftpusers" 또는, "/etc/ftpd/ftpusers") #vi /etc/ftpusers 또는, /etc/ftpd/ftpusers					
2. ftpusers 파일에 root 계정 추가 또는, 주석제거 (수정 전) #root 또는, root 계정 미등록 (수정 후) root					
< ProFTP 서비스 중지 방법>					
1. vi 편집기를 이용하여 proftpd 설정파일("/etc/proftpd.conf")을 연 후 #vi /etc/proftpd.conf					

UNIX 서버

2. proftpd 설정파일 ("/etc/proftpd.conf")에서 RootLogin off 설정

(수정 전) RootLogin on

(수정 후) RootLogin off

< vsFTP 서비스 중지 방법 >

1. vi 편집기를 이용하여 ftpusers 파일을 연 후 ("/etc/vsftp/ftpusers" 또는, "/etc/vsftpd.ftpusers")

#vi /etc/vsftp/ftpusers

2. ftpusers 파일에 root 계정 추가 또는, 주석제거

(수정 전) #root 또는, root 계정 미등록

(수정 후) root

※ vsFTP를 사용할 경우 FTP 접근제어 파일

(1) vsftpd.conf 파일에서 userlist_enable=YES인 경우: vsftpd.ftpusers, vsftpd.userlist

(ftpusers, user_list 파일에 등록된 모든 계정의 접속이 차단됨)

(2) vsftpd.conf 파일에서 userlist_enable=NO 또는, 옵션 설정이 없는 경우: vsftpd.ftpusers

(ftpusers 파일에 등록된 계정들만 접속이 차단됨)

조치 시 영향	애플리케이션에서 root로 바로 접속하여 ftp를 사용하고 있을 경우 확인 필요
----------------	--

UNIX 서버

취약점 항목		3.29. at 파일 소유자 및 권한 설정			
대상 OS	SunOS, LINUX, AIX, HP-UX	위험도	중	Code	U-64
취약점 개요	*at 명령어 사용자 제한은 at.allow 파일과 at.deny 파일에서 할 수 있으므로 보안상 해당 파일에 대한 접근제한이 필요함. 만약 at 접근제한 파일의 권한이 잘못되어 있을 경우 권한을 획득한 사용자 계정을 등록하여 불법적인 예약 파일 실행으로 시스템 피해를 발생할 수 있음.				
	*at 데몬 (일회성 작업 예약): 지정한 시간에 어떠한 작업이 실행될 수 있도록 작업 스케줄을 예약 처리해 주는 기능을 제공함. /etc/at.allow 파일에 등록된 사용자만이 at 명령을 사용할 수 있음.				
보안대책					
판단기준	양호: at 접근제어 파일의 소유자가 root이고, 권한이 640 이하인 경우				
	취약: at 접근제어 파일의 소유자가 root가 아니거나, 권한이 640 이하가 아닌 경우				
조치방법	"at.allow", "at.deny" 파일 소유자 및 권한 변경 (소유자 root, 권한 640 이하)				
보안설정방법					
OS별 점검 파일 위치 및 점검 방법					
SunOS	"/etc/cron.d/at.allow", "/etc/cron.d/at.deny" 파일의 소유자 및 권한 확인 #ls -l /etc/cron.d/at.allow #ls -l /etc/cron.d/at.deny rw-r----- root <파일명>				
LINUX	"/etc/at.allow", "/etc/at.deny" 파일의 소유자 및 권한 확인 #ls -l /etc/at.allow #ls -l /etc/at.deny rw-r----- root <파일명>				
AIX, HP-UX	"/var/adm/cron/at.allow", "/var/adm/cron/at.deny" 파일의 소유자 및 권한 확인 #ls -l /var/adm/cron/at.allow #ls -l /var/adm/cron/at.deny rw-r----- root <파일명>				

위에 제시한 파일의 소유자가 root가 아니거나 파일의 권한이 640 이하가 아닌 경우 아래의 보안설정방법에 따라 설정을 변경함

■ SunOS

1. "/etc/cron.d/at.allow" 및 "/etc/cron.d/at.deny" 파일의 소유자 및 권한 변경
chown root /etc/cron.d/at.allow
chmod 640 /etc/cron.d/at.allow
chown root /etc/cron.d/at.deny
chmod 640 /etc/cron.d/at. deny

UNIX 서버

■ LINUX

1. "/etc/at.allow" 및 "/etc/at.deny" 파일의 소유자 및 권한 변경

```
# chown root /etc/at.allow
# chmod 640 /etc/at.allow
# chown root /etc/at.deny
# chmod 640 /etc/at.deny
```

■ AIX, HP-UX

1. "/var/adm/cron/at.allow" 및 "/var/adm/cron/at.deny" 파일의 소유자 및 권한 변경

```
# chown root /var/adm/cron/at.allow
# chmod 640 / var/adm/cron/at.allow
# chown root /var/adm/cron/at.deny
# chmod 640 / var/adm/cron/at.deny
```

조치 시 영향	일반적인 경우 영향 없음
---------	---------------

UNIX 서버

취약점 항목		3.30. SNMP 서비스 구동 점검			
대상 OS	SunOS, LINUX, AIX, HP-UX	위험도	중	Code	U-65
취약점 개요	*SNMP(Simple Network Management Protocol)서비스는 시스템 상태를 실시간으로 파악하거나 설정하기 위하여 사용하는 서비스임. SNMP 서비스로 인하여 시스템의 주요 정보 유출 및 정보의 불법수정이 발생할 수 있으므로 SNMP 서비스를 사용하지 않을 경우 중지시킴.				
	*SNMP(Simple Network Management Protocol): TCP/IP 기반 네트워크상의 각 호스트에서 정기적으로 여러 정보를 자동으로 수집하여 네트워크 관리를 하기 위한 프로토콜을 의미함.				
보안대책					
점검기준	양호: SNMP 서비스를 사용하지 않는 경우				
	취약: SNMP 서비스를 사용하는 경우				
조치방법	SNMP 서비스를 사용하지 않는 경우 서비스 중지 후 시작 스크립트 변경				
보안설정방법					
OS별 점검 파일 위치 및 점검 방법					
SunOS, LINUX	#svcs -a grep snmp #svcadm disable svc:/application/management/snmpdx:default				
AIX	#ps -ef grep *Snmp* #cat /etc/rc.config.d/Snmp* grep SNMP_ grep -v '#' (1인 경우 자동실행)				
HP-UX	#ps -ef grep snmp #cat /etc/rc.tcpip grep snmp grep -v '#' #lssrc -a grep snmp #stopsrc -s snmpd #stopsrc -s snmpmibd				

불필요한 “SNMP” 서비스를 사용하는 경우 아래의 보안설정방법에 따라 설정을 변경함

■ SunOS, LINUX 설정

1. ls -al /etc/rc.d/rc*.d/* | grep snmp로 검색하여 위치 확인 후 이름 변경

2. #mv /etc/rc3.d /S76snmpdx /etc/rc3.d /_S76snmpdx

■ AIX 설정

1. ls -al /etc/rc.d/rc*.d/* | grep snmp로 검색하여 위치 확인 후 이름 변경

2. /etc/rc.tcpip 아래 주석처리

#start /usr/sbin/snmpd "\$src_running"

#start /usr/sbin/dpid2 "\$src_running"

■ HP-UX 설정

1. ls -al /sbin/rc*.d/* | grep snmp로 검색하여 위치 확인 후 이름 변경

UNIX 서버

2. 다음 파일에서 SNMP 관련 값을 0으로 변경

```
/etc/rc.config.d/SnmpHpxix -> SNMP_HPUNIX_START=0
/etc/rc.config.d/SnmpMaster -> SNMP_MASTER_START=0
/etc/rc.config.d/SnmpMib2 -> SNMP_MIB2_START=0
/etc/rc.config.d/SnmpTrpDst -> SNMP_TRAPDEST_START=0
```

■ SunOS 5.10

1. "svcs -a | grep snmp" 명령으로 데몬 확인

2. 데몬 활성화 확인

```
Ps -ef |grep snmp|grep -v "dmi"|grep -v "grep"또는,
svcs -a | grep snmp | grep -v "dmi" | grep -v "grep"
```

```
online 13:17:34svc:/application/management/snmpdx:default
```

3. "svcadm disable" 명령으로 데몬 중지

(예) svcadm disable svc:/application/management/snmpdx

조치 시 영향	일반적인 경우 영향 없음
----------------	---------------

UNIX 서버

취약점 항목		3.31. SNMP 서비스 Community String의 복잡성 설정			
대상 OS	SunOS, LINUX, AIX, HP-UX	위험도	중	Code	U-66
취약점 개요	*SNMP(Simple Network Management Protocol) 서비스는 시스템 상태를 실시간으로 파악하는 *NMS(Network Management System)를 위하여 UNIX 시스템에서 기본적으로 제공하는 서비스이며 정보를 받기 위해 일종의 패스워드인 Community String을 사용함. *Community String은 Default로 public, private로 설정된 경우가 많으며, 이를 변경하지 않으면 이 String을 악용하여 시스템의 주요 정보 및 설정을 파악할 수 있음.				
	*SNMP(Simple Network Management Protocol): TCP/IP 기반 네트워크상의 각 호스트에서 정기적으로 여러 정보를 자동으로 수집하여 네트워크 관리를 하기 위한 프로토콜을 의미함. *NMS(Network Management System): 네트워크상의 모든 장비의 중앙 감시 체제를 구축하여 모니터링, 플래닝, 분석을 시행하고 관련 데이터를 보관하여 필요 즉시 활용 가능하게 하는 관리 시스템을 말함. *Community String: SNMP는 MIB라는 정보를 주고받기 위해 인증 과정에서 일종의 비밀번호인 'Community String'을 사용함.				
보안대책					
판단기준	양호: SNMP Community 이름이 public, private 이 아닌 경우				
	취약: SNMP Community 이름이 public, private 인 경우				
조치방법	snmpd.conf 파일에서 커뮤니티명을 확인한 후 디폴트 커뮤니티명인 "public, private"를 추측하기 어려운 커뮤니티명으로 변경				
보안설정방법					
OS별 점검 파일 위치 및 점검 방법					
SunOS 9 이하 버전	#vi /etc/snmp/conf/snmpd.conf read-community public / write-community private				
SunOS 10 이상 버전	#vi /etc/sma/snmp/snmpd.conf rocommunity public / rwcommunity private				
LINUX	#vi /etc/snmp/snmpd.conf com2sec notConfigUser default public				
AIX	#vi /etc/snmpdv3.conf COMMUNITY public public noAuthNoPriv 0.0.0.0 0.0.0 -				
HP-UX	#vi /etc/snmpd.conf get-community-name: public / set-commnunity-name : private				
위의 설정과 같이 디폴트 커뮤니티명인 "public" 또는, "private"을 사용하는 경우 아래의 보안설정방법에 따라 설정을 변경함					

UNIX 서버

OS별 snmpd.conf 파일 위치	
SunOS	/etc/snmpd.conf /etc/snmp/snmpd.conf /etc/snmp/conf/snmpd.conf /etc/sma/snmp/snmpd.conf" (SunOS 10 버전 일 경우)
LINUX	/etc/snmpd.conf /etc/snmp/snmpd.conf /etc/snmp/conf/snmpd.conf
AIX	SNMP V1 을 사용할 경우: /etc/snmpd.conf SNMP V3 을 사용할 경우: /etc/snmpdv3.conf
HP-UX	/etc/snmpd.conf /etc/snmp/snmpd.conf /etc/snmp/conf/snmpd.conf

※ 일부 정보보호시스템에 따라 또는, 설치 경로에 따라 다를 수 있음

■ SunOS

1. vi 편집기를 이용하여 SNMP 설정파일을 연 후
2. Community String 값 설정 변경 (추측하기 어려운 값으로 설정)

- SunOS9 이하 버전 -

```
#vi /etc/snmp/conf/snmpd.conf
```

(수정 전) read-community public / write-community private

(수정 후) read-community <변경 값> / write-community <변경 값>

- SunOS10 이상 버전 -

```
#vi /etc/sma/snmp/snmpd.conf
```

(수정 전) rocommunity public / rwcommunity private

(수정 후) rocommunity <변경 값> / rwcommunity <변경 값>

■ LINUX

1. vi 편집기를 이용하여 SNMP 설정파일을 연 후
#vi /etc/snmp/snmpd.conf
2. Community String 값 설정 변경 (추측하기 어려운 값으로 설정)
(수정 전) com2sec notConfigUser default public
(수정 후) com2sec notConfigUser default <변경 값>

■ AIX

1. vi 편집기를 이용하여 SNMP 설정파일을 연 후
#vi /etc/snmpdv3.conf
2. Community String 값 설정 변경 (추측하기 어려운 값으로 설정)

UNIX 서버

(수정 전) COMMUNITY public public noAuthNoPriv 0.0.0.0 0.0.0 -

(수정 후) COMMUNITY <변경 값> <변경 값> noAuthNoPriv 0.0.0.0 0.0.0 -

■ HP-UX

1. vi 편집기를 이용하여 SNMP 설정파일을 연 후

#vi /etc/snmpd.conf

3. Community String 값 설정 변경 (추측하기 어려운 값으로 설정)

(수정 전) get-community-name: public / set-community-name : private

(수정 후) get-community-name: <변경 값> / set-community-name: <변경 값>

조치 시 영향

NMS에서 서버를 모니터링 하는 경우 SNMP를 사용하며, 기타 SNMP를 사용할 경우 Community String 변경 시 통신하고자 하는 Server/Client에 모두 같은 Community String을 사용하여야 함

UNIX 서버

취약점 항목	3.32. 로그인 시 경고 메시지 제공				
대상 OS	SunOS, LINUX, AIX, HP-UX	위험도	중	Code	U-67
취약점 개요	로그인 배너가 설정되지 않을 경우 배너에 서버 OS 버전 및 서비스 버전이 공격자에게 노출될 수 있으며 공격자는 이러한 정보를 통하여 해당 OS 및 서비스의 취약점을 이용하여 공격을 시도할 수 있음.				
보안대책					
판단기준	양호: 서버 및 Telnet 서비스에 로그인 메시지가 설정되어 있는 경우				
	취약: 서버 및 Telnet 서비스에 로그인 메시지가 설정되어 있지 않은 경우				
조치방법	Telnet, FTP, SMTP, DNS 서비스를 사용할 경우 설정파일 조치 후 inetd 데몬 재시작				
보안설정방법					

OS별 점검 파일 위치 및 점검 방법

SunOS, LINUX, AIX, HP-UX	#vi /etc/motd 서버 로그인 메시지 설정 여부 확인
-----------------------------	--------------------------------------

위에 제시한 파일 내에 로그인 메시지 설정이 적용되지 않은 경우 아래의 보안설정방법에 따라 로그인 메시지를 입력함

OS별 점검 파일 위치 및 점검 방법

SunOS	#vi /etc/default/telnetd BANNER="WwRwWnWwRwWn 'uname -a' 'uname -r' WwRwWnWwRwWn"
LINUX	#vi /etc/issue.net CentOS release 5.3 (Final) Kernel Ww on an Ww
AIX	#vi /etc/security/login.cfg default: 설정 없음
HP-UX	#vi /etc/inetd.conf telnet stream tcp nowait root /usr/sbin/telnetd telnetd

위에 제시한 파일 내 Telnet 배너 설정이 위와 같을 경우 아래의 보안설정방법에 따라 설정을 변경함

■ SunOS

1. 서버 로그인 메시지 설정: vi 편집기로 "/etc/motd" 파일을 연 후 로그인 메시지 입력
#vi /etc/motd
(수정 전) 내용 없음
(수정 후) 로그인 메시지 입력
2. Telnet 배너 설정: vi 편집기로 "/etc/default/telnetd" 파일을 연 후 로그인 메시지 입력
#vi /etc/default/telnetd
(수정 전) BANNER="WwRwWnWwRwWn 'uname -a' 'uname -r' WwRwWnWwRwWn"
(수정 후) BANNER="로그인 메시지 입력"

UNIX 서버

■ LINUX

1. 서버 로그인 메시지 설정: vi 편집기로 "/etc/motd" 파일을 연 후 로그인 메시지 입력
#vi /etc/motd
(수정 전) 내용 없음
(수정 후) 로그인 메시지 입력
2. Telnet 배너 설정: vi 편집기로 "/etc/issue.net" 파일을 연 후 로그인 메시지 입력
#vi /etc/issue.net
(수정 전) CentOS release 5.3 (Final) Kernel W r on an W m
(수정 후) 로그인 메시지 입력

■ AIX

1. 서버 로그인 메시지 설정: vi 편집기로 "/etc/motd" 파일을 연 후 로그인 메시지 입력
#vi /etc/motd
(수정 전) 내용 없음
(수정 후) 로그인 메시지 입력
2. Telnet 배너 설정: vi 편집기로 "/etc/security/login.cfg" 파일을 연 후 로그인 메시지 입력
#vi /etc/security/login.cfg
(수정 전) default: 설정 부분에 herald 설정 없음
(수정 후) default: 설정 부분에 herald="로그인 메시지" 설정 추가

■ HP-UX

1. 서버 로그인 메시지 설정: vi 편집기로 "/etc/motd" 파일을 연 후 로그인 메시지 입력
#vi /etc/motd
(수정 전) 내용 없음
(수정 후) 로그인 메시지 입력
2. Telnet 배너 설정: vi 편집기로 "/etc/inetd.conf" 파일을 연 후 telnet 부분에 로그인 파일 설정
#vi /etc/inetd.conf
(수정 전) telnet stream tcp nowait root /usr/sbin/telnetd telnetd
(수정 후) telnet stream tcp nowait root /usr/sbin/telnetd telnetd -b /etc/issue

조치 시 영향	일반적인 경우 영향 없음
---------	---------------

UNIX 서버

취약점 항목	3.33. NFS 설정파일 접근권한				
대상 OS	SunOS, LINUX, AIX, HP-UX	위험도	중	Code	U-68
취약점 개요	*NFS(Network File System) 접근제어 설정파일을 관리자가 아닌 일반 사용자들도 접근 및 변경이 가능하면 이를 통해 인가되지 않은 사용자를 등록하고 파일시스템을 마운트하여 불법적인 변조를 시도할 수 있음. 따라서 NFS 접근제어 설정파일을 일반 사용자들이 수정할 수 없도록 제한하고 있는지 점검하여야 함. *NFS(Network File System): 원격 컴퓨터의 파일시스템을 로컬 시스템에 마운트하여 마치 로컬 파일시스템처럼 사용할 수 있는 프로그램.				
보안대책					
판단기준	양호: NFS 접근제어 설정파일의 소유자가 root 이고, 권한이 644 이하인 경우 취약: NFS 접근제어 설정파일의 소유자가 root 가 아니거나, 권한이 644 이하가 아닌 경우				
조치방법	NFS 접근제어 설정파일의 소유자 및 권한 변경 (소유자 root, 권한 644)				
보안설정방법					
OS별 점검 파일 위치 및 점검 방법					
SunOS		#ls -al /etc/dfs/dfstab rw-r--r-- root <nfs 접근제어 파일>			
LINUX, AIX, HP-UX		#ls -al /etc/exports rw-r--r-- root <nfs 접근제어 파일>			
“NFS” 접근제어 설정파일의 소유자가 root가 아니거나 파일의 권한이 644 이하가 아닌 경우 아래의 보안설정방법에 따라 설정을 변경함 ■ SunOS “/etc/dfs/dfstab” 파일의 소유자 및 권한 변경 (소유자 root, 권한 644) <pre>#chown root /etc/dfs/dfstab #chmod 644 /etc/dfs/dfstab</pre> ■ LINUX, AIX, HP-UX “/etc/exports” 파일의 소유자 및 권한 변경 (소유자 root, 권한 644) <pre>#chown root /etc/exports #chmod 644 /etc/exports</pre>					
조치 시 영향	일반적인 경우 영향 없음				

UNIX 서버

취약점 항목		3.34. expn, vrfy 명령어 제한			
대상 OS	SunOS, LINUX, AIX, HP-UX	위험도	중	Code	U-69
취약점 개요	*SMTP(Simple Mail Transfer Protocol)는 많은 취약성을 갖고 있어 잠재적인 위험이 존재함. 서버에서 SMTP를 사용하는 목적을 검토하여 사용할 필요가 없는 경우 서비스를 제거해야 하며, SMTP 서비스 운영 시 Sendmail Abuse를 방지하기 위해 Sendmail의 기본적인 서비스인 *VRFY, *EXPN을 막아야 함.				
	*SMTP(Simple Mail Transfer Protocol) 서버: 인터넷상에서 전자우편(E-mail)을 전송할 때 이용하게 되는 표준 통신 규약을 말함.				
	*VRFY: SMTP 클라이언트가 SMTP 서버에 특정 아이디에 대한 메일이 있는지 검증하기 위해 보내는 명령어를 말함.				
	*EXPN(메일링 리스트 확장): 메일 전송 시 포워딩하기 위한 명령어를 말함.				
보안대책					
판단기준	양호: SMTP 서비스 미사용 또는, noexpn, novrfy 옵션이 설정되어 있는 경우				
	취약: SMTP 서비스를 사용하고, noexpn, novrfy 옵션이 설정되어 있지 않는 경우				
조치방법	SMTP 서비스 설정파일에 noexpn, novrfy 옵션 추가				
보안설정방법					
OS별 점검 파일 위치 및 점검 방법					
SunOS, LINUX, HP-UX		noexpn, novrfy 옵션 설정 확인 #vi /etc/mail/sendmail.cf O PrivacyOptions=authwarnings			
AIX		#vi /etc/sendmail.cf O PrivacyOptions=authwarnings			
위의 설정과 같이 noexpn, novrfy 옵션이 추가되지 않은 경우 아래의 보안설정방법에 따라 옵션 추가					
<서비스 필요 시>					
■ SunOS, LINUX, HP-UX					
1. vi 편집기를 이용하여 "/etc/mail/sendmail.cf" 파일을 연 후 (단, AIX는 /etc/sendmail.cf) #vi /etc/mail/sendmail.cf					
2. "/etc/mail/sendmail.cf" 파일에 noexpn, novrfy 옵션 추가 (수정 전) O PrivacyOptions=authwarnings (수정 후) O PrivacyOptions=authwarnings, noexpn, novrfy					
3. SMTP 서비스 재시작					
< 서비스 불필요 시>					
■ SunOS, LINUX, HP-UX					
1. 실행중인 서비스 중지 #ps -ef grep sendmail					

UNIX 서버

```
root 441 1 0 Sep19 ? 00:00:00 sendmail: accepting connections
```

```
#kill -9 [PID]
```

2. 시스템 재시작 시 SMTP 서버가 시작되지 않도록 OS별로 아래와 같이 설정함

■ SunOS, LINUX

1. 위치 확인

```
#ls -al /etc/rc*.d/* | grep sendmail
```

2. 이름 변경

```
#mv /etc/rc2.d/S88sendmail /etc/rc2.d/_S88sendmail
```

■ AIX

1. 위치 확인

```
#ls -al /etc/rc.d/rc*.d/* | grep sendmail
```

2. 이름 변경

```
#mv /etc/rc2.d/S88sendmail /etc/rc2.d/_S88sendmail
```

3. /etc/rc.tcpip 파일에서 아래 내용 #처리(주석 처리)

```
(수정 전) start /usr/lib/sendmail "$src_running" "-bd -q${qpi}"
```

```
(수정 후) #start /usr/lib/sendmail "$src_running" "-bd -q${qpi}"
```

■ HP-UX

1. 위치 확인

```
#ls -al /sbin/rc*.d/* | grep sendmail
```

2. 이름 변경

```
#mv /sbin/rc2.d/S540sendmail /sbin/rc2.d/_S540sendmail
```

3. /etc/rc.config.d/mailservs 파일에서 SENDMAIL_SERVER 값을 "0"으로 변경 (9.x 이하: /etc/netbsdsrc)
SENDMAIL_SERVER=0

■ SunOS 5.10

1. #svcs -a | grep smtp

2. 데몬 활성화 확인

```
online          13:17:45  svc:/network/smtp:sendmail
```

3. 데몬 중지

```
#svcadm disable [서비스 데몬명]
```

```
(예) #svcadm disable svc:/network/smtp:sendmail
```

조치 시 영향	일반적인 경우 영향 없음
----------------	---------------

UNIX 서버

취약점 항목		3.35. Apache 웹서비스 정보 숨김			
대상 OS	SunOS, LINUX, AIX, HP-UX	위험도	중	Code	U-70
취약점 개요	에러 페이지, 웹 서버 종류, OS 정보, 사용자 계정 이름 등 웹 서버와 관련된 불필요한 정보가 노출되지 않도록 하여야 함. 불필요한 정보가 노출될 경우 해당 정보를 이용하여 시스템의 취약점을 수집할 수 있음.				
보안대책					
판단기준	양호: ServerTokens 지시자에 Prod 옵션이 설정되어 있는 경우				
	취약: ServerTokens 지시자에 Prod 옵션이 설정되어 있지 않는 경우				
조치방법	헤더에 최소한의 정보를 제한 후 전송 (ServerTokens 지시자에 Prod 옵션 설정)				
보안설정방법					
OS별 점검 파일 위치 및 점검 방법					
SunOS, LINUX, AIX, HP-UX	Prod 옵션 설정 여부 확인 #vi /[Apache_home]/conf/httpd.conf ServerTokens Prod				
"httpd.conf" 파일 내에 ServerTokens 지시자가 위와 같이 "Prod"로 설정되지 않은 경우 아래의 보안설정방법에 따라 옵션 추가					
■ SunOS, LINUX, AIX, HP-UX					
1. vi 편집기를 이용하여 /[Apache_home]/conf/httpd.conf 파일을 연 후 #vi /[Apache_home]/conf/httpd.conf					
2. 설정된 모든 디렉터리의 ServerTokens 지시자에서 Prod 옵션 설정 (없으면 신규 삽입)					
<Directory /> Options Indexes FollowSymLinks ServerTokens Prod - 이하생략 - </Directory>					

UNIX 서버

ServerTokens 지시자 옵션		
키워드	제공하는 정보	예문
Prod	웹 서버 종류	Server Apache
Min	Prod 키워드 제공 정보 + 웹 서버 버전	Server Apache/1.3.0
OS	Min 키워드 제공 정보 + 운영체제	Server Apache/1.3.0 (Unix)
Full	OS 키워드 제공 정보 + 설치된 모듈(응용프로그램) 정보	Server Apache/1.3.0 (Unix) PHP/3.0 MyMod/1.2

조치 시 영향 일반적인 경우 영향 없음

UNIX 서버

4. 패치 관리

취약점 항목		4.1. 최신 보안패치 및 벤더 권고사항 적용			
대상 OS	SunOS, LINUX, AIX, HP-UX	위험도	상	Code	U-71
취약점 개요	주기적인 패치 적용을 통하여 보안성 및 시스템 안정성을 확보하는 것이 시스템 운용의 중요한 요소임. 서비스 중인 시스템의 경우 패치 적용에 따르는 문제점(현재 운용중인 응용프로그램의 예기치 않은 중지, 패치 자체의 버그 등)과 재부팅의 어려움 등으로 많은 패치를 적용하는 것이 매우 어렵기 때문에 패치 적용 시 많은 부분을 고려하여야 함.				
보안대책					
판단기준	양호: 패치 적용 정책을 수립하여 주기적으로 패치를 관리하고 있는 경우				
	취약: 패치 적용 정책을 수립하지 않고 주기적으로 패치관리를 하지 않는 경우				
조치방법	O/S 관리자, 서비스 개발자가 패치 적용에 따른 서비스 영향 정도를 파악하여 OS 관리자 및 벤더에서 적용함 ※ OS 패치의 경우 지속적으로 취약점이 발표되고 있기 때문에 O/S 관리자, 서비스 개발자가 패치 적용에 따른 서비스 영향 정도를 정확히 파악하여 주기적인 패치 적용 정책을 수립하여 적용하여야 함				
보안설정방법					
OS별 점검 방법					
SunOS, LINUX, AIX, HP-UX		패치 적용 정책 수립 여부 및 정책에 따른 패치 적용 여부 확인			

■ SunOS

1. "showrev -p" 로 서버에 적용되어 있는 패치 리스트 확인

2. 아래 2개 패치 사이트 중 하나를 선택 후 접속하여 패치를 찾아 적용

- OS별, 제품별, 보안 관련 그리고 y2k 패치로 분류되어 패치 파일 제공
<http://access1.sun.com/patch.y2k/>
- OS별로 추천되는 패치 파일 제공
<http://sunsolve.sun.com/pub-cgi/show.pl?target=patches/patch-access>

< 패치 적용의 예 1 >

#mkdir /var/spool/patch

위와 같은 디렉토리를 만들어 Patch 파일을 관리하도록 함

(패치 설치 순서 예): 107403-02: SunOS 5.7: rlm0d & telmod Patch 를 적용하고자 함

#showrev -p | grep 107403

Patch: 107403-01 Obsoletes: Requires: Incompatibles: Packages: SUNWcsu, SUNWcsxu

UNIX 서버

```
#ls
107403-02.zip
#unzip 107403-02.zip
#patchadd /var/spool/patch/107403-02
erifying sufficient filesystem capacity (dry run method)...
Installing patch packages...
```

Patch number 107403-02 has been successfully installed.
See /var/sadm/patch/107403-02/log for details

Patch packages installed:
SUNWcsu
SUNWcsxu

```
#showrev -p | grep 107403
Patch: 107403-01 Obsoletes: Requires: Incompatibles: Packages: SUNWcsu, SUNWcsxu
Patch: 107403-02 Obsoletes: Requires: Incompatibles: Packages: SUNWcsu, SUNWcsxu
```

※ 설치 시 주의할 점

1. 패치 적용 후 Rebooting이 필요한 경우가 있으므로 README-Patch-ID 파일 확인 필요
2. 패치 제거 방법: #patchrm Patch-ID 실행

< 패치 적용의 예 2 >

패치 cluster의 이용

패치 cluster란 Sun에서 Recommended 패치와 보안 관련 패치들을 통합하여, 각 시스템 관리자들의 편의를 도모하기 위한 패키지 형태로 제공되는 패치 묶음을 가리킴

이들 패치 cluster는 Sun의 Web 페이지와 ftp 서버에서도 구할 수 있으며, 각각의 패치 cluster들은 아래와 같은 파일명으로 구성됨

```
[version]_Recommended.tar.Z
[version]_Recommended.README
2.5.1_Recommended.tar.Z
2.5.1_Recommended.README
```

위와 같이 각 버전에 따라 Recommended.tar.Z와 같은 바이너리 패치 묶음과 해당 패치 cluster에 대한 주석을 담고 있는 README 파일이 제공되므로 각 시스템의 관리자들은 Sun 사이트에 접속하여 패치 cluster와 README 파일 다운로드 하여 시스템에 설치할 수 있음

<http://sunsolve.sun.com/pub-cgi/show.pl?target=patches/patch-license&nav=pub-patches>

UNIX 서버

< 패치 적용의 예 3 >

Automate patch management tool를 사용하여 현재 시스템에서 업데이트 패치 및 설치될 패치를 분석하여 웹상에서 자동으로 patch list를 다운받아서 설치함

현재 Automate patch management tool을 사용하여 적용될 수 있는 시스템들은 다음과 같음

```
#gunzip -dc pproSunOSx865.9jre2.2.tar.gz | tar xvf -
#zcat pproSunOSSparc5.6jre2.2.tar.Z | tar xvf -
#cd pproSunOSSparc5.9jre2.2
#./setup
```

< 시스템 현황 >

SunOS 2.6 - 9, Sun Cluster, Network Storage, and E10Ks and Star Fires

< Patch management tool download >

<https://sunsolve.sun.com/patchpro/patchpro.html>

■ LINUX

Linux는 서버에 설치된 패치 리스트의 관리가 불가능하므로 rpm 패키지 별 버그가 Fix된 최신 버전 설치가 필요함

Linux는 오픈 되고, 커스터마이징 된 OS이므로 Linux를 구입한 벤더에 따라 rpm 패키지가 다를 수 있으며, 아래의 사이트는 RedHat Linux에 대한 버그 Fix 관련 사이트임

<Red Hat 일 경우>

Step 1. 다음의 사이트에서 해당 버전을 찾음

<http://www.redhat.com/security/updates/>

<http://www.redhat.com/security/updates/eol/> (Red Hat Linux 9 이하 버전)

Step 2. 발표된 Update 중 현재 사용 중인 보안 관련 Update 찾아 해당 Update Download

Step 3. Update 설치

```
#rpm -Uvh <package-name>
```

■ AIX

"instfix -iv | grep ML"로 서버에 적용되어 있는 패치 리스트 확인

버전4.3의 경우 아래 사이트에서 다음과 같은 방법으로 패치 버전을 다운받을 수 있고 원하는 레벨의 ML를 찾을 수 있음

※ current를 현재 버전 level로 등록하고, update to를 최신의 대상 패치 버전으로 선택

<http://techsupport.services.ibm.com/server/mlfixes/43/>

UNIX 서버

< 패치 적용의 예 1>

Click on the package name below.

Put the package (a tar.gz file) in /usr/sys/inst.images

Extract the filesets from the package.

```
cd /usr/sys/inst.images
```

```
gzip -d -c 4330910.tar.gz | tar -xvf -
```

Back up your system. 0

Install the package by creating a table of contents for install to use. Then update the install subsystem itself. Run SMIT to complete the installation.

```
inutoc /usr/sys/inst.images
```

```
installp -acgXd /usr/sys/inst.images bos.rte.install
```

```
smit update_all
```

Reboot your system. This maintenance package replaces critical operating system code.

< Security Patch Check 관련 사이트 >

<http://techsupport.services.ibm.com/server/nav?fetch=pm>

■ HP-UX

'swlist -l product'로 서버에 적용된 패치 리스트 확인

HPUX 는 다양한 하드웨어 플랫폼과 O/S로 인해 General 한 Security Patch가 공개되어 있지 않으며, security_patch_check 프로그램(필 스크립트)을 서버에 설치·실행하여 서버의 취약한 Security Patch 리스트를 얻을 수 있음

security_patch_check는 현재 적용되고 있는 패치 리스트를 분석하는 툴로써, 적용 가능한 패치와 설치되지 않은 패치 정보를 리포트 형식으로 제공하고 보안 패치에 대한 오류 정보를 자동으로 체크하여 알려줌

security_patch_check 프로그램을 사용하기 위해서는 Service Control Manager 도구를 서버에 설치하여야 함 (security_patch_check 사용관련 내용은 '비고' 참조)

< Security Patch Check 관련 사이트 >

http://www.software.hp.com/cgi-bin/swdepot_parser.cgi/cgi/displayProductInfo.pl?productNumber=B6834AA

< 패치 적용의 예 1>

1. 수작업에 의한 패치 적용

운영자에 의한 패치 적용은 다음과 같은 단계에 의해 수행됨

- 1) <http://support2.itrc.hp.com/service/patch/mainPage.do> 접속
- 2) HPUX 선택하여 해당 페이지 이동
- 3) 해당되는 H/W, OS 선택
- 4) 키워드, Patch-ID, Patch 리스트 옵션을 선택하여 검색

UNIX 서버

- 5) 검색 결과 확인
- 6) 필요한 패치를 선택하여 다운로드 받음
- 7) 패치 간의 dependency를 고려하여 적용할 패치 결정

2. Custom Patch Manager에 의한 패치 적용

CPM(Custom Patch Manager)은 해당 시스템에 적합한 패치를 선택하고 다운로드 받을 수 있도록 하는 툴이며, CPM을 이용하여 환경에서 설정된 일정 기간 간격별로 패치를 자동 적용할 수 있고 dependency 관계나 conflict 관계에 대해 자동 분석된 결과를 얻어 적용할 패치 정보를 확인할 수 있음

CPM을 이용하는 단계는 다음과 같은 단계에 의해 수행됨

- 1) ITRC 웹 사이트 <http://itrc.hp.com>로 이동하여 로그인
- 2) maintenance/support 링크를 클릭한 후 customized patch bundles를 선택
- 3) cpm_collect.sh 스크립트를 다운로드 받아 실행 후 현재 configuration에 대한 정보를 취합
- 4) cpm_collect.sh 스크립트를 실행 후 configuration에 대한 결과를 ITRC 페이지에 업로드
- 5) Perform Patch Analysis를 클릭하여 필요한 candidate patch list를 얻음
- 6) 선택한 패치 간의 conflict가 없는지 점검
- 7) 선택한 패치를 Package 버튼을 선택하여 다운로드 받은 후 패치 설치

조치 시 영향	일반적인 경우 영향 없음
----------------	---------------

UNIX 서버

5. 로그 관리

취약점 항목	5.1. 로그의 정기적 검토 및 보고				
대상 OS	SunOS, LINUX, AIX, HP-UX	위험도	상	Code	U-72
취약점 개요	로그 정보는 침해사고 발생 시 해킹의 흔적 및 공격기법을 확인할 수 있는 중요 자료로 정기적인 로그 분석을 통하여 시스템 침입 흔적과 취약점을 확인할 수 있음.				
보안대책					
판단기준	양호: 로그 기록의 검토, 분석, 리포트 작성 및 보고 등이 정기적으로 이루어지는 경우				
	취약: 로그 기록의 검토, 분석, 리포트 작성 및 보고 등이 정기적으로 이루어지지 않는 경우				
조치방법	원격 접속 시 root 계정으로 바로 접속 할 수 없도록 설정파일 수정				
보안설정방법					
OS별 점검 방법					
SunOS, LINUX, AIX, HP-UX	로그 분석 계획 수립 여부 및 로그 분석 결과에 대한 점검				

■ SunOS, LINUX, AIX, HP-UX

정기적인 로그 분석을 위하여 아래와 같은 절차 수립

1. 정기적인 로그 검토 및 분석 주기 수립

2. 로그 분석에 대한 결과 보고서 작성

3. 로그 분석 결과보고서 보고 체계 수립

조치 시 영향	일반적인 경우 영향 없음
---------	---------------

UNIX 서버

취약점 항목		5.2. 정책에 따른 시스템 로깅 설정			
대상 OS	SunOS, LINUX, AIX, HP-UX	위험도	하	Code	U-73
취약점 개요	감사 설정이 구성되어 있지 않거나 보안 정책에 비하여 감사 설정 수준이 낮아 보안 사고가 발생한 경우 원인 파악 및 각종 침해 사실에 대한 확인이 어려우며, 법적 대응을 위한 충분한 증거로 사용할 수 없음.				
보안대책					
판단기준	양호: 로그 기록 정책이 정책에 따라 설정되어 수립되어 있는 경우				
	취약: 로그 기록 정책 미수립, 또는, 정책에 따라 설정되어 있지 않은 경우				
조치방법	로그 기록 정책을 수립하고, 정책에 따라 syslog.conf 파일을 설정				
보안설정방법					
■ SunOS					
1. vi 편집기를 이용하여 "/etc/syslog.conf" 파일을 연 후 #vi /etc/syslog.conf					
2. 아래와 같이 수정 또는, 신규 삽입					
<pre>mail.debug /var/log/mail.log *.info /var/log/syslog.log *.alert /var/log/syslog.log *.alert /dev/console *.alert root *.emerg *</pre>					
3. 위와 같이 설정 후 SYSLOG 데몬 재시작					
- SunOS 9 이하 버전 -					
#ps -ef grep syslogd					
root 7524 6970 0 Apr 23 - 0:02 /usr/sbin/syslogd					
#kill -HUP [PID]					
- SunOS 10 이상 버전 -					
#svcs -a grep system-log					
online 16:23:03 svc:/system/system-log:default					
#svcadm refresh svc:/system/system-log:default					
■ LINUX					
1. vi 편집기를 이용하여 "/etc/syslog.conf" 파일을 연 후 #vi /etc/syslog.conf					
2. 아래와 같이 수정 또는, 신규 삽입					

UNIX 서버

```
*.info;mail.none;authpriv.none;cron.none /var/log/messages
authpriv.*      /var/log/secure
mail.*          /var/log/maillog
cron.*          /var/log/cron
*.alert         /dev/console
*.emerg         *
```

3. 위와 같이 설정 후 SYSLOG 데몬 재시작

```
#ps -ef |grep syslogd
root 7524 6970 0 Apr 23 - 0:02 /usr/sbin/syslogd
#kill -HUP [PID]
```

■ AIX

1. vi 편집기를 이용하여 "/etc/syslog.conf" 파일을 연 후

```
#vi /etc/syslog.conf
```

2. 아래와 같이 수정 또는, 신규 삽입

```
*.emerg         *
*.alert         /dev/console
*.alert         /var/adm/alert.log
*.err           /var/adm/error.log
mail.info       /var/adm/mail.log
auth.info       /var/adm/auth.log
daemon.info     /var/adm/daemon.log
*.emerg;*.alert;*.crit;*.err;*.warning;*.notice;*.info /var/adm/messages
```

3. 위와 같이 설정 후 SYSLOG 데몬 재시작

```
#refresh -s syslogd 또는,
#ps -ef |grep syslogd
root 7524 6970 0 Apr 23 - 0:02 /usr/sbin/syslogd
#kill -HUP [PID]
```

■ HP-UX

1. vi 편집기를 이용하여 "/etc/syslog.conf" 파일을 연 후

```
#vi /etc/syslog.conf
```

2. 아래와 같이 수정 또는, 신규 삽입

```
*.notice       /var/adm/syslog/syslog.log
*.alert        /dev/console
*.emerg        *
```

UNIX 서버

3. 위와 같이 설정 후 SYSLOG 데몬 재시작

```
#ps -ef |grep syslogd
root 7524 6970 0 Apr 23 - 0:02 /usr/sbin/syslogd
#kill -HUP [PID]
```

메시지 종류	
메시지	설명
auth	로그인 등의 인증 프로그램 유형이 발생한 메시지
authpriv	개인 인증을 요구하는 프로그램 유형이 발생한 메시지
cron	cron, at 데몬에서 발생한 메시지
daemon	telnet, ftpd 등과 같은 데몬이 발생한 메시지
kern	커널이 발생한 메시지
lpr	프린터 유형의 프로그램이 발생한 메시지
mail	메일 시스템에서 발생한 메시지
news	유즈넷 뉴스 프로그램 유형이 발생한 메시지
syslog	syslog 프로그램 유형이 발생한 메시지
user	사용자 프로세스 관련 메시지
uucp	시스템이 발생한 메시지
local0	여분으로 남겨둔 유형

메시지 우선순위	
메시지	설명
alert	즉각적으로 조치를 취해야 할 상황
crit	급한 상황은 아니지만, 치명적인 시스템 문제 발생 시
deberg	프로그램 실행 시 발생하는 오류 발생 시
emerg	매우 위험한 상황
err	에러 발생 시
info	단순한 프로그램에 대한 정보 메시지
notice	에러가 아닌 알림에 관한 메시지
warning	주의를 요하는 메시지

조치 시 영향

위에 제시한 모든 로그설정을 강제화할 경우, 시스템 퍼포먼스와 로그 저장에 따른 서버 용량 문제가 발생할 수 있으므로 시스템 운영 환경과 특성을 고려하여 적용

UNIX 서버

부 록

01. cat 명령어로 파일 내용 확인

cat 명령어는 텍스트 파일 내용 출력, 쓰기, 복사 시 사용하며 주로 텍스트 파일 내용을 표준 출력장치로 출력하여 확인하는 경우 사용됨. 명령어 입력 방법은 다음과 같음.

1. *#cat 파일 경로/파일명* : 파일을 열어 내용을 출력
2. *#cat > 파일 경로/파일명*
 같은 이름의 파일이 없는 경우 -> 파일을 새로 만들고 내용 입력
 같은 이름의 파일이 있는 경우 -> 파일을 덮어쓰고 새로 내용 입력
3. *#cat >> 파일 경로/파일명*
 같은 이름의 파일이 없는 경우 -> 파일을 새로 만들고 내용 입력
 같은 이름의 파일이 있는 경우 -> 기존 파일의 내용 밑에 이어서 입력

※ 덧붙여 사용할 수 있는 명령어

more	많은 내용 출력 시 사용하는 옵션 "Enter"를 누르면 한 줄씩, "SpaceBar"를 누르면 한 화면씩 더 보여줌
grep [Word]	특정 단어가 포함된 줄만 출력하는 명령어 [Word]에 특정 단어를 입력하여 호출
nl	파일의 내용이 총 몇 줄인지 출력하는 명령어
head	파일의 앞부분 10줄만 출력하는 명령어
tail	파일의 뒷부분 10줄만 출력하는 명령어

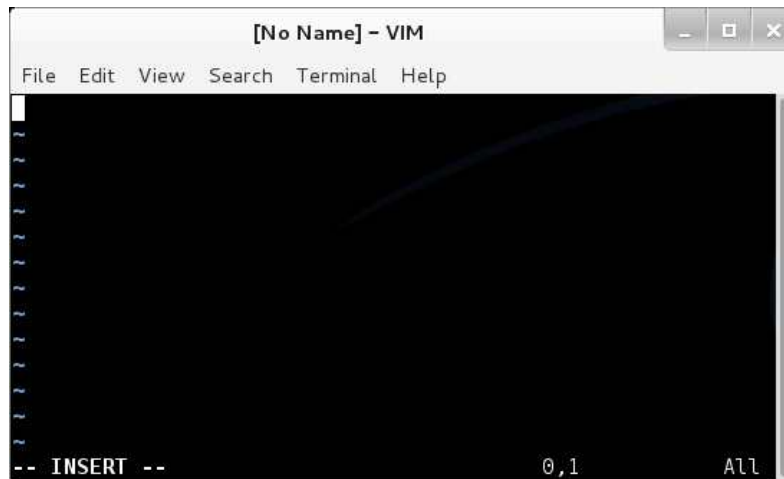
UNIX 서버

02. vi 편집기를 사용하여 파일 내용 수정

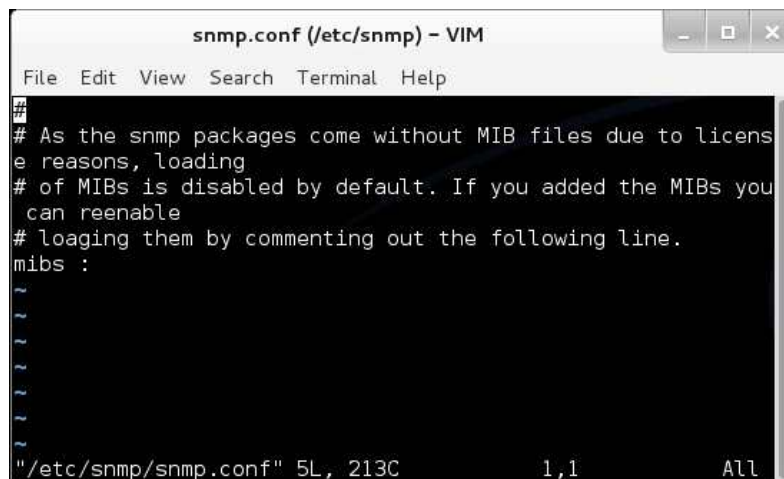
vi 편집기는 윈도우의 메모장처럼 사용되는 유닉스에서 제공하는 표준편집기를 말함.
이미 존재하는 파일을 수정하는 경우 또는, 신규 파일을 만들고자 할 때 vi 명령을 사용함.

#vi <파일 경로/파일명>

vi 명령어를 입력하여 프로그램을 시작하면 일반적으로 명령(normal)모드로 시작되고, 이때 키보드에서 "I" 키를 누르게 되면 편집(insert)모드로 바뀌어 "Esc" 키를 누를 때까지 문서 작성을 할 수 있음. (편집모드에서는 아래 화면과 같이 "--INSERT--"를 확인할 수 있음)



편집중인 문서 저장 시 ":w"를 입력하고, 수정 완료 후 ":q"를 입력하여 프로그램을 종료함.
파일에 쓰기 권한이 없을 때 'readonly' option qis set (use ! to override)라는 메시지가 출력이 되면서 저장이 안 되는 경우가 있는데 이때는 강제 옵션인 "!"를 추가로 붙여서 문제를 해결함.



※ vi 편집기는 아래의 "3가지 모드"로 구성됨.

1. 명령모드: 기본 구성 / 텍스트 편집 불가 / 명령어 수행
2. 편집모드: 텍스트 편집만 가능
3. 확장모드: 종료하거나 저장이 가능한 확장 기능 수행

UNIX 서버

03. find 명령어를 사용하여 파일 경로 확인

find 명령어는 원하는 파일을 계속 필터링 하면서 찾아볼 수 있도록 하고, 잘못 수정 된 파일을 추적할 때 유용하게 사용됨. 취약점 진단 시 각 운영체제별로 파일이 존재하는 위치에 차이가 있어 진단 조치 또는, 설정 여부 확인이 어려운 경우가 종종 있는데 find 명령어를 이용하여 파일이 위치한 경로를 쉽게 확인할 수 있음. find 명령어 기본형은 다음과 같음.

```
#find . -name 'pattern'
```

<find 명령어 사용 예시>

01. #find . -name '*.html'

. 은 현재 디렉터리에서 찾음, /usr와 같이 특정 위치에서 찾으려면 #find /usr -name '*.html'
-name은 파일 이름으로 찾으라는 조건으로 확장자가 .html 로 끝나는 파일만을 검색

02. #find . -type d

디렉터리만 검색

03. #find . -group admin -type l

그룹이 admin이면서 심볼릭 링크만 조회

04. #find . - user icocoa -maxdepth 1 -type d

현재 디렉터리 내에서 소유자가 icocoa이며, 디렉터리인 것만을 검색

05. #find . -name '*.jpg' -o -name '*.html'

-o 옵션은 OR 옵션으로 확장자가 .jpg인 것과 .html인 파일을 검색

06. #find . -atime -2

2일 동안 액세스가 일어나지 않은 파일 검색

07. #find . -atime +3

액세스가 일어난 후 3일된 파일 검색

08. #find . -mtime +7

7일 넘도록 변경되지 않은 파일 검색 (m: modification time)

09. #find . -mmin +30 -maxdepth 1 -type f

현재 디렉터리 내에서 변경이 있는 후 30분 지난 파일 검색(+,- 기호 사용)

10. #find . -name '*.xml' -exec grep -l 'Version' {} \;

현재 디렉터리 내에서 Version이라는 단어가 들어간 .xml 확장자를 가진 파일 검색

11. #find . \! -name '*.jpg'

.jpg로 끝나지 않는 파일 검색

12. #find . -newermm test.txt

test.txt 보다 나중에 수정된 파일 검색 (-newermm은 -newer와 동일)

13. #find . -size +100c(+,- 기호 사용)

사이즈가 100바이트 이상인 파일 검색(c: bytes) (-인 경우 100바이트보다 작은 파일 검색)

UNIX 서버

04. /etc/passwd, /etc/shadow, /etc/group 파일 구조

파일	속 성
/etc/passwd	사용자 ID, Shell 등 사용자 계정 정보 저장
/etc/shadow	root 또는, 사용자 계정의 암호 저장
/etc/group	각 그룹 목록에 대한 정보 저장

■ /etc/passwd

```

root@localhost:/etc
파일(F) 편집(E) 보기(V) 검색(S) 터미널(T) 도움말(H)
games:x:12:100:games:/usr/games:/sbin/nologin
gopher:x:13:30:gopher:/var/gopher:/sbin/nologin
ftp:x:14:50:FTP User:/var/ftp:/sbin/nologin
nobody:x:99:99:Nobody:/:/sbin/nologin
dbus:x:81:81:System message bus:/:/sbin/nologin
usbmuxd:x:113:113:usbmuxd user:/:/sbin/nologin
vcsa:x:69:69:virtual console memory owner:/dev:/sbin/nologin
rpc:x:32:32:Rpcbind Daemon:/var/cache/rpcbind:/sbin/nologin
rtkit:x:499:497:RealtimeKit:/proc:/sbin/nologin
avahi-autoipd:x:170:170:Avahi IPv4LL Stack:/var/lib/avahi-autoipd:/sbin/nologin
pulse:x:498:496:PulseAudio System Daemon:/var/run/pulse:/sbin/nologin
haldaemon:x:68:68:HAL daemon:/:/sbin/nologin
ntp:x:38:38:/:etc/ntp:/sbin/nologin
apache:x:48:48:Apache:/var/www:/sbin/nologin
saslauth:x:497:76:"Saslauthd user":/var/empty/saslauth:/sbin/nologin
postfix:x:89:89:/:var/spool/postfix:/sbin/nologin
abrt:x:173:173:/:etc/abrt:/sbin/nologin
rpcuser:x:29:29:RPC Service User:/var/lib/nfs:/sbin/nologin
nfsnobody:x:65534:65534:Anonymous NFS User:/var/lib/nfs:/sbin/nologin
gdm:x:42:42:/:var/lib/gdm:/sbin/nologin
sshd:x:74:74:Privilege-separated SSH:/var/empty/sshd:/sbin/nologin
tcpdump:x:72:72:/:/sbin/nologin
namegpark:x:500:500:namegpark:/home/namegpark:/bin/bash
[root@localhost etc]#

```

namegpark	x	500	500	namegpark	/home/namegpark	/bin/bash
계정명	패스워드	UID	GID	계정설명	홈 디렉터리	Shell 정보

UNIX 서버

■ /etc/shadow

```

root@localhost:etc
파일(F) 편집(E) 보기(V) 검색(S) 터미널(T) 도움말(H)

root@localhost:etc# cat shadow
root:$6$7QkaZvftw.YzVle3$Uv.dfQkeKxnCEklTHyF2o1S7NTQbdqQpI5xdDuYmDTod55b.mNIc8Q1GlkPSc25aoMiCip04bDmDDa6WjT/NN.:15788:0:99999:7:::
bin:!:15628:0:99999:7:::
daemon:!:15628:0:99999:7:::
adm:!:15628:0:99999:7:::
lp:!:15628:0:99999:7:::
sync:!:15628:0:99999:7:::
shutdown:!:15628:0:99999:7:::
halt:!:15628:0:99999:7:::
mail:!:15628:0:99999:7:::
uucp:!:15628:0:99999:7:::
operator:!:15628:0:99999:7:::
games:!:15628:0:99999:7:::
gopher:!:15628:0:99999:7:::
ftp:!:15628:0:99999:7:::
nobody:!:15628:0:99999:7:::
dbus:!:15788:!:!:!:
usbmuxd:!:15788:!:!:!:
vcsa:!:15788:!:!:!:
rpc:!:15788:0:99999:7:::
rtkit:!:15788:!:!:!:
avahi-autoipd:!:15788:!:!:!:

```

root	\$6\$7~	15788	0	99999	7
계정명	패스워드	암호 생성일자	변경가능 최소시간	유효기간	경고일수

■ /etc/group

```

root@localhost:etc
파일(F) 편집(E) 보기(V) 검색(S) 터미널(T) 도움말(H)

taped: x: 33:
dialout: x: 18:
wbpriv: x: 88:
pulse: x: 496:
pulse-access: x: 495:
fuse: x: 494:
haldaemon: x: 68: haldaemon
ntp: x: 38:
apache: x: 48:
sasauth: x: 76:
postdrop: x: 90:
postfix: x: 89:
abrt: x: 173:
rpcuser: x: 29:
nfsnobody: x: 65534:
gdm: x: 42:
stapusr: x: 156:
stapusr: x: 157:
stapdev: x: 158:
sshd: x: 74:
tcpdump: x: 72:
slocate: x: 21:
namepark: x: 500:
root@localhost:etc#

```

namepark	x	500	-
그룹명	패스워드	GID	그룹 구성원

UNIX 서버

05. 계정 설명

- lp:x:4:7:lp:/var/spool/lpd:/sbin/nologin = 로컬 프린트 서버
- sync:x:5:0:sync:/sbin:/bin/sync = 원격지 서버 동기화
- shutdown:x:6:0:shutdown:/sbin:/sbin/shutdown = soft 시스템 종료
- halt:x:7:0:halt:/sbin:/sbin/halt = 강제 시스템 종료
- mail:x:8:12:mail:/var/spool/mail:/sbin/nologin = 메일 서비스 계정
- news:x:9:13:news:/etc/news:/sbin/nologin
- uucp:x:10:14:uucp:/var/spool/uucp:/sbin/nologin = 유닉스 시스템 간 파일을 복사 프로토콜
- operator:x:11:0:operator:/root:/sbin/nologin = 설정에 따라 다르지만 /etc/syslog.conf 에 대해서 daemon.err operator라고 표기되어 있다면 데몬 관련 에러를 operator 계정을 이용해 출력하라는 의미임
- games:x:12:100:games:/usr/games:/sbin/nologin
- gopher:x:13:30:gopher:/var/gopher:/sbin/nologin = 웹(www)이 나오기 전 대표적인 서비스 중 하나로 gopher사이트 접속 후 잘 정리된 메뉴를 이용해서 웹 서핑을 즐기도록 한 서비스
- ftp:x:14:50:FTP User:/var/ftp:/sbin/nologin = ftp 사용 시 필요
- squid:x:23:23::/var/spool/squid:/sbin/nologin = 프록시 서버
- named:x:25:25:Named:/var/named:/sbin/nologin = 네임서비스 데몬 계정
- mysql:x:27:27::/home/mysql:/bin/bash = mysql 서비스 시작 시 사용하는 계정
- nscd:x:28:28:NSCD Daemon:/sbin/nologin = 네임서비스에 대한 캐시 기능 제공
- rpcuser:x:29:29:RPC Service User:/var/lib/nfs:/sbin/nologin
- rpc:x:32:32:Portmapper RPC user:/sbin/nologin = 원격 호출 관련 데몬
- netdump:x:34:34:Network Crash Dump user:/var/crash:/bin/bash = 네트워크 오류 파일 저장 서비스
- rpm:x:37:37::/var/lib/rpm:/sbin/nologin = 레드햇 패키지 매니저
- ntp:x:38:38::etc/ntp:/sbin/nologin = 컴퓨터 간 시간 동기화 Network Time Protocol
- gdm:x:42:42::/var/gdm:/sbin/nologin = x-window 사용
- xfs:x:43:43:X Font Server:/etc/X11/fs:/sbin/nologin = X윈도우 폰트서버
- mailnull:x:47:47::/var/spool/mqueue:/sbin/nologin = 메일 큐
- apache:x:48:48:Apache:/var/www:/sbin/nologin = httpd 사용
- smmsp:x:51:51::/var/spool/mqueue:/sbin/nologin = root가 아닌 smmsp로 메일 발송
- pegasus:x:66:65:tog-pegasus OpenPegasus WBEM/CIM services:/var/lib/Pegasus:/sbin/nologin = System Center Operation Manager가 이기종 환경 관리를 위해 Cross-Platform Extension 제공
- webalizer:x:67:67:Webalizer:/var/www/usage:/sbin/nologin = 웹 로그 분석 프로그램
- haldaemon:x:68:68:HAL daemon:/sbin/nologin = 디바이스 장치 인식 데몬
- vcsa:x:69:69:virtual console memory owner:/dev:/sbin/nologin = 가상메모리 생성 시 계정
- sshd:x:74:74:Privilege-separated SSH:/var/empty/sshd:/sbin/nologin = 보안 셸 계정
- pcap:x:77:77::/var/arpwatch:/sbin/nologin = 패킷 캡처 관련 라이브러리 계정
- dbus:x:81:81:System message bus:/sbin/nologin = 시스템 메시지
- ident:x:98:98::/home/ident:/sbin/nologin = inetd에서 구동되는 데몬
- nobody:x:99:99:Nobody:/sbin/nologin = 익명 연결 (웹 서비스 등 누구나 연결 가능한 서비스 사용 시)
- nfsnobody:x:65534:65534:Anonymous NFS User:/var/lib/nfs:/sbin/nologin

윈도우즈 서버 보안가이드라인

2014. 01



안전행정부 *희망의 새시대*

윈도우즈 서버 취약점 분석·평가 항목

분류	점검항목	항목 중요도	항목코드
1. 계정관리	Administrator 계정 이름 바꾸기	상	W-01
	Guest 계정 상태	상	W-02
	불필요한 계정 제거	상	W-03
	계정 잠금 임계값 설정	상	W-04
	해독 가능한 암호화를 사용하여 암호 저장	상	W-05
	관리자 그룹에 최소한의 사용자 포함	상	W-06
	Everyone 사용 권한을 익명 사용자에게 적용	중	W-07
	계정 잠금 기간 설정	중	W-08
	패스워드 복잡성 설정	중	W-09
	패스워드 최소 암호 길이	중	W-10
	패스워드 최대 사용 기간	중	W-11
	패스워드최소사용기간	중	W-12
	마지막 사용자 이름 표시 안함	중	W-13
	로컬 로그인 허용	중	W-14
	익명 SID/이름 변환 허용	중	W-15
	최근 암호 기억	중	W-16
	콘솔 로그인 시 로컬 계정에서 빈 암호 사용 제한	중	W-17
	원격터미널 접속 가능한 사용자 그룹 제한	중	W-18
2. 서비스 관리	공유 권한 및 사용자 그룹 설정	상	W-19
	하드디스크 기본 공유 제거	상	W-20
	불필요한 서비스 제거	상	W-21
	IIS 서비스 구동 점검	상	W-22
	IIS 디렉토리 리스팅 제거	상	W-23
	IIS CGI 실행 제한	상	W-24
	IIS 상위 디렉토리 접근 금지	상	W-25
	IIS 불필요한 파일 제거	상	W-26
	IIS 웹 프로세스 권한 제한	상	W-27
	IIS 링크 사용금지	상	W-28
	IIS 파일 업로드 및 다운로드 제한	상	W-29
	IIS DB 연결 취약점 점검	상	W-30
	IIS 가상 디렉토리 삭제	상	W-31
	IIS 데이터 파일 ACL 적용	상	W-32
	IIS 미사용 스크립트 매핑 제거	상	W-33
	IIS Exec 명령어 쉘 호출 진단	상	W-34
	IIS WebDAV 비활성화	상	W-35
	NetBIOS 바인딩 서비스 구동 점검	상	W-36
	FTP 서비스 구동 점검	상	W-37
	FTP 디렉토리 접근권한 설정	상	W-38
	Anonymouse FTP 금지	상	W-39
	FTP 접근 제어 설정	상	W-40

	DNS Zone Transfer 설정	상	W-41
	RDS(RemoteDataServices)제거	상	W-42
	터미널 서비스 암호화 수준 설정	중	W-43
	IIS 웹서비스 정보 숨김	중	W-44
	SNMP 서비스 구동 점검	중	W-45
	SNMP 서비스 커뮤니티스트링의 복잡성 설정	중	W-46
	SNMP Access control 설정	중	W-47
	DNS 서비스 구동 점검	중	W-48
	HTTP/FTP/SMTP 배너 차단	하	W-49
	Telnet 보안 설정	중	W-50
	불필요한 ODBC/OLE-DB 데이터 소스와 드라이브 제거	중	W-51
	원격터미널 접속 타임아웃 설정	중	W-52
	예약된 작업에 의심스러운 명령이 등록되어 있는지 점검	중	W-53
3. 패치관리	최신 HOT FIX 적용	상	W-54
	백신 프로그램 업데이트	상	W-55
	정책에 따른 시스템 로깅 설정	중	W-56
4. 로그 관리	로그의 정기적 검토 및 보고	상	W-57
	원격으로 액세스할 수 있는 레지스트리 경로	중	W-58
	정책에 따른 시스템 로깅 설정	중	W-59
	이벤트 로그 관리 설정	하	W-60
	원격에서 이벤트 로그 파일 접근 차단	중	W-61
5. 보안 관리	백신 프로그램 설치	상	W-62
	SAM 파일 접근 통제 설정	상	W-63
	화면보호기설정	상	W-64
	로그온하지 않고 시스템 종료 허용	상	W-65
	원격 시스템에서 강제로 시스템 종료	상	W-66
	보안 감사를 로그할 수 없는 경우 즉시 시스템 종료	상	W-67
	SAM 계정과 공유의 익명 열거 허용 안 함	상	W-68
	Autologon 기능 제어	상	W-69
	이동식 미디어 포맷 및 꺼내기 허용	상	W-70
	디스크볼륨 암호화 설정	상	W-71
	Dos공격 방어 레지스트리 설정	중	W-72
	사용자가 프린터 드라이버를 설치할 수 없게 함	중	W-73
	세션 연결을 중단하기 전에 필요한 유희시간	중	W-74
	경고 메시지 설정	하	W-75
	사용자별 홈 디렉터리 권한 설정	중	W-76
	LAN Manager 인증 수준	중	W-77
	보안 채널 데이터 디지털 암호화 또는 서명	중	W-78
	파일 및 디렉토리 보호	중	W-79
	컴퓨터 계정 암호 최대 사용 기간	중	W-80
	시작프로그램 목록 분석	중	W-81
6. DB관리	Windows 인증 모드 사용	중	W-82

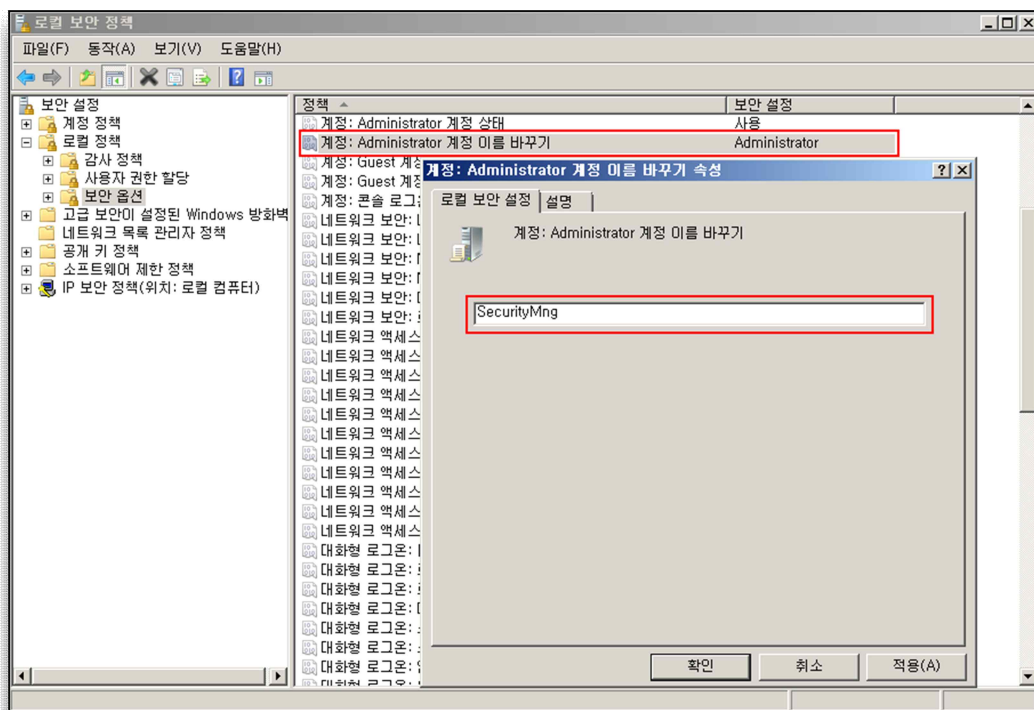
윈도우즈 서버

1. 계정 관리

취약점 항목	1.1. Administrator 계정 이름 바꾸기				
대상 OS	NT, 2000, 2003, 2008	위험도	상	Code	W-01
취약점 개요	일반적으로 관리자 계정을 Administrator로 설정한 경우 로그인 시도 실패 횟수의 제한이 없는 점을 이용해 악의적인 사용자가 패스워드 유추 공격을 계속해서 시도할 수 있음. 관리자 계정의 이름을 변경함으로써 공격자가 패스워드뿐만 아니라 계정 이름을 쉽게 유추하지 못하도록 하여야 함.				
보안대책					
판단기준	양호: Administrator Default 계정 이름을 변경한 경우				
	취약: Administrator Default 계정 이름을 변경하지 않은 경우				
조치방법	Administrator Default 계정 이름 변경				
보안설정방법					

■ Window NT, 2000, 2003, 2008

1. 시작> 프로그램> 제어판> 관리 도구> 로컬 보안 정책> 로컬 정책> 보안 옵션>
2. "계정: Administrator 계정 이름 바꾸기"를 유추하기 어려운 계정 이름으로 변경



조치 시 영향 일반적으로 영향 없음

윈도우즈 서버

취약점 항목	1.2. Guest 계정 상태				
대상 OS	NT, 2000, 2003, 2008	위험도	상	Code	W-02
취약점 개요	Guest 계정은 시스템 임시 접근을 허용하는 취약한 계정으로 사용을 제한하여야 함. 대부분의 시스템은 Guest 계정의 사용이 필요치 않으며, 불특정 다수의 접근이 필요할 경우 Guest 계정이 아닌 일반 사용자 계정을 생성해 사용하도록 하여야 함.				
보안대책					
판단기준	양호: Guest 계정이 비활성화 되어 있는 경우				
	취약: Guest 계정이 활성화 되어 있는 경우				
조치방법	Guest 계정 비활성화				
보안설정방법					

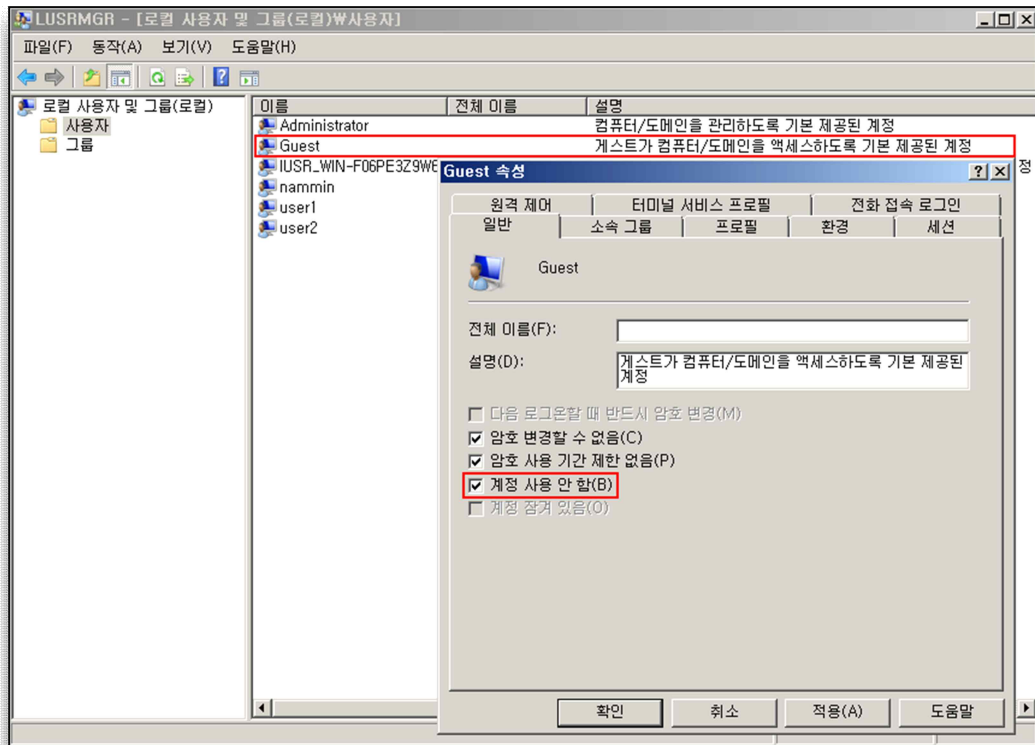
■ Window NT

1. 시작> 프로그램> 관리 도구> 도메인 사용자 관리> Guest 계정 선택> 등록 정보
2. "계정 사용 안 함"에 체크

■ Window 2000, 2003, 2008

1. 시작> 실행> LUSRMGR.MSC> 사용자> Guest> 속성
2. "계정 사용 안 함"에 체크

윈도우즈 서버



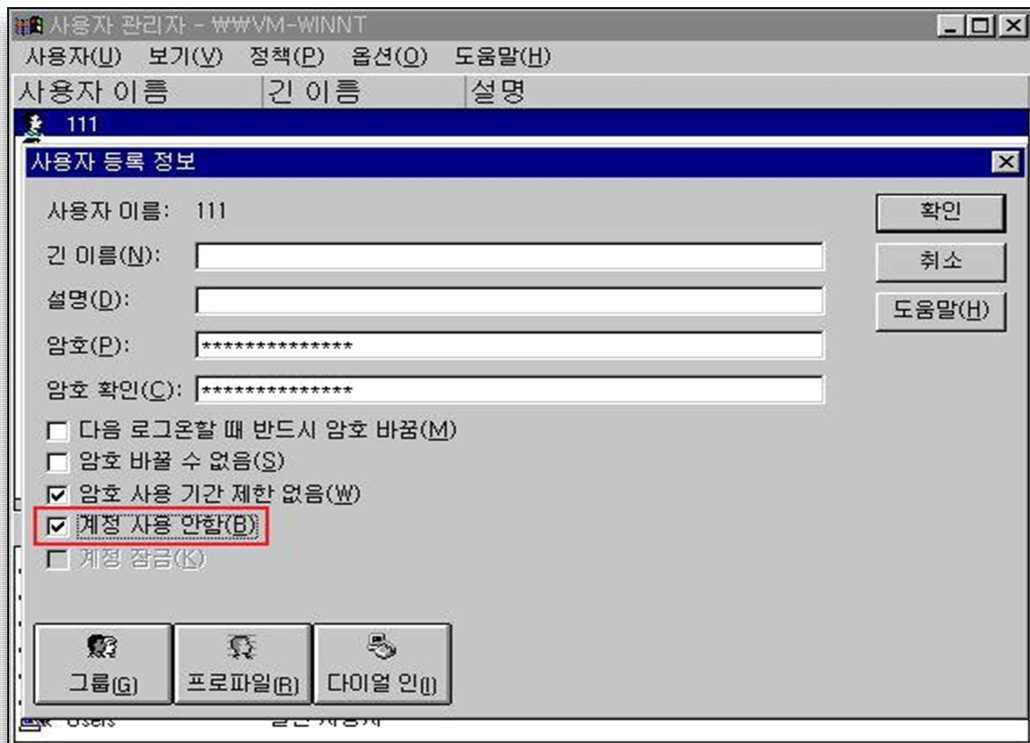
조치 시 영향 | 일반적으로 영향 없음

윈도우즈 서버

취약점 항목	1.3. 불필요한 계정 제거				
대상 OS	NT, 2000, 2003, 2008	위험도	상	Code	W-03
취약점 개요	퇴직, 전직, 휴직 등의 이유로 더 이상 사용하지 않는 계정, 불필요한 계정, 의심스러운 계정이 존재하는지 점검함. 관리되지 않은 불필요한 계정은 장기간 패스워드가 변경되지 않아 *무작위 대입 공격(Brute Force Attack)이나 패스워드 추측 공격>Password Guessing)에 의해 계정 정보가 유출되어도 인지하기 어려움.				
	*무작위 대입 공격(Brute Force Attack): 컴퓨터로 암호를 해독하기 위해 가능한 모든 키를 하나하나 추론해 보는 시도를 말함.				
보안대책					
판단기준	양호: 불필요한 계정이 존재하지 않는 경우				
	취약: 불필요한 계정이 존재하는 경우				
조치방법	현재 계정 현황 확인 후 불필요한 계정 삭제				
보안설정방법					

■ Window NT

- 시작> 프로그램> 관리 도구> 도메인 사용자 관리> 계정 선택> 등록 정보
- "계정 사용 안함"에 체크하거나 계정 삭제

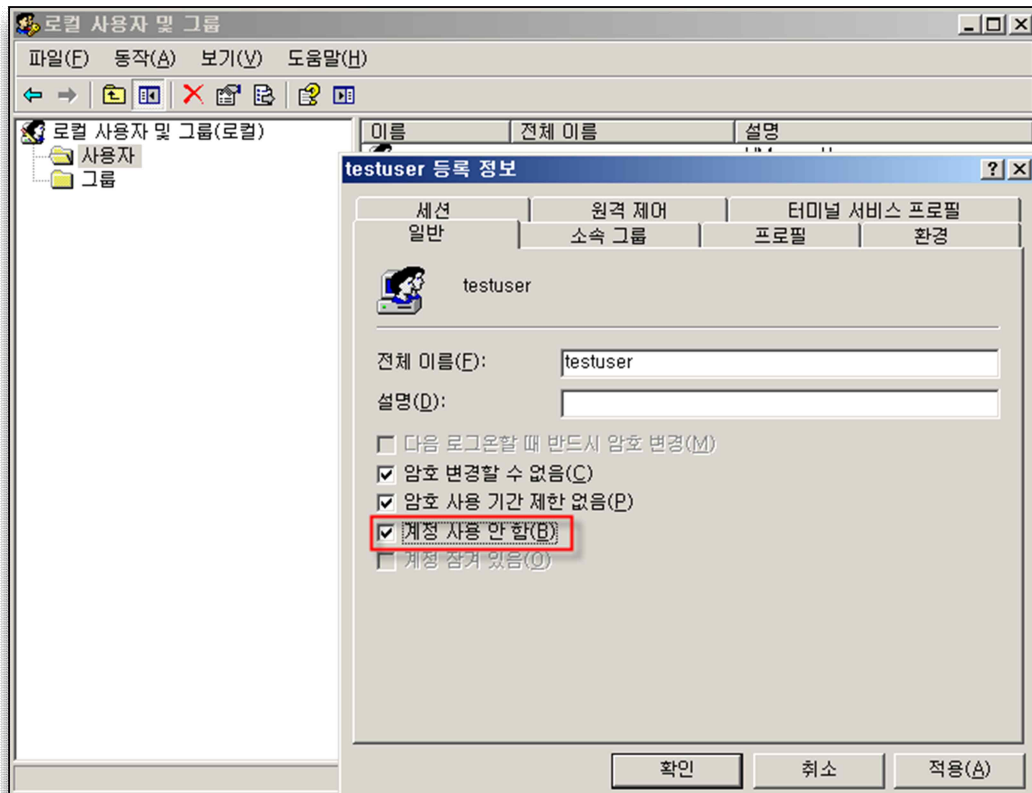


■ Window 2000, 2003, 2008

- 시작> 실행> LUSRMGR.MSC> 사용자> "불필요한 사용자" 선택> 속성

윈도우즈 서버

2. “계정 사용 안 함”에 체크하거나 계정 삭제



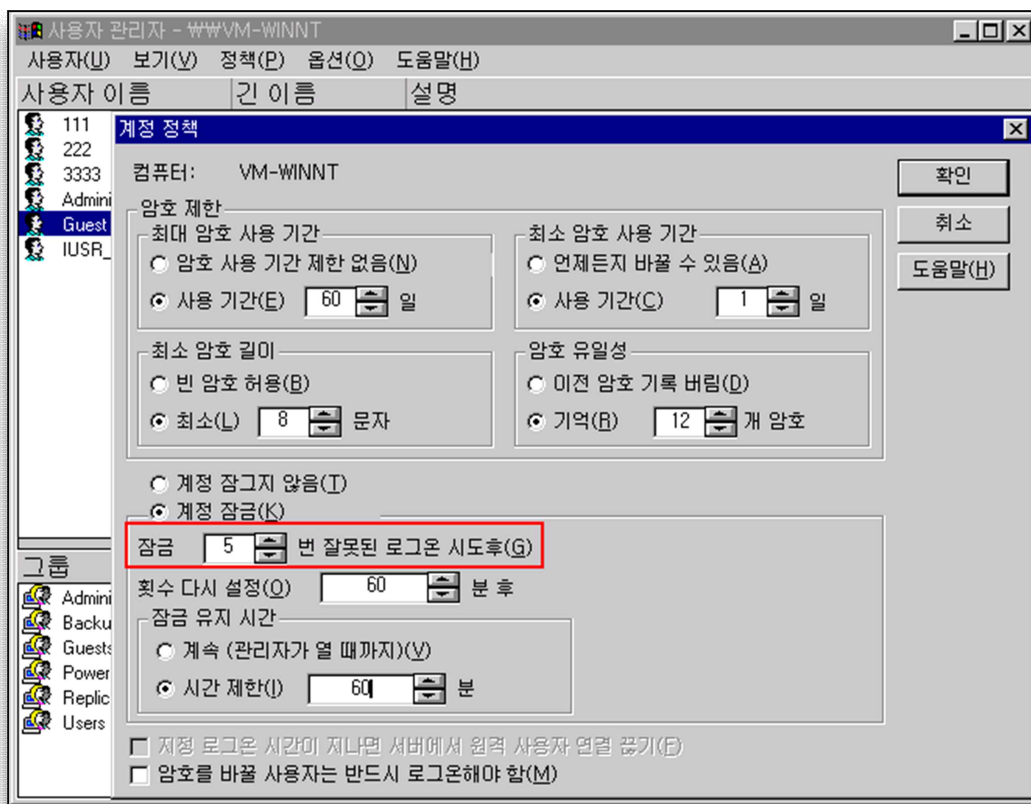
조치 시 영향 | 계정의 사용여부를 파악하여 사용하지 않는 계정일 경우 제거

윈도즈 서버

취약점 항목	1.4. 계정 잠금 임계값 설정				
대상 OS	NT, 2000, 2003, 2008	위험도	상	Code	W-04
취약점 개요	자동화된 방법을 이용하여 공격자는 모든 사용자 계정에 대해 암호조합 공격을 시도할 수 있으므로 계정 잠금 임계값 설정을 적용하여 로그인 실패 횟수를 제한하여야 함.				
보안대책					
판단기준	양호: 계정 잠금 임계값이 5 이하의 값으로 설정되어 있는 경우				
	취약: 계정 잠금 임계값이 5 이하의 값으로 설정되어 있지 않은 경우				
조치방법	계정 잠금 임계값을 5번 이하의 값으로 설정				
보안설정방법					

■ Window NT

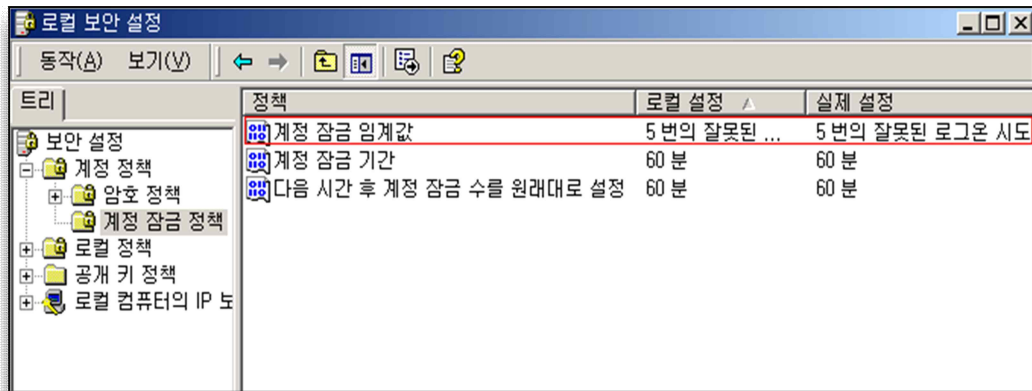
- 시작> 프로그램> 관리 도구> 도메인 사용자 관리자> 정책> 계정 정책
- “계정 잠금” 선택 후 “잠금”에 “5” 이하의 값 설정



■ Window 2000, 2003, 2008

- 시작> 실행> SECPOL.MSC> 계정 정책> 계정 잠금 정책
- “계정 잠금 임계값”을 “5” 이하의 값으로 설정

윈도우즈 서버



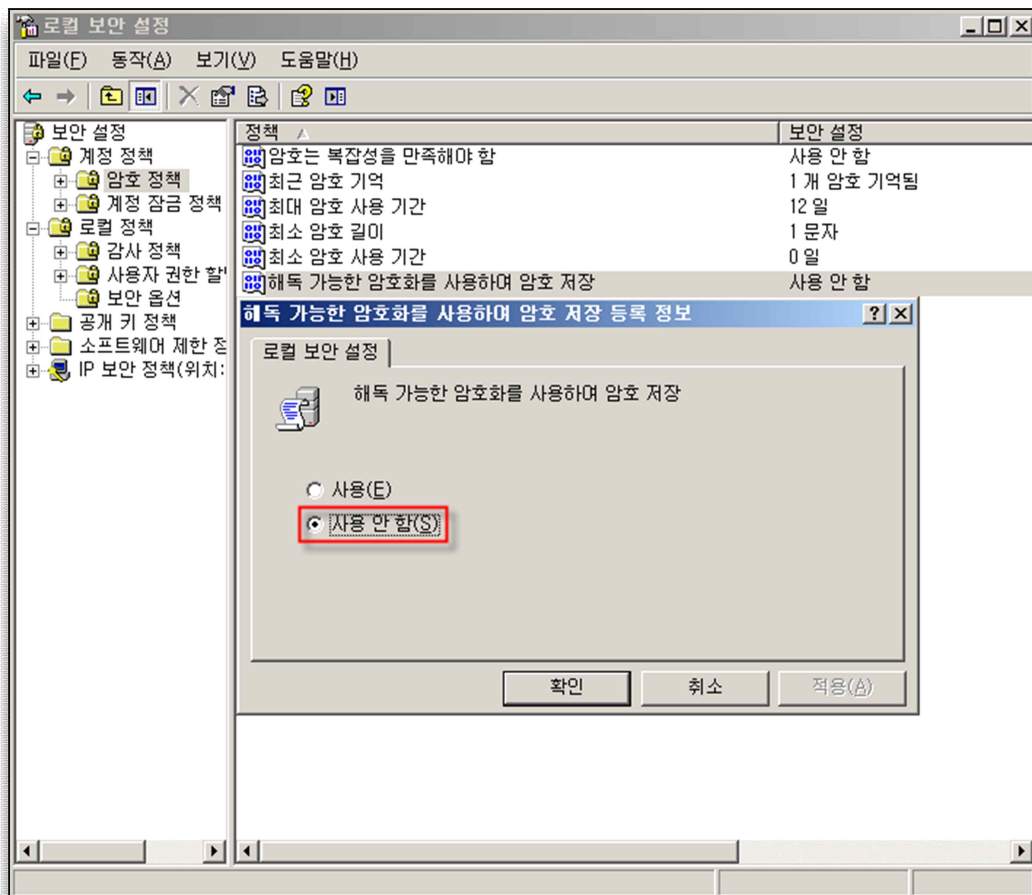
조치 시 영향 Administrator 계정은 잠기지 않으며, 일반 계정의 경우 5번 패스워드 입력 실패 시 잠김

윈도우즈 서버

취약점 항목	1.5. 해독 가능한 암호화를 사용하여 암호 저장				
대상 OS	NT, 2000, 2003, 2008	위험도	상	Code	W-05
취약점 개요	인증을 위해 사용자 암호를 알아야 하는 응용 프로그램 프로토콜이 지원될 경우 해독 가능한 방식으로 암호를 저장하기 때문에 암호공격을 이용한 공격자가 노출된 계정을 사용하여 네트워크 리소스에 로그인할 수 있음.				
보안대책					
판단기준	양호: "해독 가능한 암호화를 사용하여 암호 저장" 정책이 "사용 안 함" 으로 되어 있는 경우				
	취약: "해독 가능한 암호화를 사용하여 암호 저장" 정책이 "사용" 으로 되어 있는 경우				
조치방법	"해독 가능한 암호화를 사용하여 암호 저장"을 "사용 안 함"으로 설정				
보안설정방법					

■ Windows NT, 2000, 2003, 2008

1. 시작> 실행> SECPOL.MSC> 계정 정책> 암호 정책
2. "해독 가능한 암호화를 사용하여 암호 저장"을 "사용 안 함" 으로 설정



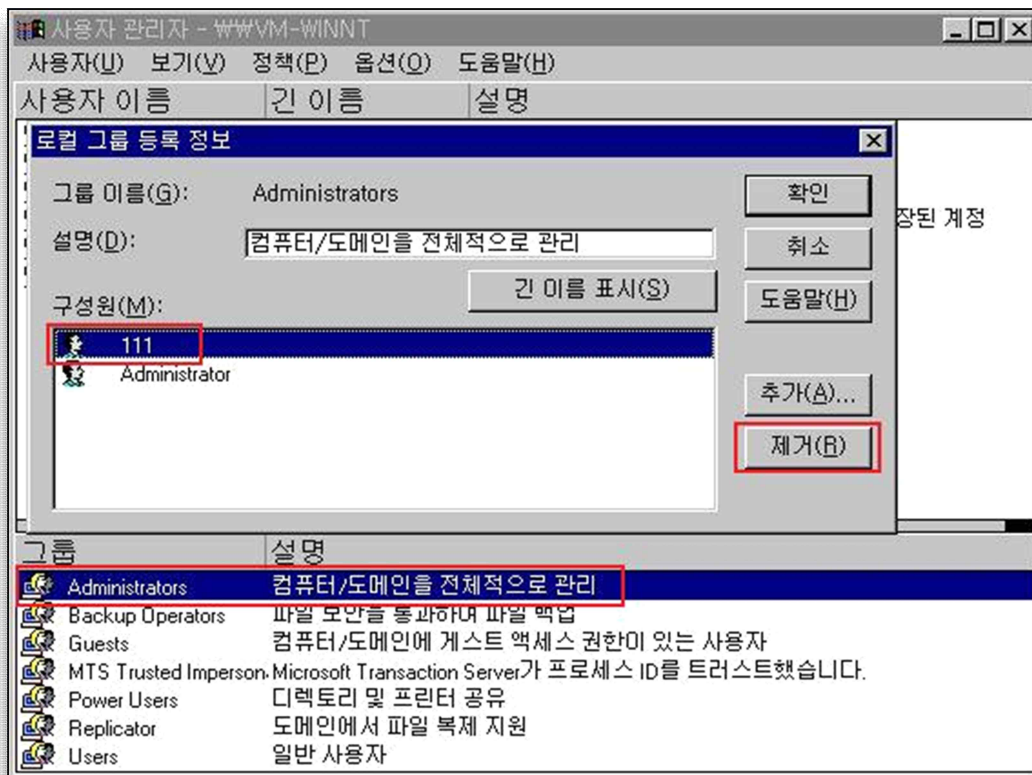
조치 시 영향 | 일반적으로 영향 없음

윈도우즈 서버

취약점 항목	1.6. 관리자 그룹에 최소한의 사용자 포함				
대상 OS	NT, 2000, 2003, 2008	위험도	상	Code	W-06
취약점 개요	일반 사용자 권한으로부터 받을 수 있는 시스템 피해를 줄이기 위해서 관리 업무를 위한 계정과 일반 업무를 위한 계정을 분리하여 사용하는 것이 바람직함. 시스템 관리를 위해서는 각각 두 개의 계정을 가져야 하며 관리자 그룹에는 가능한 최소한의 사용자만 포함하도록 하여야 함.				
보안대책					
판단기준	양호: Administrators 그룹에 불필요한 관리자 계정이 존재하지 않는 경우				
	취약: Administrators 그룹에 불필요한 관리자 계정이 존재하는 경우				
조치방법	Administrators 그룹에 포함된 불필요한 계정 제거				
보안설정방법					

■ Windows NT

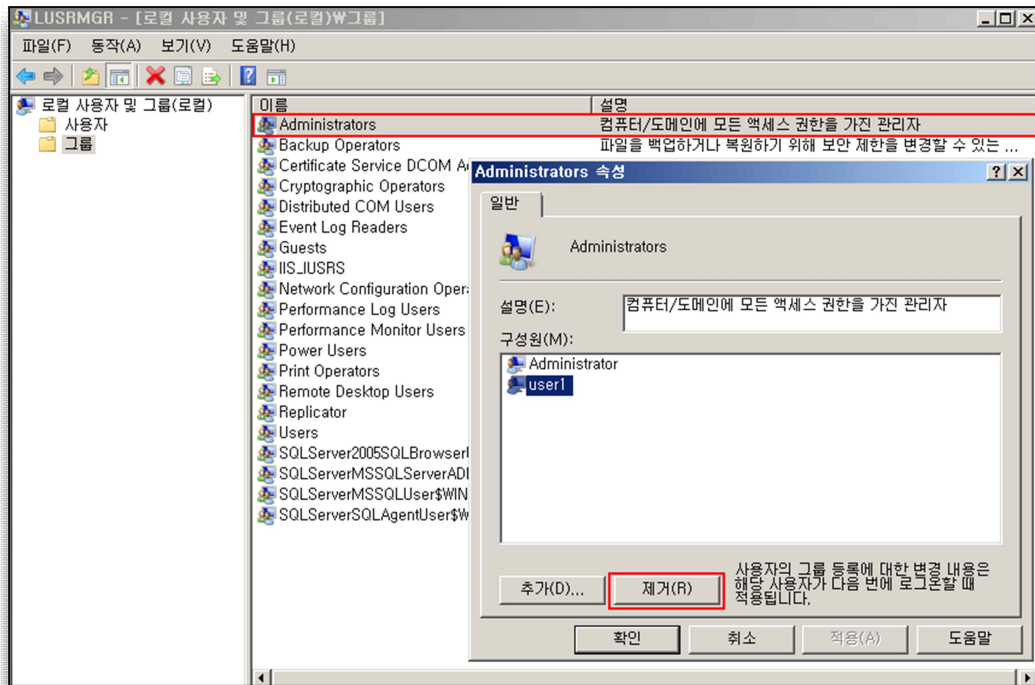
1. 시작> 프로그램> 관리 도구> 도메인 사용자 관리> Administrators 그룹> 등록 정보
2. Administrator 그룹에서 불필요한 계정 제거 후 그룹 변경



■ Windows 2000, 2003, 2008

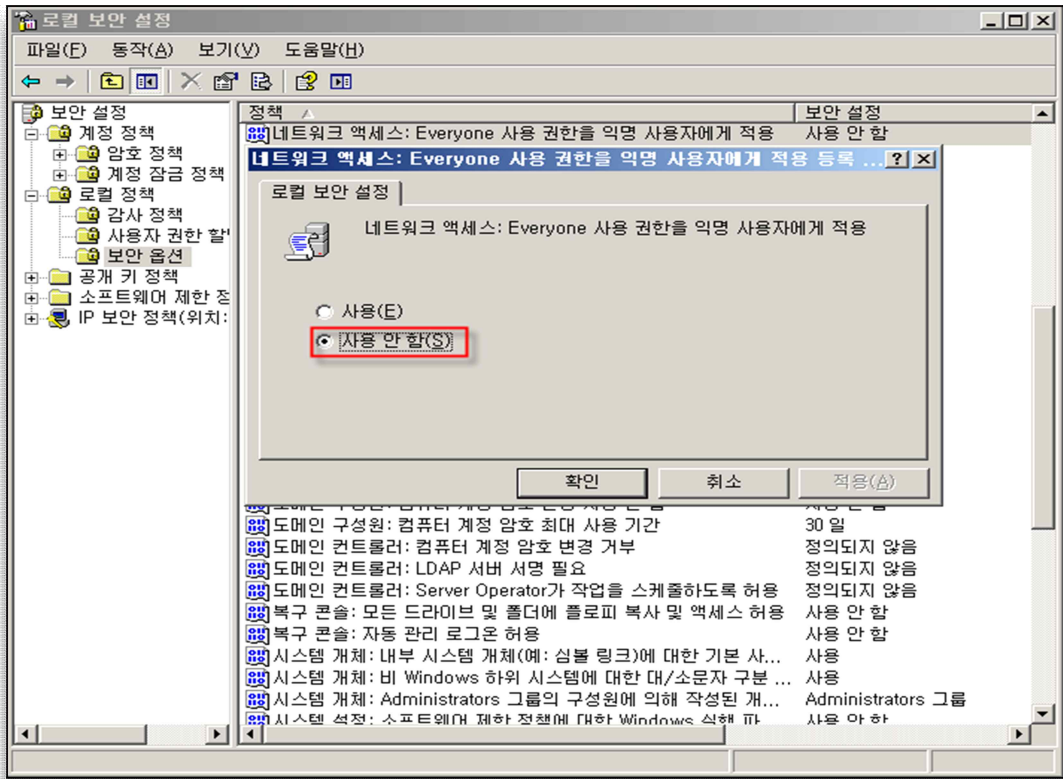
1. 시작> 실행> LUSRMGR.MSC> 그룹> Administrators> 속성
2. Administrators 그룹에서 불필요한 계정 제거 후 그룹 변경

윈도우즈 서버



조치 시 영향 Administrators 권한이 필요 없을 경우 변경 시 영향 없음

윈도우즈 서버

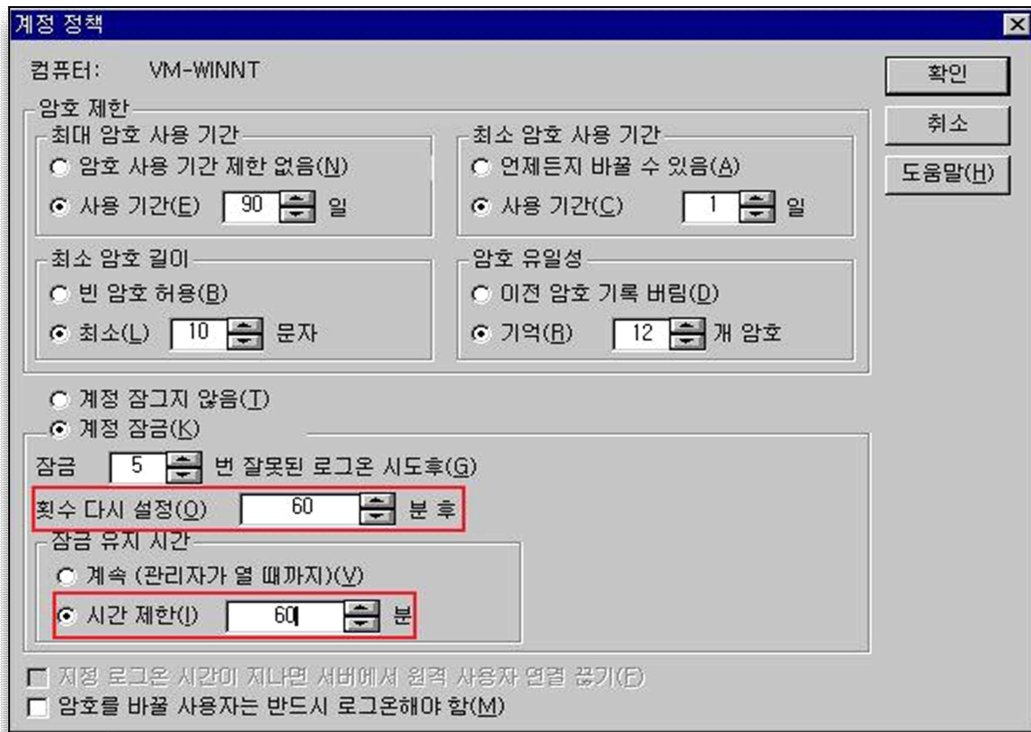
취약점 항목	1.7. Everyone 사용 권한을 익명 사용자에게 적용				
대상 OS	2003, 2008	위험도	중	Code	W-07
취약점 개요	익명 사용자가 Everyone 그룹으로 사용 권한을 준 모든 리소스에 접근할지를 결정함. 만약 "사용"으로 설정할 경우 권한이 없는 사용자가 익명으로 계정 이름 및 공유 리소스를 나열하고 이 정보를 사용하여 암호를 추측하거나 *DoS(Denial of Service) 공격을 실행할 수 있음. *DoS(Denial of Service): 관리자 권한 없이도 특정서버에 처리할 수 없을 정도로 대량의 접속 신호를 한꺼번에 보내 해당 서버가 마비되도록 하는 해킹 기법임.				
보안대책					
판단기준	양호: "Everyone 사용 권한을 익명 사용자에게 적용" 정책이 "사용 안 함" 으로 되어 있는 경우 취약: "Everyone 사용 권한을 익명 사용자에게 적용" 정책이 "사용" 으로 되어 있는 경우				
조치방법	네트워크 액세스 : Everyone 사용 권한을 익명 사용자에게 적용 -> 사용 안 함				
보안설정방법					
■ Windows 2003, 2008 - 시작> 실행> SECPOL.MSC> 로컬 정책> 보안 옵션 "Everyone 사용 권한을 익명 사용자에게 적용" 정책이 "사용 안 함" 으로 설정					
 The screenshot shows the 'Local Security Policy' window. In the left-hand tree, 'Security Options' is expanded. The right pane displays the policy 'Network Access: Everyone use permissions for anonymous users'. The policy is currently set to 'Do not use' (사용 안 함), which is highlighted with a red box. Other policies listed below include 'Domain member: Manage machine account expiration', 'Domain member: Restrict anonymous access to Named Pipes and SMB', etc.					
조치 시 영향	애플리케이션이나 Backup 용도로 Everyone 공유를 사용하지 않는지 확인 필요				

윈도우즈 서버

취약점 항목	1.8. 계정 잠금 기간 설정				
대상 OS	NT, 2000, 2003, 2008	위험도	중	Code	W-08
취약점 개요	계정 잠금 기간 설정을 사용하면 지정한 기간 동안 잠긴 계정은 사용할 수 없으며, 계정 잠금이 해제될 때까지 접근할 수 없음. 따라서 공격자가 자동으로 암호를 추측하는 것이 어렵게 되어 암호공격 효과를 낮출 수 있음.				
보안대책					
판단기준	양호: "계정 잠금 기간" 및 "계정 잠금 기간 원래대로 설정 기간"이 설정되어 있는 경우 ※ 60분 이상의 값으로 설정하기를 권고함				
	취약: "계정 잠금 기간" 및 "잠금 기간 원래대로 설정 기간"이 설정되지 않은 경우				
조치방법	"계정 잠금 기간" 및 "잠금 기간 원래대로 설정 기간" 60분 설정				
보안설정방법					

■ Windows NT

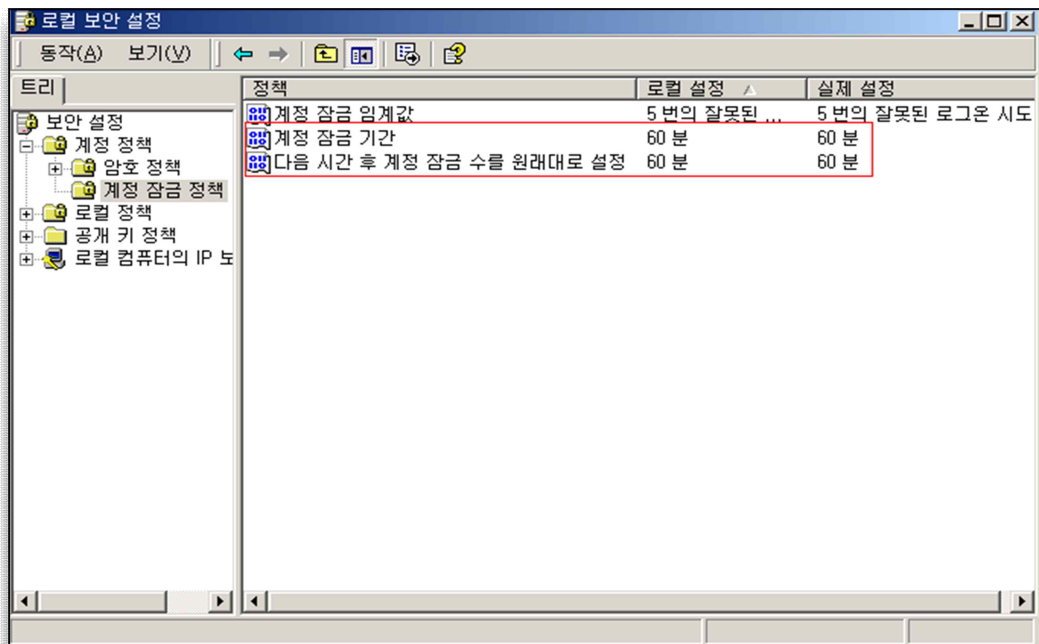
1. 시작> 프로그램> 관리 도구> 도메인 사용자 관리자> 정책> 계정 정책
2. "횟수 다시 설정"을 "60분 후"로 설정, "잠금 유지 시간"의 "시간 제한"을 "60분"으로 설정



■ Windows 2000, 2003, 2008

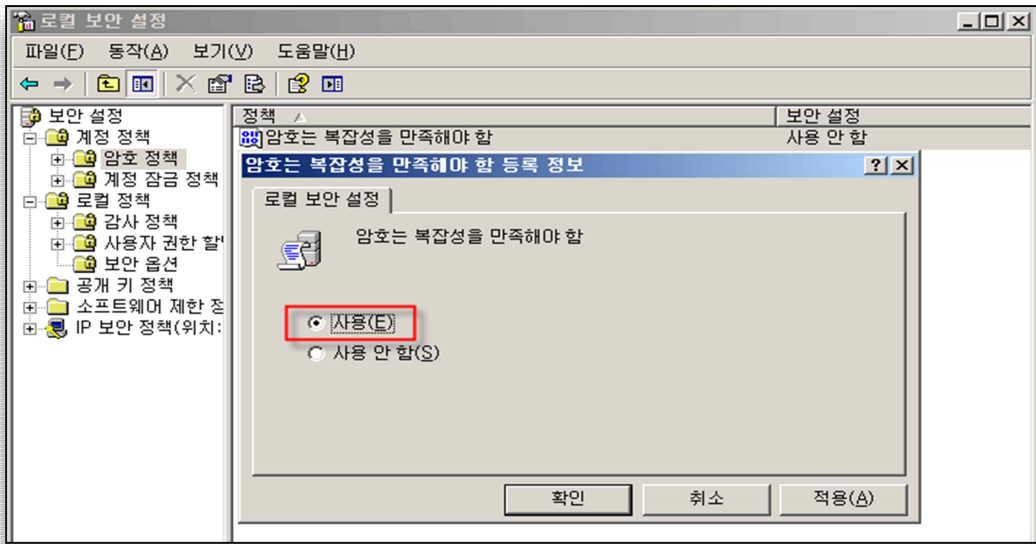
1. 시작> 실행> SECPOL.MSC> 계정 정책> 계정 잠금 정책
2. "계정 잠금 기간", "다음 시간 후 계정 잠금 수를 원래대로 설정"에 대해 각각 "60분" 설정

윈도우즈 서버



조치 시 영향 | 일반적으로 영향 없음

윈도우즈 서버

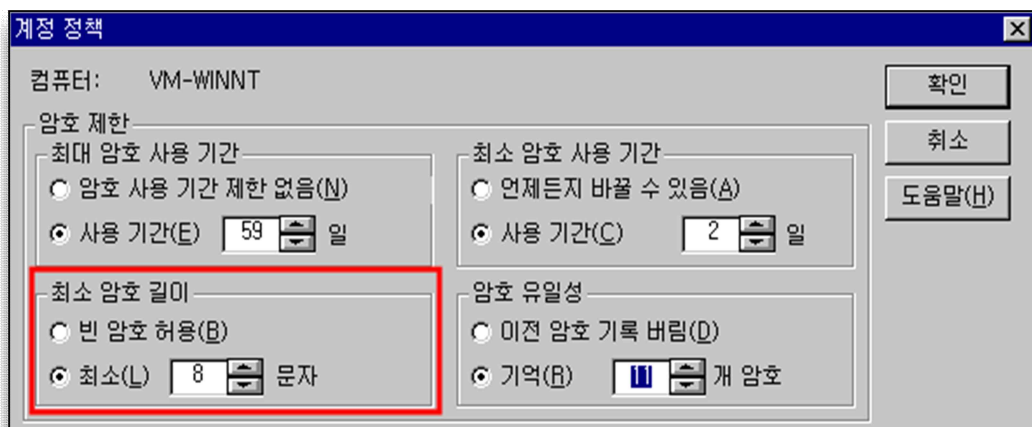
취약점 항목	1.9. 패스워드 복잡성 설정				
대상 OS	NT, 2000, 2003, 2008	위험도	중	Code	W-09
취약점 개요	패스워드 설정 시 문자/숫자/특수문자를 모두 포함하여 강력한 패스워드가 설정될 수 있도록 암호 복잡성을 설정하여야 함. 영·숫자만으로 이루어진 암호는 현재 공개된 패스워드 크랙 유틸리티에 의해 쉽게 유추할 수 있으므로 패스워드 조합 및 길이에 따라 최소 암호 길이 및 암호 복잡성을 적절하게 설정하여 패스워드를 알아낼 수 있는 평균 시간을 증가시킬 수 있도록 설정하여야 함.				
보안대책					
판단기준	양호: "암호는 복잡성을 만족해야 함" 정책이 "사용" 으로 되어 있는 경우				
	취약: "암호는 복잡성을 만족해야 함" 정책이 "사용 안 함" 으로 되어 있는 경우				
조치방법	암호는 복잡성을 만족해야 함 → 사용				
보안설정방법					
■ Windows NT, 2000, 2003, 2008 - 시작> 실행> SECPOL.MSC> 계정 정책> 암호 정책 "암호는 복잡성을 만족해야 함"을 "사용" 으로 설정					
					
※ 이 정책 설정은 암호를 변경하거나 새로운 암호 생성 시 아래와 같은 일련의 규정을 만족하는지 결정함 다음 각 목의 문자 종류 중 2종류 이상을 조합하여 최소 10자리 이상 또는, 3종류 이상을 조합하여 최소 8자리 이상의 길이로 구성 가. 영문 대문자(26개) 나. 영문 소문자(26개) 다. 숫자(10개) 라. 특수문자(32개)					
조치 시 영향	일반적으로 영향 없음				

윈도우즈 서버

취약점 항목	1.10. 패스워드 최소 암호 길이				
대상 OS	NT, 2000, 2003, 2008	위험도	중	Code	W-10
취약점 개요	일반적인 단어와 구를 이용해 취약하게 암호를 설정한 계정은 사전 공격과 가능한 모든 문자의 조합을 시도하는 무작위 공격을 통해 권한이 도용당할 수 있음. 최소 암호 길이를 8자리로 설정하면 대부분 환경에서 적절한 보안이 제공될 뿐만 아니라 사용자가 쉽게 기억할 수 있으며 무작위 공격을 방어할 수 있음.				
보안대책					
판단기준	양호: 최소 암호 길이가 8문자 이상으로 설정되어 있는 경우				
	취약: 최소 암호 길이가 설정되지 않았거나 8문자 미만으로 설정되어 있는 경우				
조치방법	최소 암호 길이 8문자 이상으로 설정				
보안설정방법					

■ Windows NT

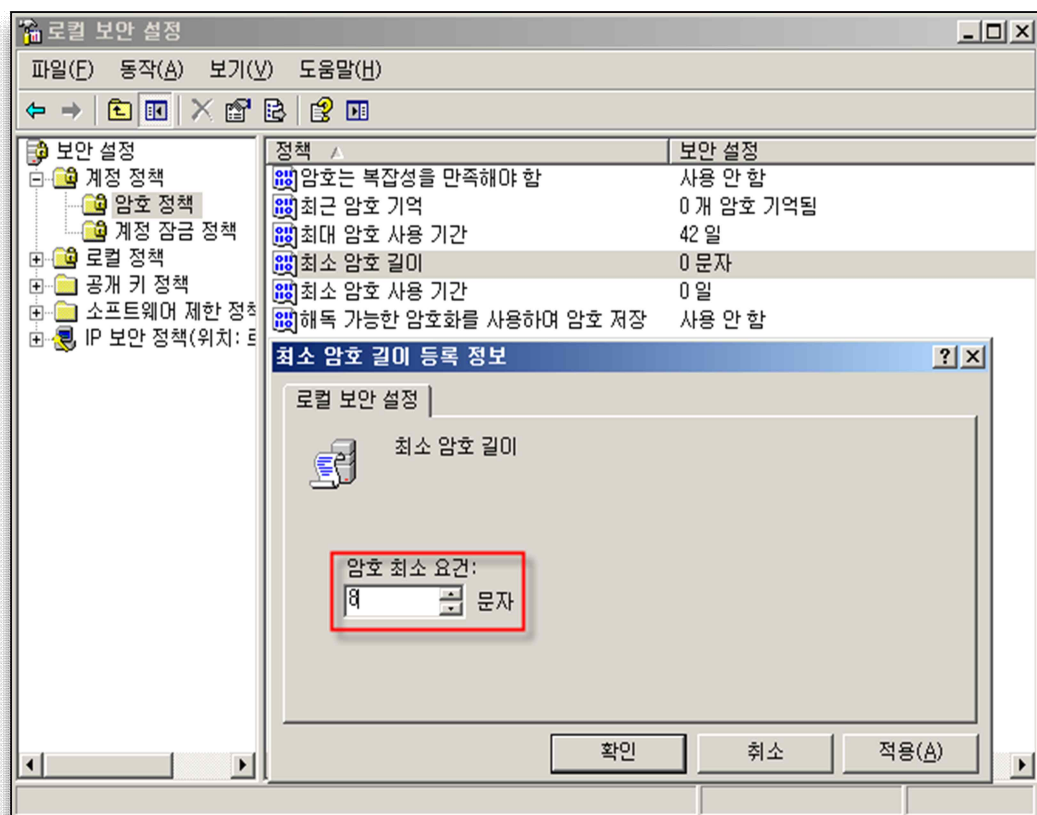
1. 시작> 프로그램> 관리 도구> 도메인 사용자 관리자> 정책> 계정 정책
2. "최소 암호 길이"에 "최소"를 "8문자"로 설정



■ Windows 2000, 2003, 2008

1. 시작> 실행> SECPOL.MSC> 암호 정책
2. "최소 암호 길이"를 "8문자"로 설정

윈도우즈 서버



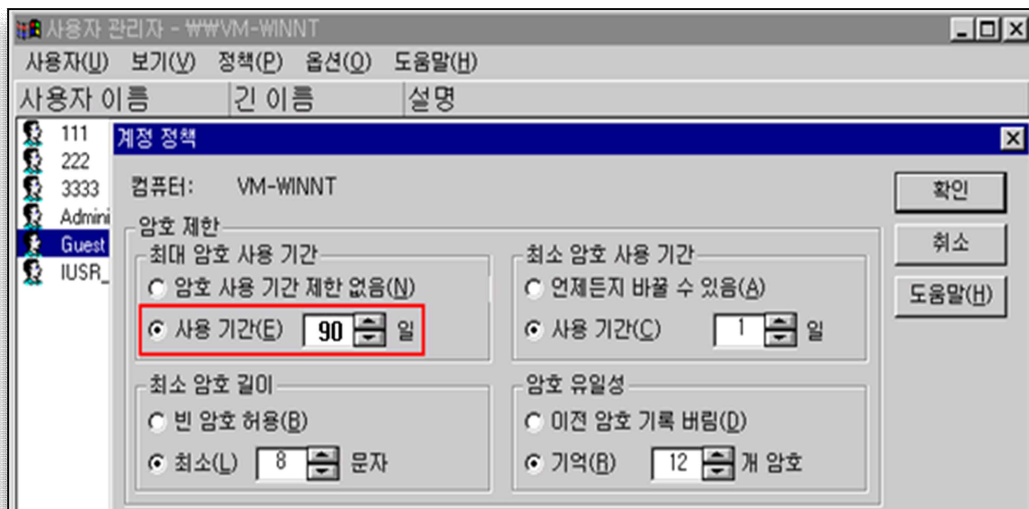
조치 시 영향 다음 패스워드 변경 시 8자 이상의 패스워드를 설정하여야 함

윈도즈 서버

취약점 항목	1.11. 패스워드 최대 사용 기간				
대상 OS	NT, 2000, 2003, 2008	위험도	중	Code	W-11
취약점 개요	가장 복잡한 암호를 포함한 모든 암호는 추측 공격에 의해 유출될 수 있으므로 패스워드가 일정 기간이 지나도 유효하다면 침해 발생 가능성이 있음. 사용자가 암호를 자주 바꾸도록 하면 유효한 암호가 공격당하는 위험을 줄일 뿐만 아니라 누군가가 불법으로 획득한 암호를 사용하여 무단 로그인하는 경우를 줄일 수 있음.				
보안대책					
판단기준	양호: 최대 암호 사용 기간이 90일 이하로 설정되어 있는 경우				
	취약: 최대 암호 사용 기간이 설정되지 않았거나 90일을 초과하는 값으로 설정된 경우				
조치방법	최대 암호 사용 기간 90일 설정				
보안설정방법					

■ Windows NT

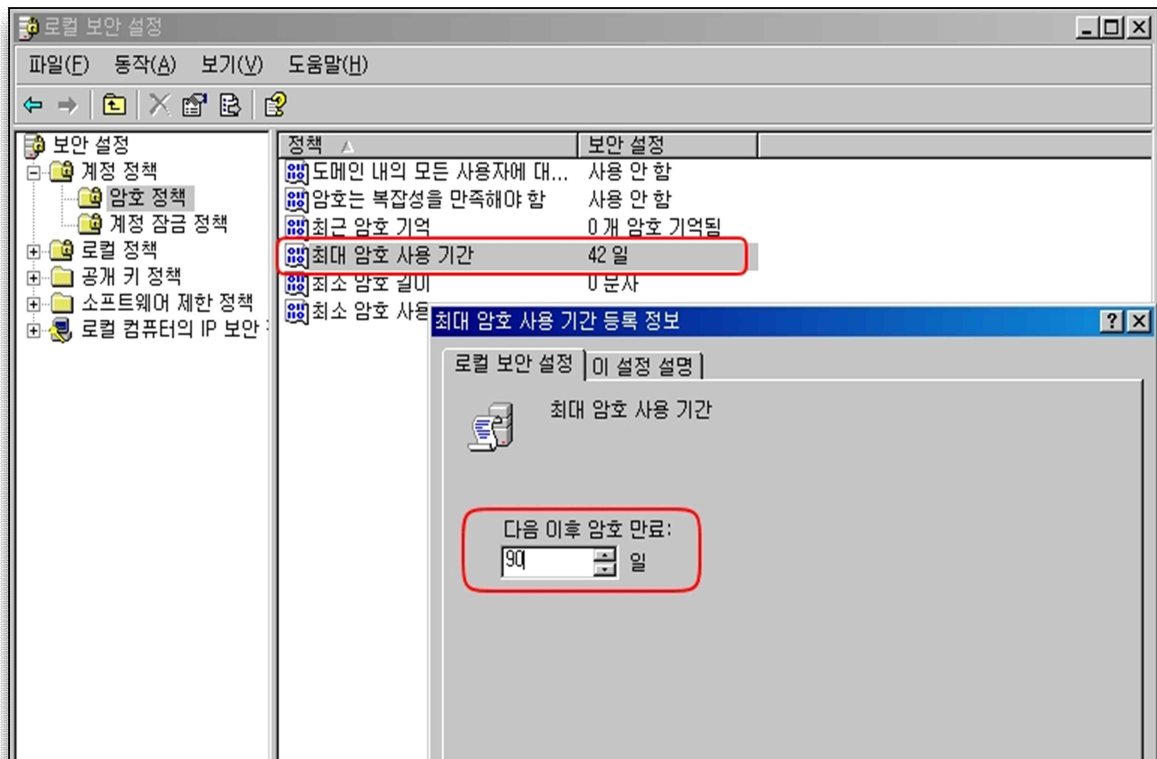
1. 시작> 프로그램> 관리 도구> 도메인 사용자 관리자> 정책> 계정
2. "최대 암호 사용 기간"의 "사용 기간"을 "90일"로 설정



■ Windows 2000, 2003, 2008

1. 시작> 실행> SECPOL.MSC> 암호 정책
2. "최대 암호 사용 기간"의 다음 이후 암호 만료 기간을 "90일"로 설정

윈도우즈 서버



조치 시 영향

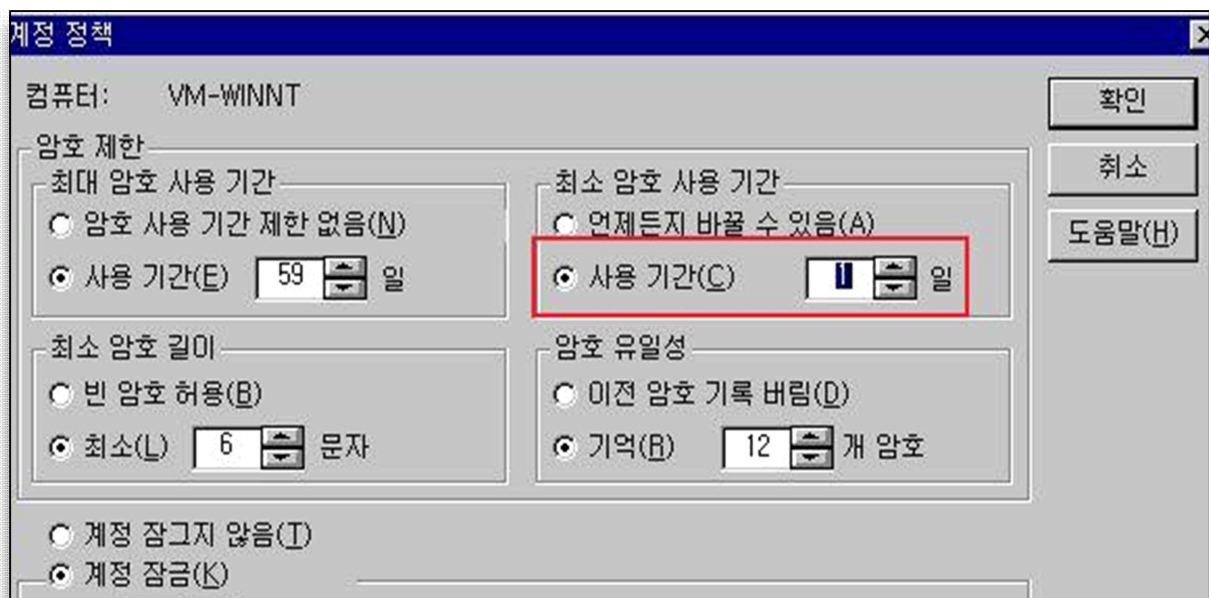
암호 사용기간이 90일로 설정되며 90일 주기로 패스워드를 변경하여야 함
패스워드 사용기간 만료 전 패스워드 변경을 위한 경고 메시지 제공을 권고함

윈도우즈 서버

취약점 항목	1.12. 패스워드 최소 사용 기간				
대상 OS	NT, 2000, 2003, 2008	위험도	중	Code	W-12
취약점 개요	패스워드 변경에 시간적 제약이 없다면 이전에 즐겨 사용하던 암호를 다시 사용할 수 있으므로 주기적으로 패스워드를 변경하는 정책의 효과가 없어짐. 최소 암호 사용 기간 정책 설정을 0보다 큰 값으로 구성하면 최근 암호 기억 설정을 유효하게 사용함으로써 이전 암호를 다시 사용하는 것을 막을 수 있음.				
보안대책					
판단기준	양호: 최소 암호 사용 기간이 0보다 큰 값으로 설정되어 있는 경우				
	취약: 최소 암호 사용 기간이 0으로 설정되어 있는 경우				
조치방법	최소 암호 사용 기간 1일 설정				
보안설정방법					

■ Windows NT

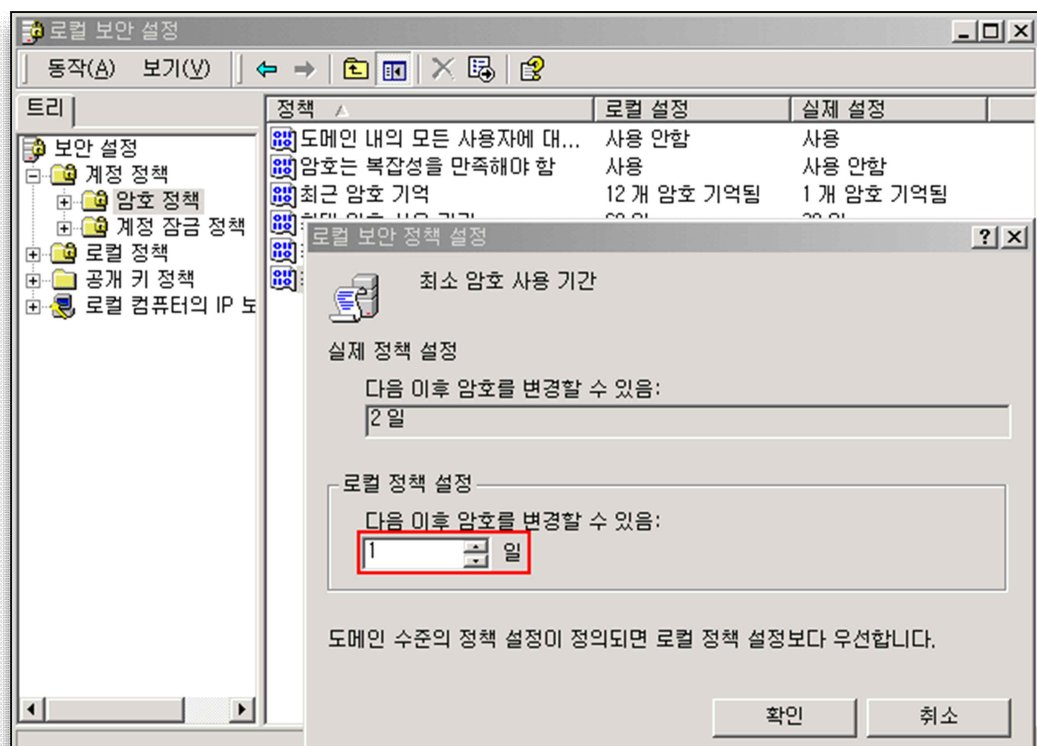
1. 시작> 프로그램> 관리 도구> 도메인 사용자 관리자> 정책> 계정
2. "최소 암호 사용 기간"에서 "사용 기간" "1일"로 설정



■ Windows 2000, 2003, 2008

1. 시작> 실행> SECPOL.MSC> 암호 정책
2. "최소 암호 사용 기간"을 "1일"로 설정

윈도우즈 서버



조치 시 영향 패스워드를 변경 후 다시 변경하기 위해서는 1일이 지나야 하며, 일반적으로 영향 없음

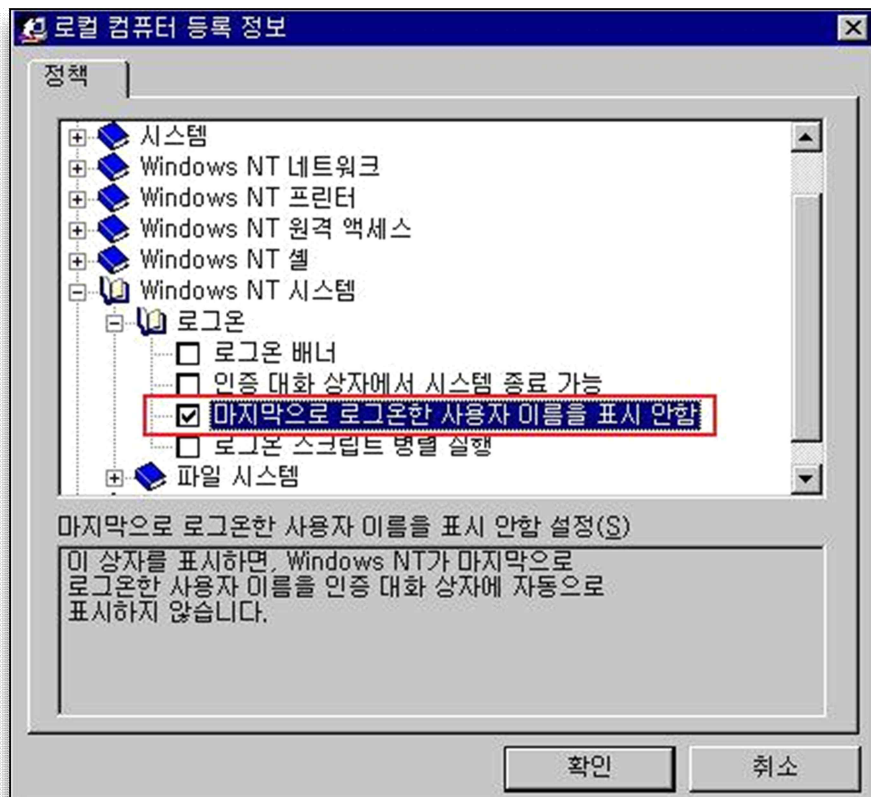
윈도우즈 서버

취약점 항목	1.13. 마지막 사용자 이름 표시 안함				
대상 OS	NT, 2000, 2003, 2008	위험도	중	Code	W-13
취약점 개요	마지막으로 로그인한 사용자의 이름이 로그인 대화 상자에 표시될 경우 공격자는 이를 획득하여 암호를 추측하거나 무작위 공격을 시도할 수 있음. 실제로 콘솔에 접근할 수 있는 사용자 또는, 터미널 서비스를 통해 서버에 연결할 수 있는 사용자들에게 쉽게 노출될 수 있으므로 사용자 이름이 표시되지 않도록 설정하여야 함.				
보안대책					
판단기준	양호: "마지막 사용자 이름 표시 안 함"이 "사용"으로 설정되어 있는 경우				
	취약: "마지막 사용자 이름 표시 안 함"이 "사용 안 함"으로 설정되어 있는 경우				
조치방법	Windows NT: 마지막으로 로그인한 사용자 이름 표시 안 함 → 설정 후 저장 Windows 2000: 로그인 스크린에 마지막 사용자 이름 표시 안 함 → 사용 Windows 2003, 2008: 대화형 로그인: 마지막 사용자 이름 표시 안 함 → 사용				

보안설정방법

■ Windows NT

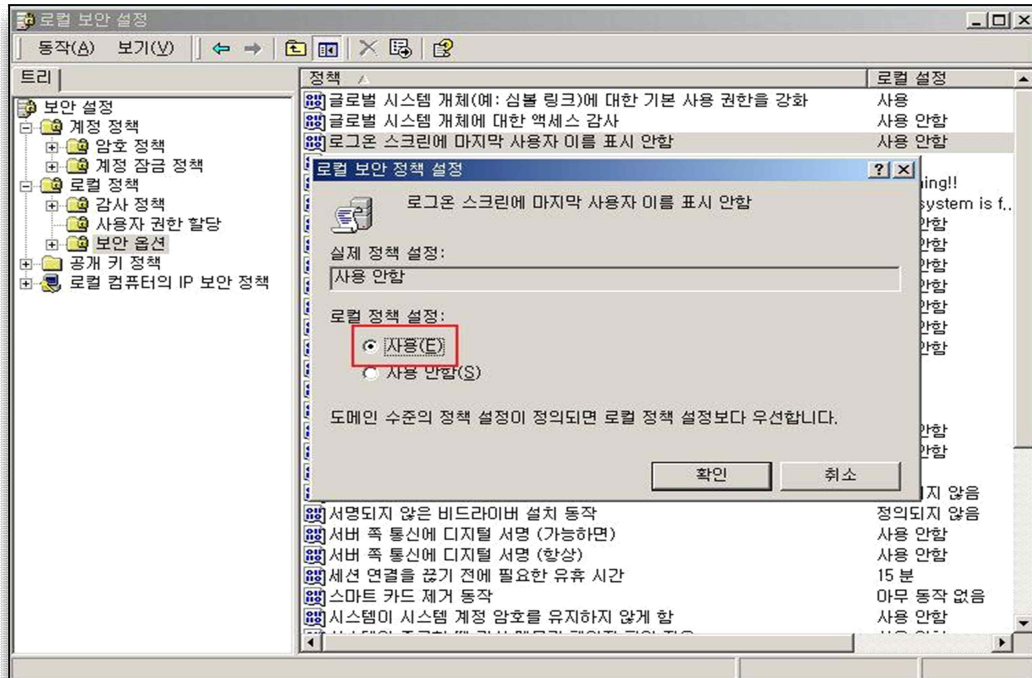
1. 시작> 프로그램> 관리 도구> 시스템 정책 편집기> 파일> 레지스트리 열기> 로컬 컴퓨터> 편집> 등록 정보> Windows NT 시스템> 로그인> “마지막으로 로그인한 사용자 이름 표시 안함”을 설정 후 저장



윈도우즈 서버

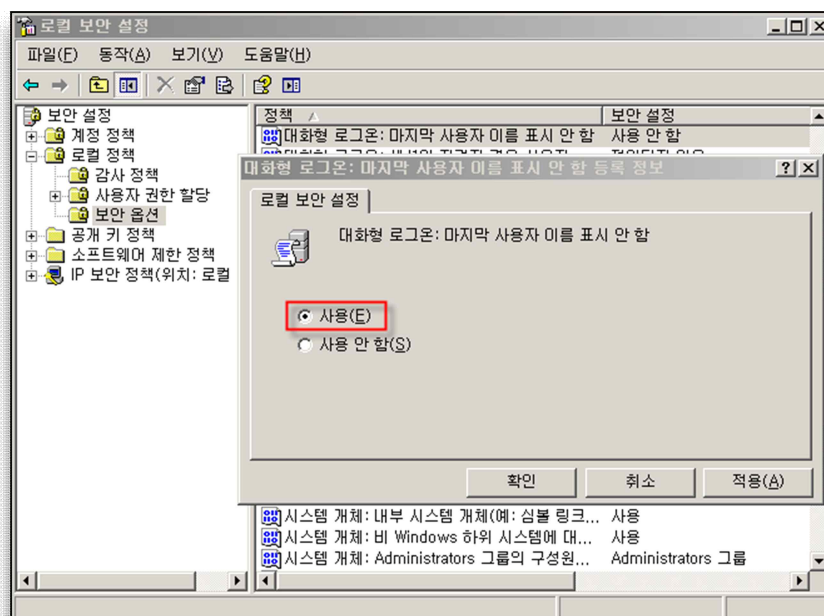
■ Windows 2000

1. 시작> 실행> SECPOL.MSC> 로컬 정책> 보안 옵션
2. "로그온 스크린에 마지막 사용자 이름 표시 안 함"을 "사용"으로 설정



■ Windows 2003, 2008

1. 시작> 실행> SECPOL.MSC> 로컬 정책> 보안 옵션
2. "대화형 로그온: 마지막 사용자 이름 표시 안 함"을 "사용"으로 설정



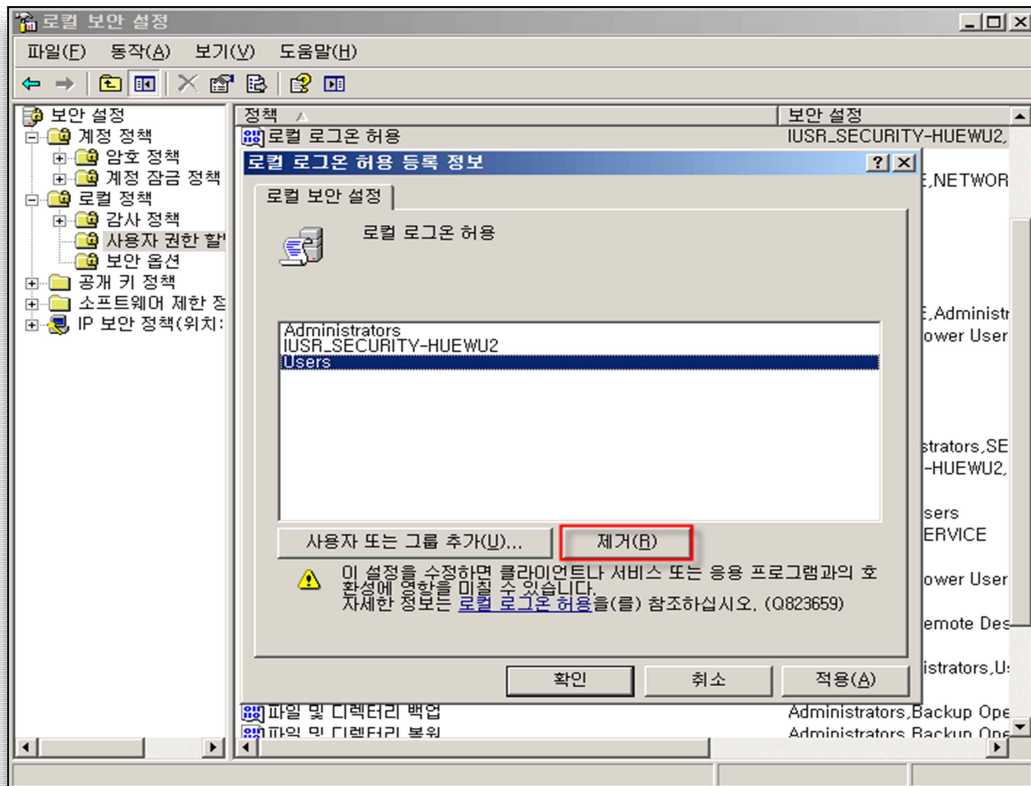
조치 시 영향 | 일반적인 경우 영향 없음

윈도즈 서버

취약점 항목	1.14. 로컬 로그인 허용				
대상 OS	NT, 2000, 2003, 2008	위험도	중	Code	W-14
취약점 개요	“로컬로 로그인 허용” 권한은 시스템 콘솔에 로그인을 허용하는 권한으로 반드시 콘솔 접근이 필요한 사용자 계정에만 해당 권한을 부여하여야 함. 만약 해당 권한을 적절하게 제한하지 않는 경우 권한 없는 사용자가 자신의 사용 권한을 상승시키기 위해 악의적인 코드를 실행할 수 있음. ※ IIS 서비스를 사용할 경우 이 권한에 IUSR_<ComputerName> 계정을 할당함.				
보안대책					
판단기준	양호: 로컬 로그인 허용 정책에 Administrators, IUSR_만 존재하는 경우				
	취약: 로컬 로그인 허용 정책에 Administrators, IUSR_ 외 다른 계정 및 그룹이 존재하는 경우				
조치방법	Administrators, IUSR_외 다른 계정 및 그룹의 로컬 로그인 제한				
보안설정방법					

■ Windows NT, 2000, 2003, 2008

1. 시작 > 실행 > SECPOL.MSC > 로컬 정책 > 사용자 권한 할당
2. “로컬 로그인 허용(또는, 로컬 로그인)” 정책에 “Administrators”, “IUSR_” 외 다른 계정 및 그룹 제거



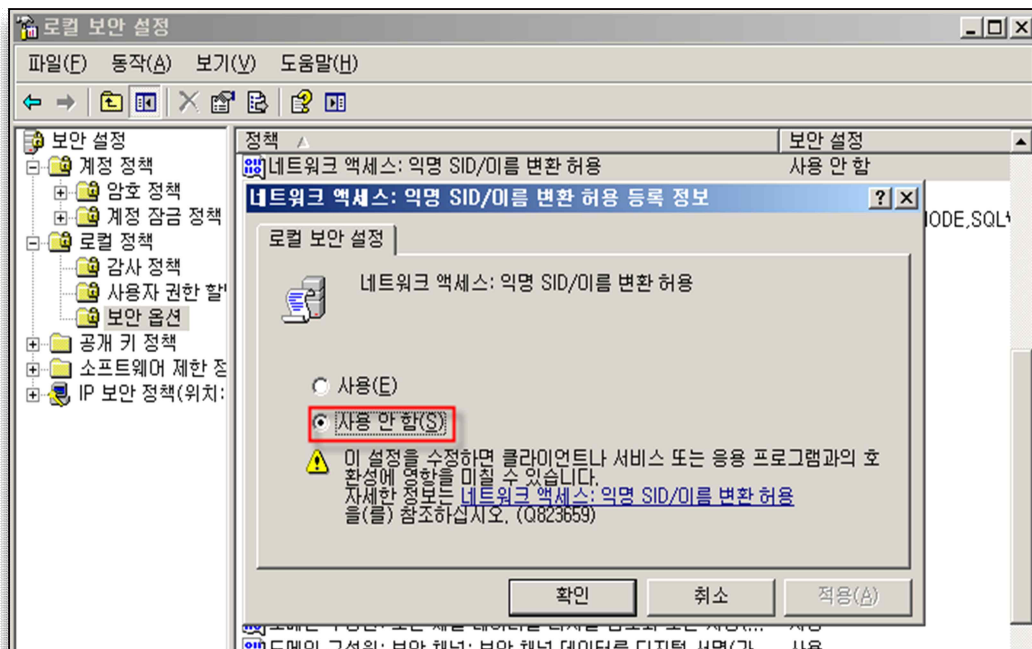
조치 시 영향 | 일반적인 경우 영향 없음

윈도즈 서버

취약점 항목	1.15. 익명 SID/이름 변환 허용				
대상 OS	2003, 2008	위험도	중	Code	W-15
취약점 개요	익명 사용자가 다른 사용자의 SID 특성을 요청할 수 있는지를 결정함. 이를 이용해 로컬 접근 권한이 있는 사용자가 잘 알려진 Administrator SID를 사용하여 Administrator 계정의 실제 이름을 알아낼 수 있으며 암호 추측 공격을 실행할 수 있음. "사용 안 함"으로 정책을 설정할 경우 Windows NT 도메인 환경에서 통신이 불가능하게 될 수 있음.				
보안대책					
판단기준	양호: "익명 SID/이름 변환 허용" 정책이 "사용 안 함" 으로 되어 있는 경우				
	취약: "익명 SID/이름 변환 허용" 정책이 "사용" 으로 되어 있는 경우				
조치방법	네트워크 액세스: 익명 SID/이름 변환 허용 → 사용 안 함				
보안설정방법					

■ Windows 2003, 2008

1. 시작> 실행> SECPOL.MSC> 로컬 정책> 보안 옵션
2. "네트워크 액세스: 익명 SID/이름 변환 허용" 정책이 "사용 안 함" 으로 설정



※ Windows Server 2000 이하 버전 해당 사항 없음

조치 시 영향	일반적으로 영향 없음
---------	-------------

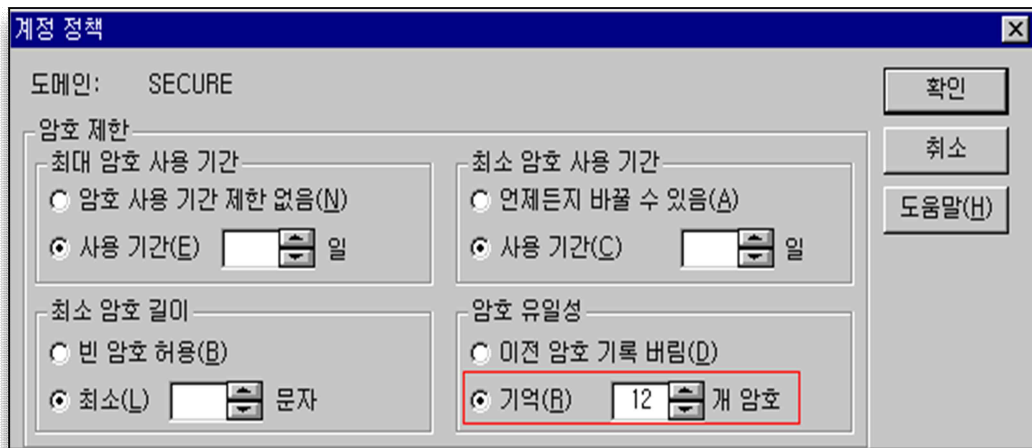
윈도우즈 서버

취약점 항목	1.16. 최근 암호 기억				
대상 OS	NT, 2000, 2003, 2008	위험도	중	Code	W-16
취약점 개요	사용자가 현재 암호 또는, 최근에 사용했던 암호와 똑같은 새 암호로 설정할 수 없도록 하여야 함. 특정 계정에 같은 암호를 오래 사용할수록 공격자가 무작위 공격을 통해 암호를 확인할 가능성이 커지며, 유출된 계정의 암호를 바꾸지 않는 한 계속 악용될 수 있음. 또한, 암호를 변경해야 할 경우 암호를 다시 사용하는 것을 금지하지 않거나, 적은 수의 암호를 계속해서 다시 사용할 수 있도록 허용하면 좋은 암호 정책의 효과가 크게 반감됨.				
보안대책					
판단기준	양호: 최근 암호 기억이 12개 이상으로 설정되어 있는 경우				
	취약: 최근 암호 기억이 12개 미만으로 설정되어 있는 경우				
조치방법	최근 암호 기억을 12개 암호로 설정				

보안설정방법

■ Windows NT

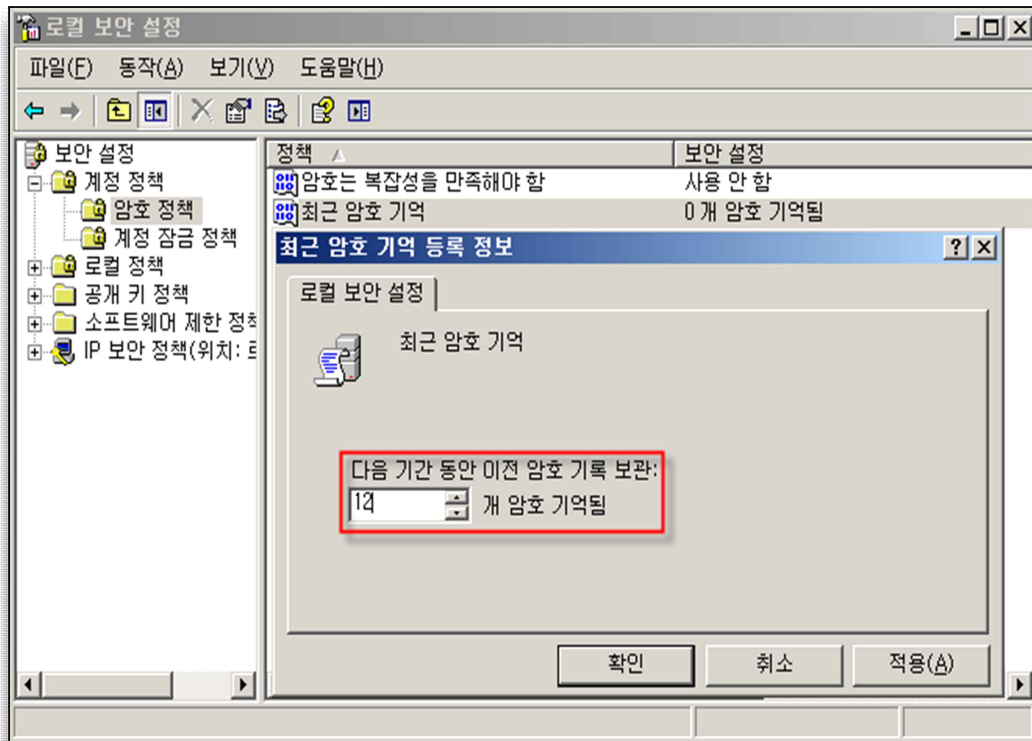
1. 시작> 프로그램> 관리 도구> 도메인 사용자 관리자> 정책> 계정
2. "암호 유일성"에서 "기억"을 "12개"로 설정



■ Windows 2000, 2003, 2008

1. 시작> 실행> SECPOL.MSC> 암호 정책
2. "최근 암호 기억"을 "12개 암호 기억됨"으로 설정

윈도우즈 서버



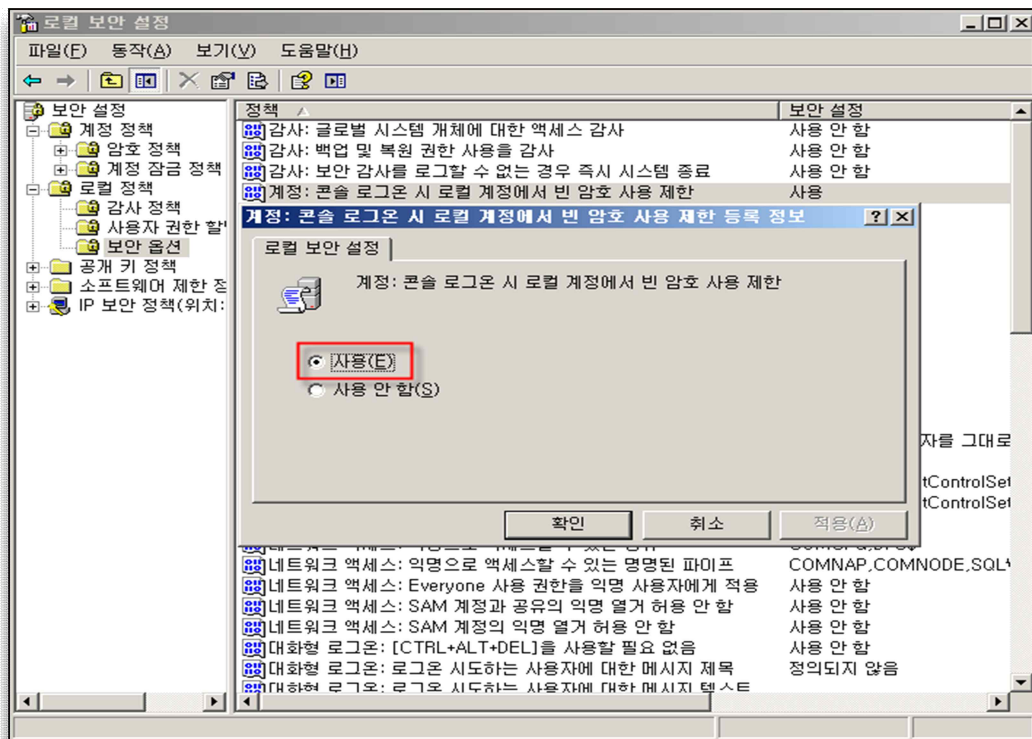
조치 시 영향 | 일반적으로 영향 없음

윈도우즈 서버

취약점 항목	1.17. 콘솔 로그인 시 로컬 계정에서 빈 암호 사용 제한				
대상 OS	2003, 2008	위험도	중	Code	W-17
취약점 개요	암호로 보호되지 않는 로컬 계정을 사용하여 터미널 서비스, Telnet 및 FTP와 같은 네트워크 서비스의 원격 대화형 로그인이 가능하므로 이를 허용할지를 결정함. 콘솔에서 실제로 수행하는 대화형 로그인이나 도메인 계정을 사용하는 로그인에는 영향을 주지 않음.				
보안대책					
판단기준	양호: "콘솔 로그인 시 로컬 계정에서 빈 암호 사용 제한" 정책이 "사용"인 경우				
	취약: "콘솔 로그인 시 로컬 계정에서 빈 암호 사용 제한" 정책이 "사용 안 함"인 경우				
조치방법	계정: 콘솔 로그인 시 로컬 계정에서 빈 암호 사용 제한 → 사용				
보안설정방법					

■ Windows 2003, 2008

1. 시작> 실행> SECPOL.MSC> 로컬 정책> 보안 옵션
2. "콘솔 로그인 시 로컬 계정에서 빈 암호 사용 제한" 정책을 "사용" 으로 설정



조치 시 영향 일반적으로 영향 없음

윈도우즈 서버

취약점 항목	1.18. 원격터미널 접속 가능한 사용자 그룹 제한				
대상 OS	2003, 2008	위험도	중	Code	W-18
취약점 개요	원격터미널의 그룹이나 계정을 제한하지 않으면 임의의 사용자가 원격으로 접속하여 해당 서버에 정보를 변경하거나 정보가 유출될 가능성이 있으므로 사용자 그룹과 계정을 설정하여 접속을 제한하여야 함.				
보안대책					
판단기준	양호: (관리자 계정을 제외한) 원격접속이 가능한 계정을 생성하여 타 사용자의 원격접속을 제한하고, 원격접속 사용자 그룹에 불필요한 계정이 등록되어 있지 않은 경우				
	취약: (관리자 계정을 제외한) 원격접속이 가능한 별도의 계정이 존재하지 않는 경우				
조치방법	관리자 계정과 이외의 계정을 생성, 권한을 제한 → 사용				
보안설정방법					
■ Windows 2003, 2008 1. 제어판> 사용자 계정> 관리자 계정 이외의 계정 생성한 후 2. 제어판> 시스템> [원격] 탭> [원격] 탭 메뉴에서 "사용자가 이 컴퓨터에 원격으로 연결할 수 있음"에 체크> "원격 사용자 선택"에서 원격 사용자 지정 후 확인					
조치 시 영향	일반적으로 영향 없음				

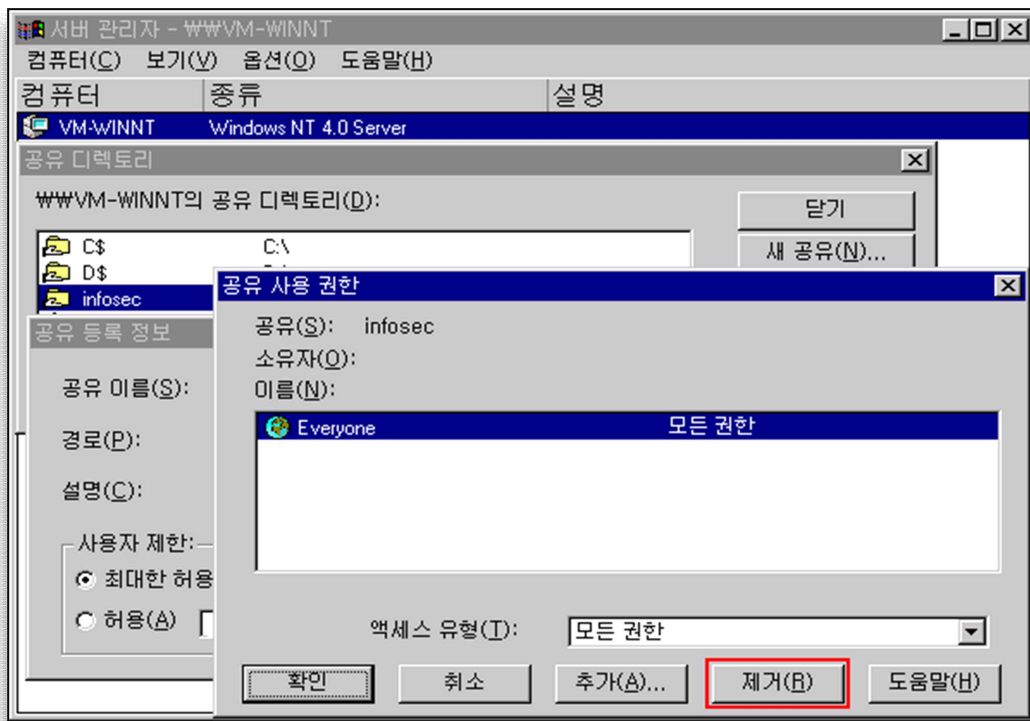
윈도우즈 서버

2. 서비스 관리

취약점 항목	2.1. 공유 권한 및 사용자 그룹 설정				
대상 OS	NT, 2000, 2003, 2008	위험도	상	Code	W-19
취약점 개요	Everyone이 공유계정에 포함되어 있으면 익명 사용자의 접근이 가능하므로 디폴트 공유인 C\$, D\$, Admin\$, IPC\$ 등을 제외한 공유 폴더가 Everyone 그룹으로 공유가 금지되었는지를 점검하여 익명 사용자의 접근 여부를 확인하여야 함.				
보안대책					
판단기준	양호: 일반 공유 디렉터리가 없거나 공유 디렉터 접근 권한에 Everyone 권한이 없는 경우				
	취약: 일반 공유 디렉터리의 접근 권한에 Everyone 권한이 있는 경우				
조치방법	공유 디렉터리 접근 권한에서 Everyone 권한 제거 후 필요한 계정 추가				
보안설정방법					

■ Window NT

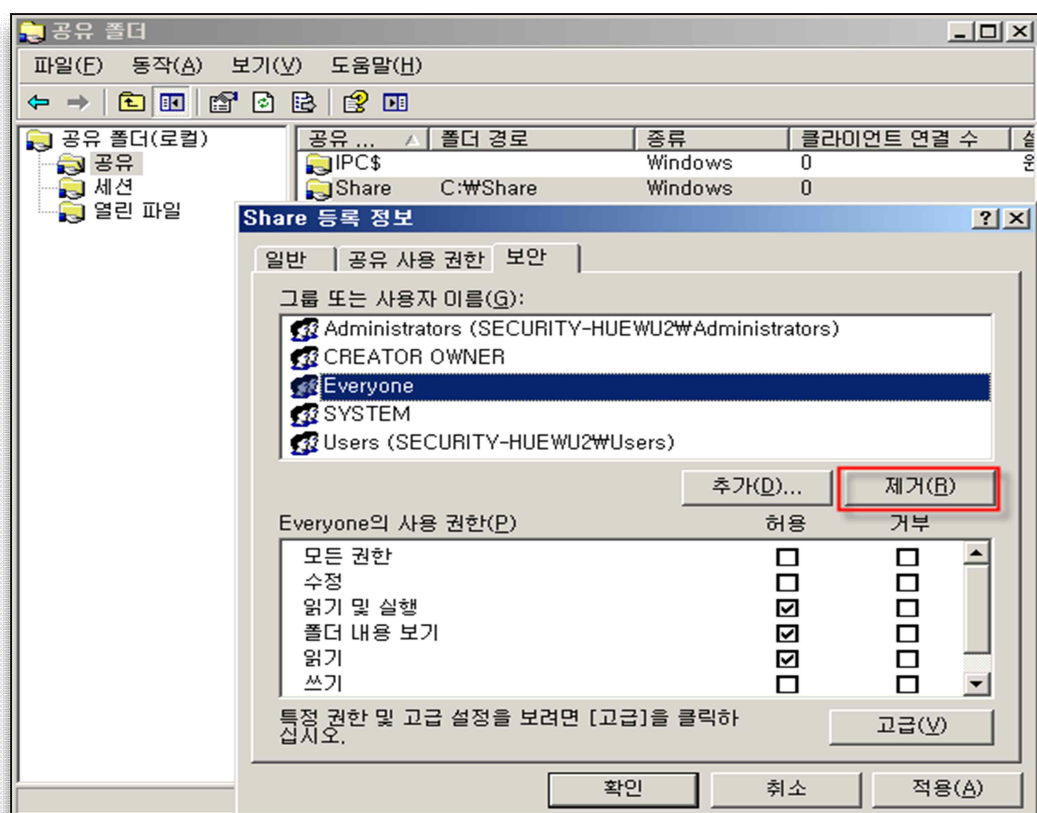
1. 프로그램> 관리 도구> 서버 관리자> 컴퓨터> 공유 디렉터리> 등록 정보> 사용 권한에서 Everyone으로 된 공유를 제거하고 접근이 필요한 계정의 적절한 권한 추가



■ Window 2000, 2003, 2008

1. 시작> 실행> FSMGMT.MSC> 공유
2. 사용 권한에서 Everyone으로 된 공유를 제거하고 접근이 필요한 계정의 적절한 권한 추가

윈도우즈 서버



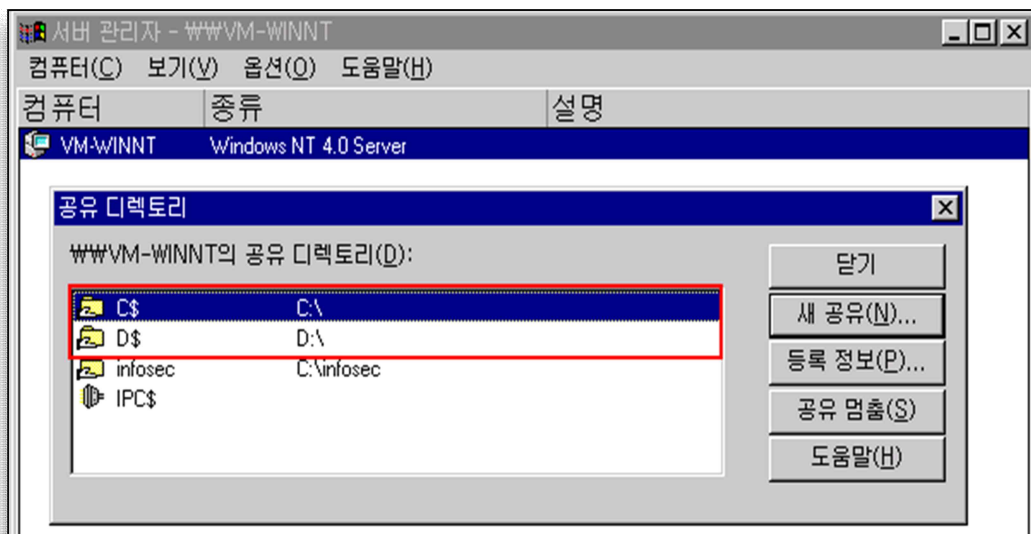
조치 시 영향 애플리케이션이나 Backup 용도로 Everyone 공유를 사용하지 않는지 확인 필요

윈도우즈 서버

취약점 항목	2.2. 하드디스크 기본 공유 제거				
대상 OS	NT, 2000, 2003, 2008	위험도	상	Code	W-20
취약점 개요	Windows는 프로그램 및 서비스를 네트워크나 컴퓨터 환경에서 관리하기 위해 시스템 기본 공유 항목을 자동으로 생성함. 이를 제거하지 않으면 비인가자가 모든 시스템 자원에 접근할 수 있는 위험한 상황이 발생할 수 있으며 이러한 공유 기능의 경로를 이용하여 바이러스가 침투될 수 있음.				
보안대책					
판단기준	양호: AutoShareServer (WinNT: AutoShareWks)가 0이며 기본 공유가 존재하지 않는 경우				
	취약: AutoShareServer (WinNT: AutoShareWks)가 1이거나 기본 공유가 존재하는 경우				
조치방법	기본 공유 중지 후 레지스트리 값 설정(IPC\$, 일반 공유 제외)				
보안설정방법					

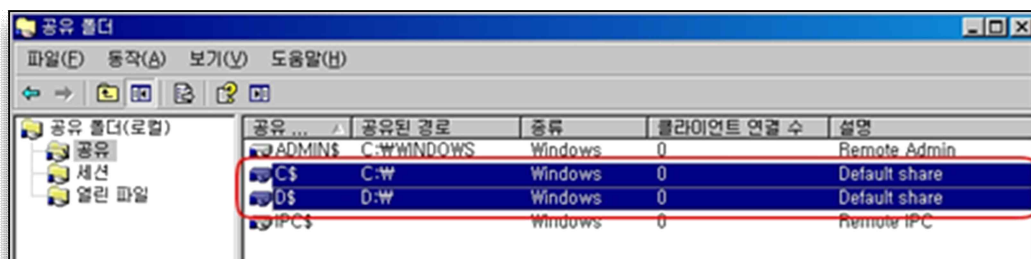
■ Window NT

1. 프로그램 > 관리 도구 > 서버 관리자 > 컴퓨터 > 공유 디렉터리 > 공유



■ Window 2000, 2003, 2008

1. 시작 > 실행 > FSMGMT.MSC > 공유 > 기본 공유 선택 > 공유 중지



윈도즈 서버

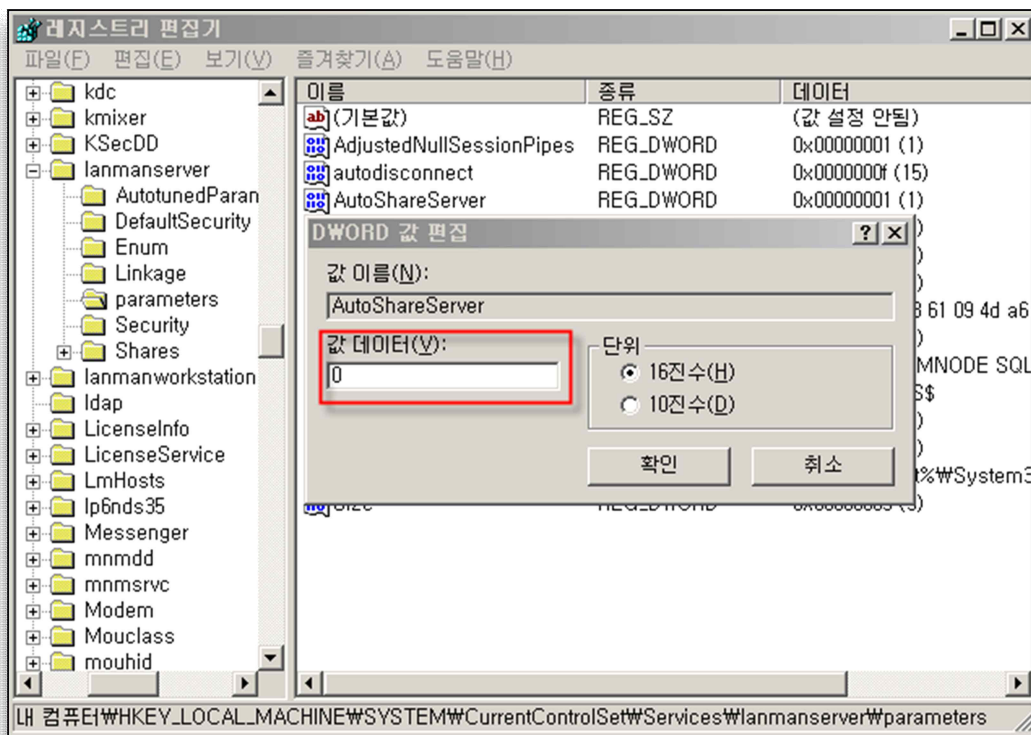
※ "net share 공유 이름 /delete" 로 공유한 폴더를 공유 해제

2. 시작 > 실행 > REGEDI

아래 레지스트리 값을 0 으로 수정함 (키 값이 없을 경우 새로 생성함)

"HKLM\SYSTEM\CurrentControlSet\Services\Lanmanserver\parameters\AutoShareServer"

(Windows NT일 경우: AutoShareWks)



※ 방화벽과 라우터에서 135~139(TCP/UDP)포트를 차단하여 외부로부터의 위험을 제거함으로써 보안성을 높일 수 있음 (Windows 2008 제외)

조치 시 영향

*Active Directory, *Clustered system에서는 적용 시 영향 있음

*Active Directory: 중앙 집중화된 자원 관리를 위한 계층적 디렉터리 서비스

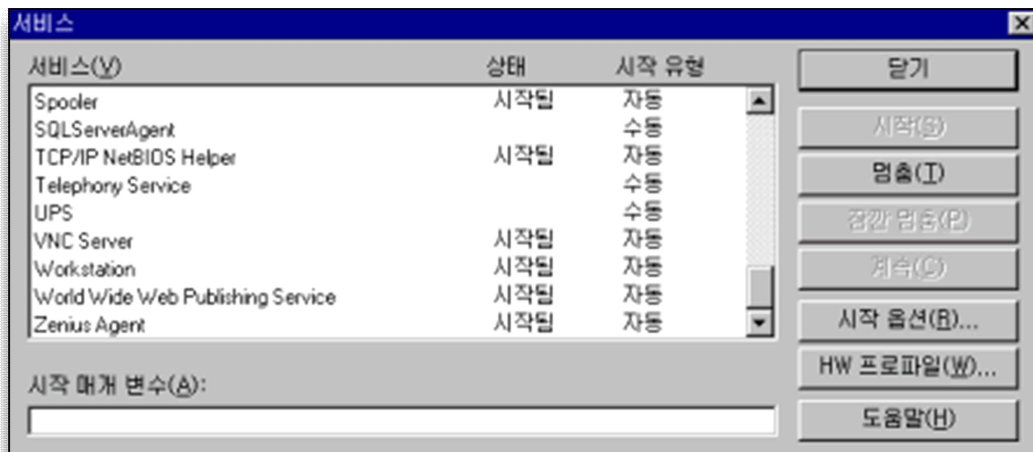
*Clustered system: 여러 개의 시스템을 결합하여 사용함

윈도우즈 서버

취약점 항목	2.3. 불필요한 서비스 제거				
대상 OS	NT, 2000, 2003, 2008	위험도	상	Code	W-21
취약점 개요	일반적으로 시스템에는 필요하지 않은 취약한 서비스들이 디폴트로 설치되어 실행되고 있으며 이러한 서비스 또는, 응용 프로그램은 공격 지점이 될 수 있으므로 사용자의 환경에서 필요하지 않은 서비스나 실행 파일을 사용하지 않거나 제거하여야 함.				
보안대책					
판단기준	양호: 아래 서비스가 중지되어 있는 경우				
	취약: 아래 서비스가 구동 중인 경우 • Alerter(서버에서 클라이언트로 경고 메시지를 보냄) • Clipbook(서버 내 Clipbook을 다른 클라이언트와 공유) • Messenger(net send 명령어를 이용하여 클라이언트에 메시지 보냄) • Simple TCP/IP Services(Echo, Discard, Character Generator, Daytime, Quote of the Day)				
조치방법	서비스 중지 후 “사용 안 함” 설정				
보안설정방법					

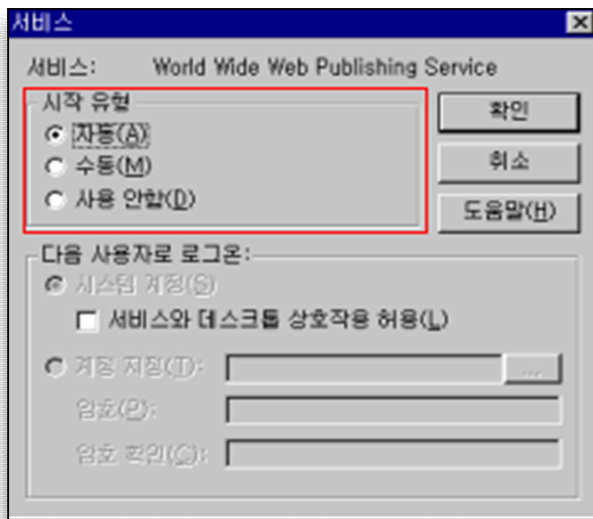
■ Window NT

1. 시작> 설정> 제어판> 서비스를 선택하여 불필요한 서비스를 중지하고, 시작 옵션에서 "시작 유형"을 "사용 안함"으로 수정



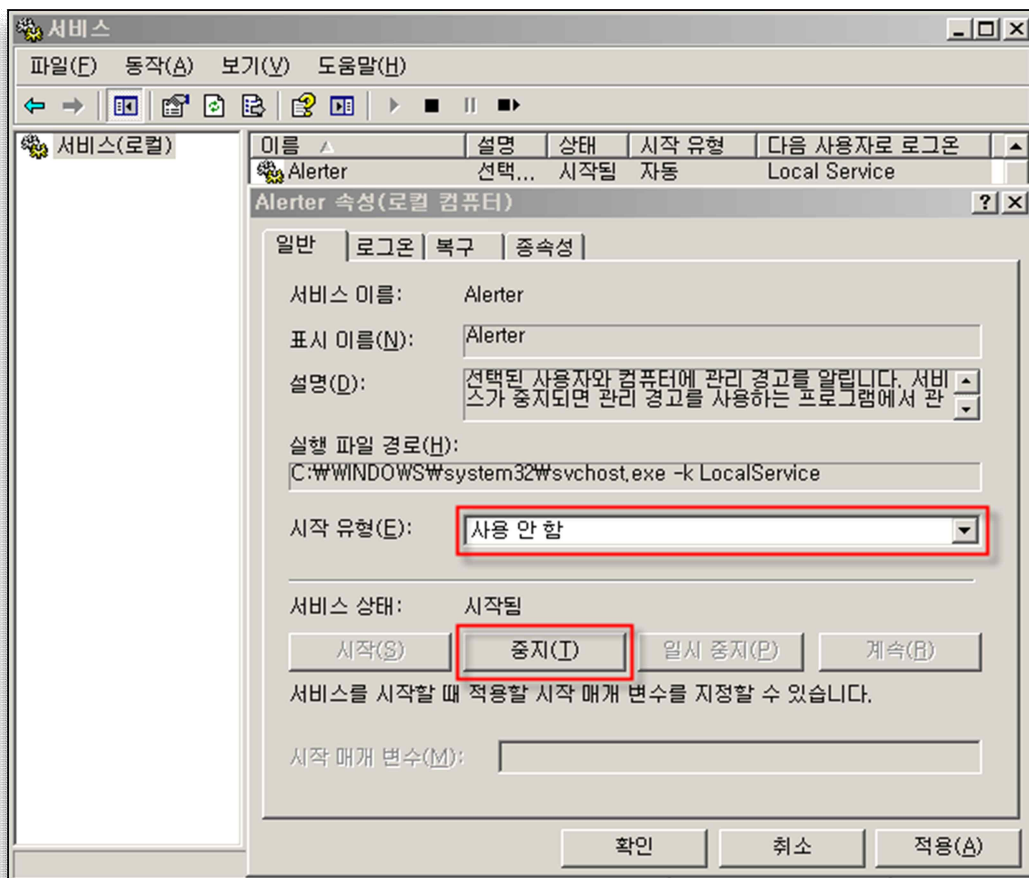
2. 해당 서비스를 선택하고 오른쪽 메뉴에서 "시작 옵션"을 클릭하면 시스템이 시작할 때 해당 서비스의 시작 유형을 선택할 수 있음. 만약, 시스템 시작 시 자동으로 시작되게 하려면 [자동], 수동으로 서비스를 시작하려면 [수동], 서비스 자체를 사용하지 않으려면 [사용 안함]을 선택한 후 [확인]을 클릭함

윈도우즈 서버



■ Window 2000, 2003, 2008

1. 시작 > 실행 > SERVICES.MSC > “해당 서비스” 선택 > 속성
2. 시작 유형 → 사용 안 함
시작 상태 → 중지 설정



윈도우즈 서버

특별한 목적을 위해 사용하는 서비스가 아니라면 시스템의 업무에 부합되는 서비스가 아닌 기타 디폴트 서비스를 사용하지 않는 것이 좋으며, 시스템 관리자는 대상 시스템의 용도를 정확히 파악해 불필요한 서비스를 제거하여야 함

서비스 시작 유형	설 명
사용 안 함	설치되어 있으나 실행되지 않음
수동	다른 서비스나 응용 프로그램에서 해당 기능을 필요로 할 때만 시작됨
자동	부팅 시에 해당 장치 드라이버가 로드된 후에 운영 체제에 의해 시작됨

각 서비스마다 옵션을 설정할 수 있으며 해당 서비스를 선택하고 더블 클릭하게 되면 시작 유형을 선택할 수 있으며 시작 시 로그인 계정을 별도로 설정할 수 있음. 만약, 시스템 시작 시 자동으로 시작되게 하려면 [자동], 수동으로 서비스를 시작하려면 [수동], 서비스 자체를 사용하지 않으려면 [사용 안 함]을 선택한 후 [확인]을 클릭함

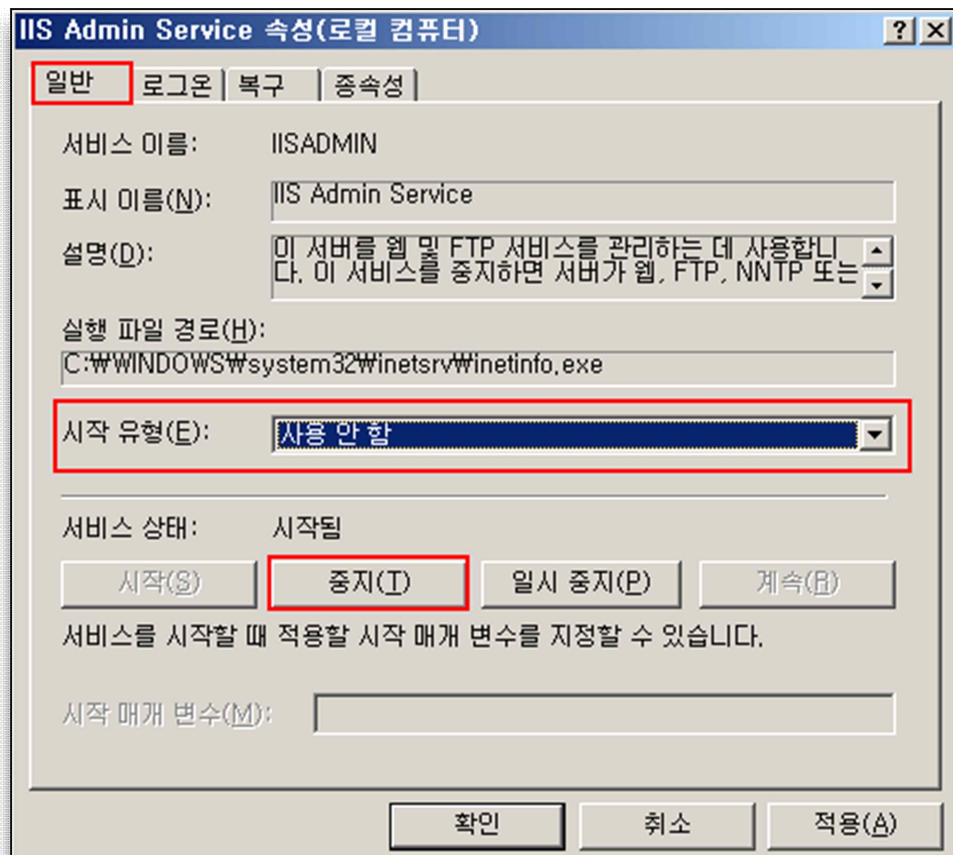
조치 시 영향	일반적으로 영향 없음
---------	-------------

윈도우즈 서버

취약점 항목	2.4. IIS 서비스 구동 점검				
대상 OS	NT, 2000, 2003, 2008	위험도	상	Code	W-22
취약점 개요	IIS 서비스는 WEB, FTP 등의 서비스를 제공해주는 유용한 서비스이지만 프로파일링, 서비스 거부, 불법적인 접근, 임의의 코드실행, 정보 공개, 바이러스, 웜, 트로이목마 등의 위협에 노출될 수 있으므로 필요하지 않은 서비스는 중지하여야 함.				
보안대책					
판단기준	양호: IIS 서비스가 필요하지 않아 이용하지 않는 경우				
	취약: IIS 서비스를 필요하지 않지만 사용하는 경우				
조치방법	IIS 서비스를 사용하지 않는 경우 IIS 서비스 중지				
보안설정방법					

■ Window NT, 2000, 2003, 2008

1. 시작> 실행> services.msc> IISADMIN> 속성> "시작 유형"을 "사용 안 함" 설정 후 중지



조치 시 영향 | 일반적으로 영향 없음

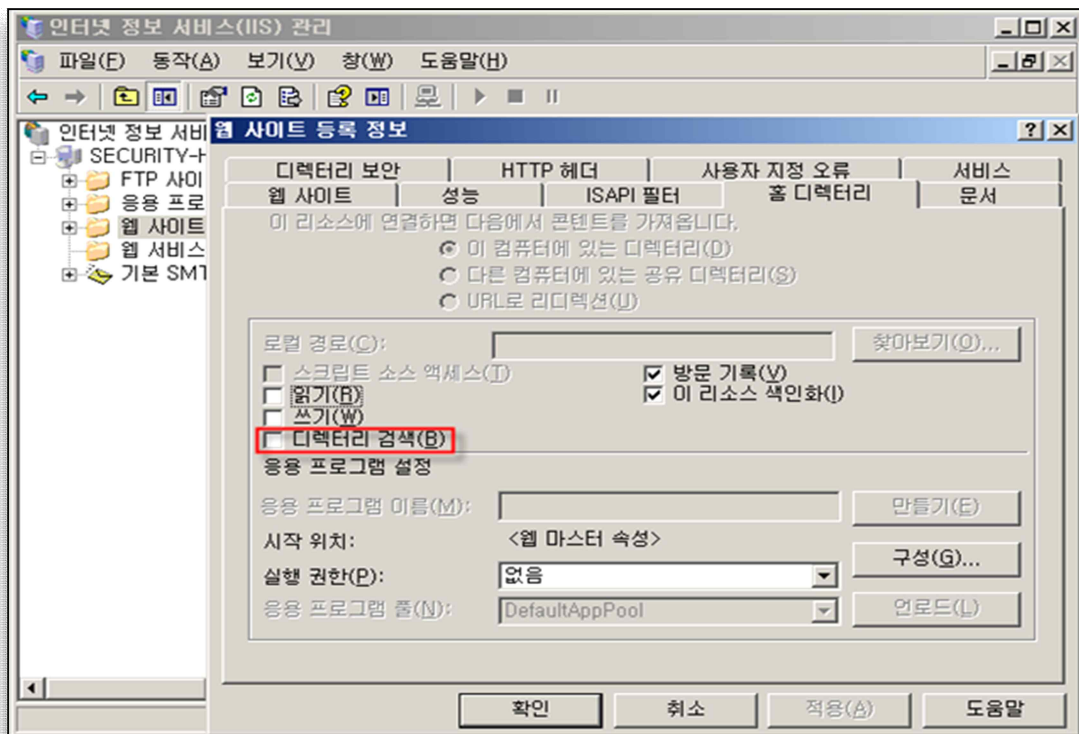
윈도우즈 서버

취약점 항목	2.5. IIS 디렉터리 리스팅 제거				
대상 OS	NT, 2000, 2003, 2008	위험도	상	Code	W-23
취약점 개요	디렉터리 검색은 디렉터리에 대한 요청 시 기본 페이지가 호출되어 사용자에게 전송하지만, 기본 페이지가 존재하지 않는 경우 디렉터리 내에 존재하는 모든 파일의 목록을 보여줌. 따라서 디렉터리 검색이 허용될 경우 외부에서 디렉터리 내의 모든 파일에 대한 접근이 가능하므로 중요한 파일들이 노출될 수 있음.				
보안대책					
판단기준	양호: "디렉터리 검색"이 체크되어 있지 않은 경우				
	취약: "디렉터리 검색"이 체크되어 있는 경우 ※ 조치 시 마스터 속성과 모든 사이트에 적용함				
조치방법	사용하지 않는 경우 IIS 서비스 중지, 사용할 경우 디렉터리 검색 체크 해제				
보안설정방법					

운영체제	IIS 버전
Windows 2000	IIS 5.0
Windows 2003	IIS 6.0
Windows 2008	IIS 7.0

■ IIS 5.0, 6.0

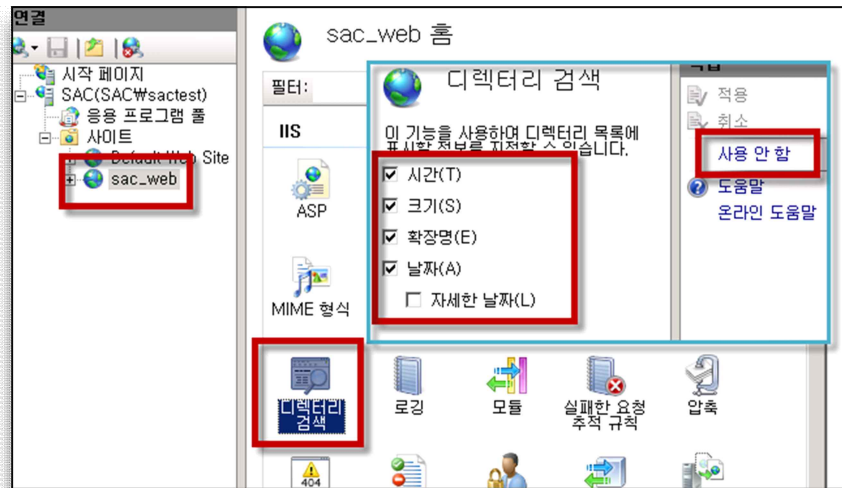
1. 시작 > 실행 > INETMGR > 웹 사이트 > 속성 > 홈 디렉터리
2. "디렉터리 검색" 체크 해제



윈도즈 서버

■ IIS 7.0

1. 인터넷 정보 서비스(IIS) 관리> 해당 웹 사이트> IIS> “디렉터리 검색” 선택 후 “사용 안 함” 선택



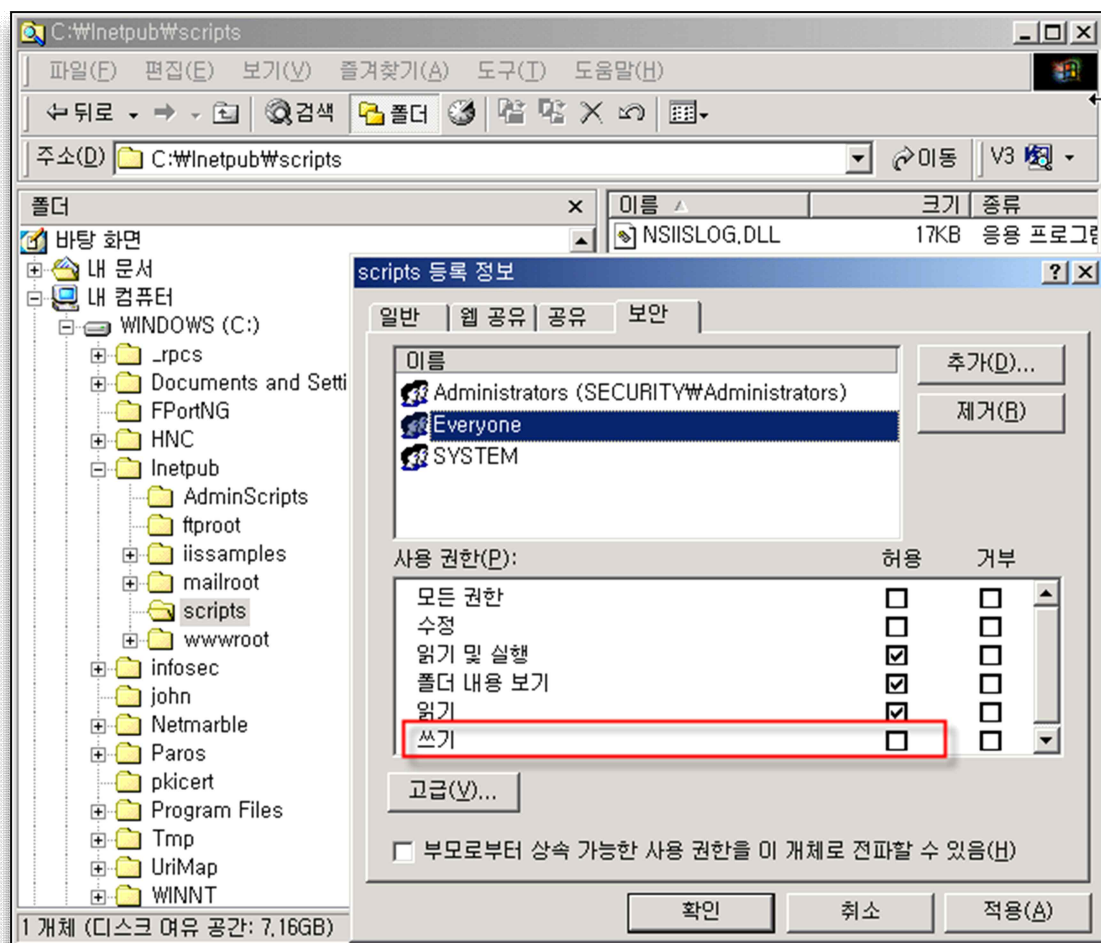
조치 시 영향

일반적으로 영향 없음

윈도우즈 서버

취약점 항목	2.6. IIS CGI 실행 제한				
대상 OS	NT, 2000, 2003, 2008	위험도	상	Code	W-24
취약점 개요	*CGI 스크립트는 정해진 디렉터리에서만 실행되도록 하여야 함. 게시판이나 자료실과 같이 업로드 되는 파일이 저장되는 디렉터리에 CGI 스크립트가 실행 가능하다면 악의적인 파일을 업로드하고 이를 실행하여 시스템의 중요 정보가 노출될 수 있으며 침해사고의 경로로 이용될 수 있음. *CGI(Common Gateway Interface): 사용자가 서버로 보낸 데이터를 서버에서 작동중인 데이터처리프로그램에 전달하고, 여기에서 처리된 데이터를 다시 서버로 되돌려 보내는 등의 일을 하는 프로그램.				
보안대책					
판단기준	양호: 해당 디렉터리 Everyone에 모든 권한, 수정 권한, 쓰기 권한이 부여되지 않은 경우 취약: 해당 디렉터리 Everyone에 모든 권한, 수정 권한, 쓰기 권한이 부여되어 있는 경우 ※ 조치 시 마스터 속성과 모든 사이트에 적용함				
조치방법	사용하지 않는 경우 IIS 서비스 중지, 사용할 경우 Everyone에 모든 권한, 수정 권한 쓰기 권한 제거 후 Administrators, System 그룹 추가(모든 권한)				
보안설정방법					
■ IIS 5.0, 6.0, 7.0					
1. 탐색기> 해당 디렉터리> 속성> 보안 (기본 CGI 디렉터리 위치 C:WinetpubWscripts)					
2. Everyone 의 모든 권한, 수정 권한, 쓰기 권한 제거					

윈도우즈 서버



조치 시 영향

일반적으로 기본 CGI 디렉터리(C:\inetpub\scripts)를 사용하지 않음
해당 디렉터리 확인 후 추가적인 파일이 없다면 영향 없음

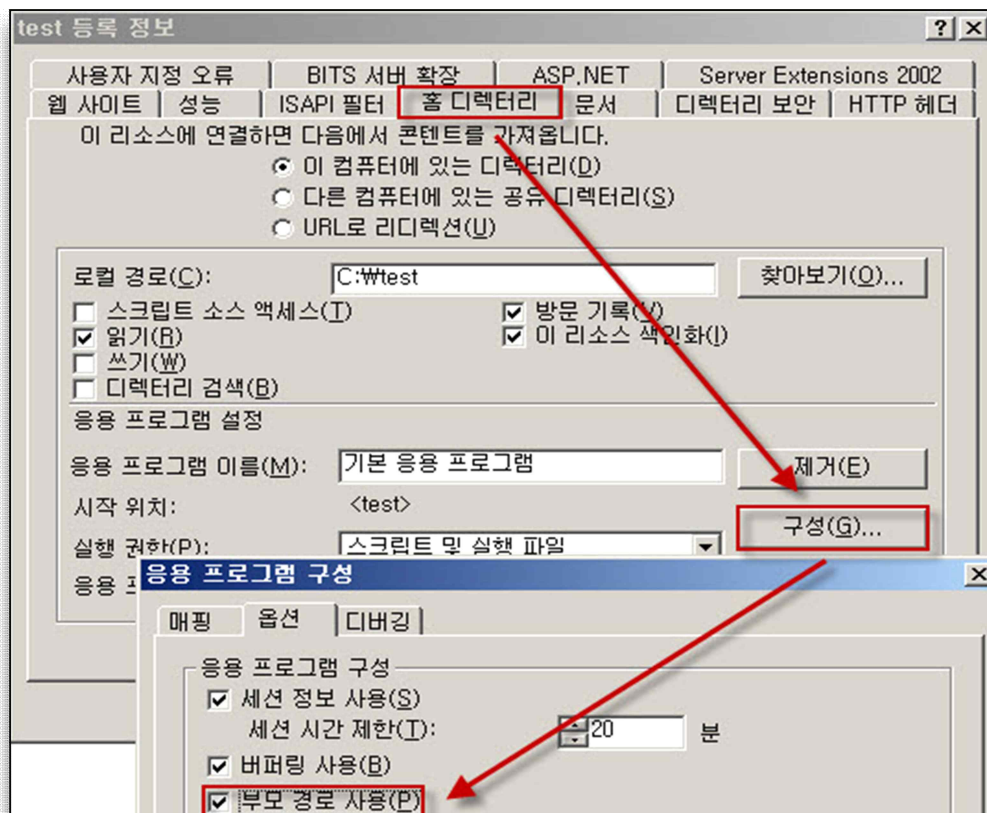
윈도즈 서버

취약점 항목	2.7. IIS 상위 디렉터리 접근 금지				
대상 OS	Windows 계열 OS (NT, 2000, 2003, 2008)	위험도	상	Code	W-25
취약점 개요	상위경로로 이동하는 것이 가능할 때 하위경로에 접속하여 상위로 이동함으로써 해킹을 당할 위험이 있으며, Unicode 버그 및 서비스 거부 공격에 이용당하기 쉬우므로 되도록이면 "." 와 같은 상위 경로를 사용하지 못하도록 설정하는 것이 바람직함. "." 는 unicode 버그, 서비스 거부와 같은 공격에 쉽게 이용되므로 허용하지 않는 것을 권장함.				
보안대책					
판단기준	양호: 상위 패스 기능을 제거한 경우				
	취약: 상위 패스 기능을 제거하지 않은 경우 ※ 조치 시 마스터 속성과 모든 사이트에 적용함				
조치방법	사용하지 않는 경우 IIS 서비스 중지, 사용할 경우 Everyone에 모든 권한, 수정 권한 쓰기 권한 제거 후 Administrators, System 그룹 추가(모든 권한)				
보안설정방법					

■ IIS 5.0, 6.0

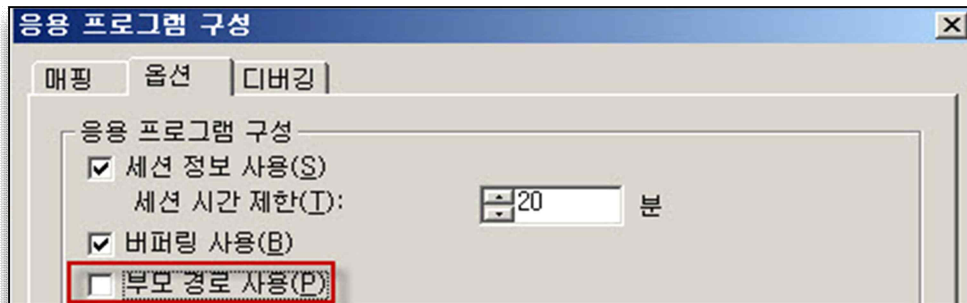
1. 인터넷 정보 서비스(IIS) 관리> 해당 웹 사이트> 속성> 홈 디렉터리> 구성>

[옵션] 탭에서 "부모 경로 사용" 설정 확인



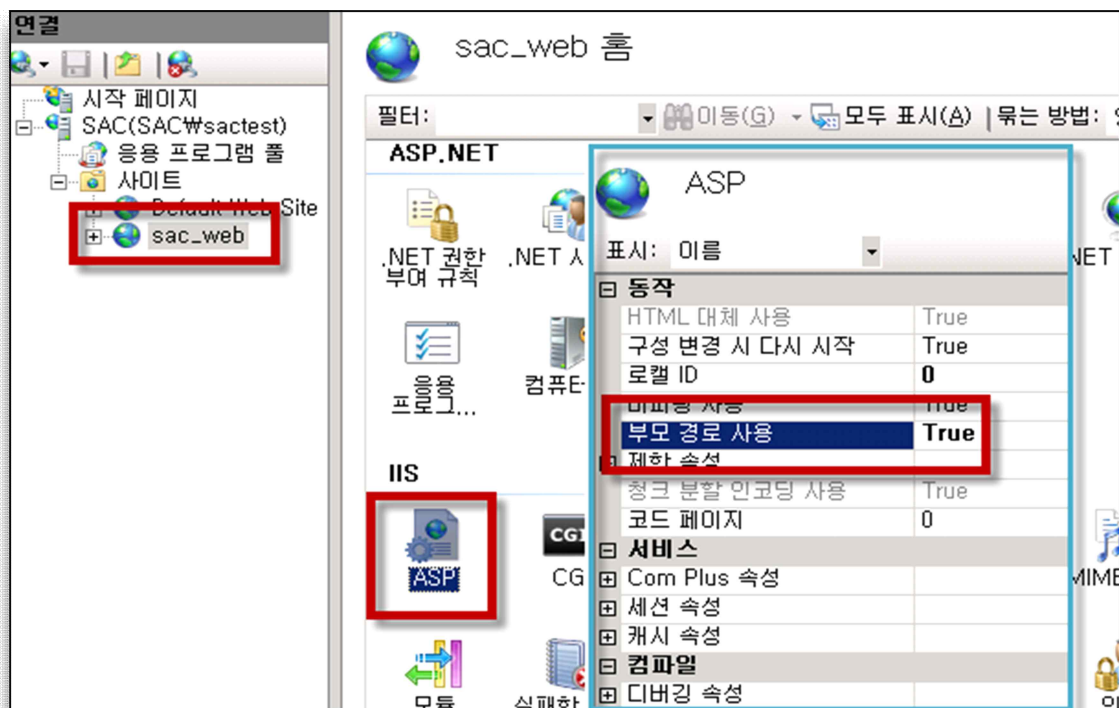
윈도즈 서버

2. 인터넷 정보 서비스(IIS) 관리> 해당 웹 사이트> 등록 정보> 홈 디렉터리> 구성
 [옵션] 탭 선택 후 "부모 경로 사용"의 체크박스 활성화 해제



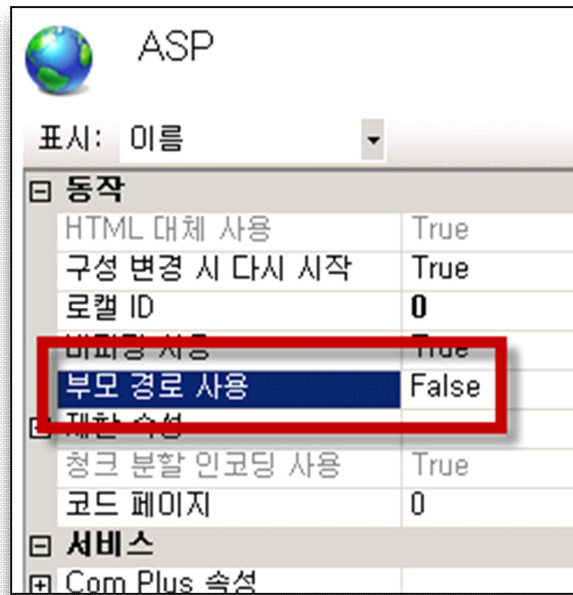
■ IIS 7.0

1. 인터넷 정보 서비스(IIS) 관리자> 해당 웹 사이트> IIS> ASP 선택,
 "부모 경로 사용" 항목에서 설정 확인



2. 인터넷 정보 서비스(IIS) 관리자> 해당 웹 사이트> IIS> ASP 선택,
 "부모 경로 사용" 항목을 "False"로 설정 변경

윈도우즈 서버



조치 시 영향 애플리케이션에서 "../" 와 같이 상대경로를 사용하도록 코딩되어 있을 경우 영향 있음

윈도우즈 서버

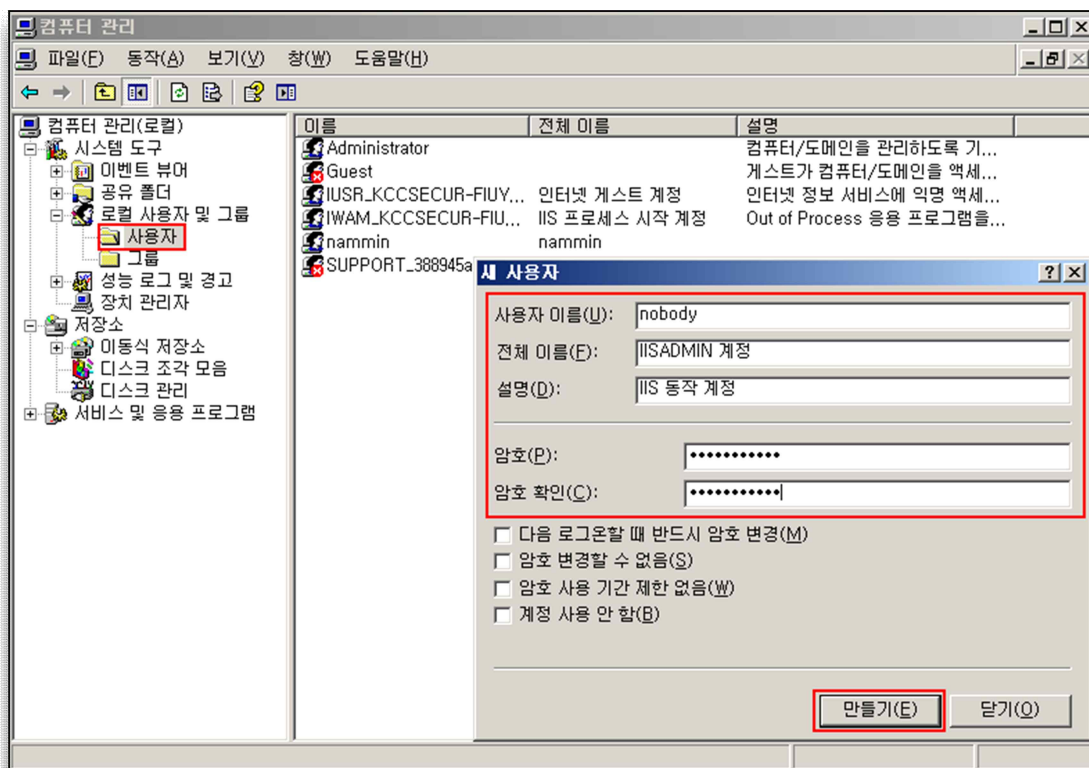
취약점 항목	2.8. IIS 불필요한 파일 제거				
대상 OS	NT, 2000, 2003, 2008	위험도	상	Code	W-26
취약점 개요	샘플 애플리케이션은 IIS 서비스 설치 시 디폴트로 설치되는 예제 스크립트로 제거하는 것이 안전함. IIS를 설치하면 기본적으로 예제와 설명서 등이 같이 설치되는데 이러한 폴더들은 공격 대상으로 이용되거나 백도어가 심어질 위험이 있으므로 제거해 주어야 함.				
보안대책					
판단기준	양호: 해당 웹 사이트에 IISamples, IISHelp 가상 디렉터리가 존재하지 않는 경우				
	취약: 해당 웹 사이트에 IISamples, IISHelp 가상 디렉터리가 존재하는 경우 ※ 조치 시 마스터 속성과 모든 사이트에 적용함				
조치방법	사용하지 않는 경우 IIS 서비스 중지, 사용할 경우 가상 디렉터리 삭제				
보안설정방법					
■ IIS 5.0, 6.0					
1. Sample 디렉터리 확인					
아래의 Sample 디렉터리를 확인함					
c:\inetpub\wwwroot\iisamples c:\winnt\help\iis\iishelp (IIS 설명서) c:\program files\common files\system\msadc\sample (데이터 액세스) %SystemRoot%\System32\inet\iisadmpwd					
2. Sample 디렉터리 확인 후 삭제					
※ IIS 7.0 이상 버전 해당 사항 없음					
조치 시 영향	애플리케이션에서 "../" 와 같이 상대경로를 사용하도록 코딩되어 있을 경우 영향 있음				

윈도우즈 서버

취약점 항목	2.9. IIS 웹 프로세스 권한 제한				
대상 OS	NT, 2000, 2003, 2008	위험도	상	Code	W-27
취약점 개요	웹 프로세스에서 권한을 제한하지 않는다면, 웹 사이트 방문자가 웹 서비스의 취약점을 이용하여 시스템 권한을 획득할 수 있음. 웹 취약점을 통해 접속 권한을 획득한 경우에는 관리자 권한을 획득할 수 있고 서버에 접속하여 해당 정보를 해킹하거나 변경 손실할 우려가 있음.				
보안대책					
판단기준	양호: 웹 프로세스가 웹 서비스 운영에 필요한 최소한 권한으로 설정되어 있는 경우				
	취약: 웹 프로세스가 관리자 권한이 부여된 계정으로 구동되고 있는 경우				
조치방법	시작> 제어판> 관리 도구> 로컬 보안 정책에서 nobody 계정 설정				
보안설정방법					

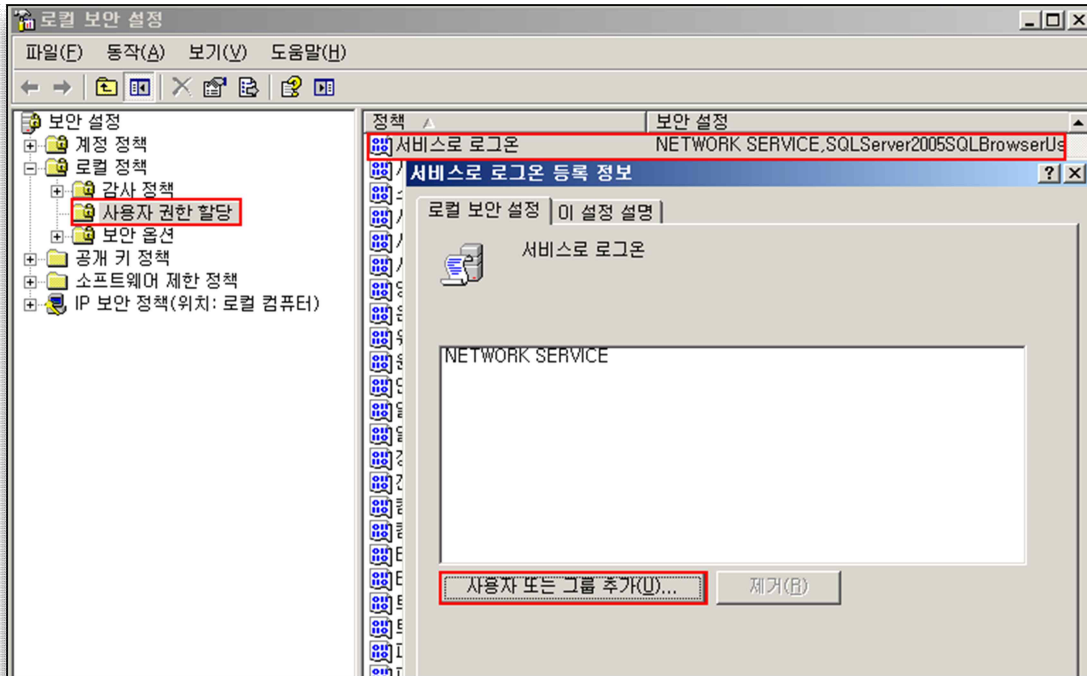
■ Windows NT, 2000, 2003, 2008

1. 시작> 제어판> 관리 도구> 컴퓨터 관리> 로컬 사용자 및 그룹> 사용자 선택
2. nobody 계정 추가 (nobody 계정의 소속 그룹에 정해진 User가 있으면 제거)

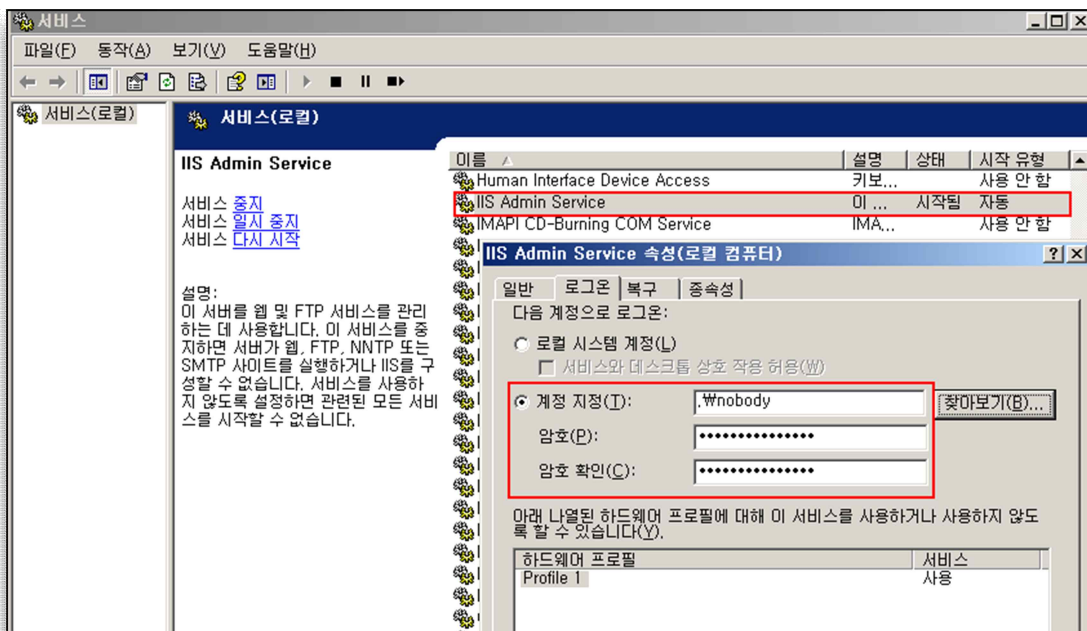


3. 시작> 제어판> 관리 도구> 로컬 보안 정책> 로컬 정책> 사용자 권한 할당 선택,
"서비스 로그인"에 "nobody" 계정 추가

윈도우즈 서버



4. 시작 > 실행 > SERVICES.MSC > IISADMIN > 속성 > [로그온] 탭의 계정 지정에 nobody 계정 및 패스워드 입력



5. 시작 > 프로그램 > 윈도우 탐색기 > IIS가 설치된 폴더 속성 [보안] 탭에 들어간 후 nobody 계정을 추가하고, 모든 권한 체크

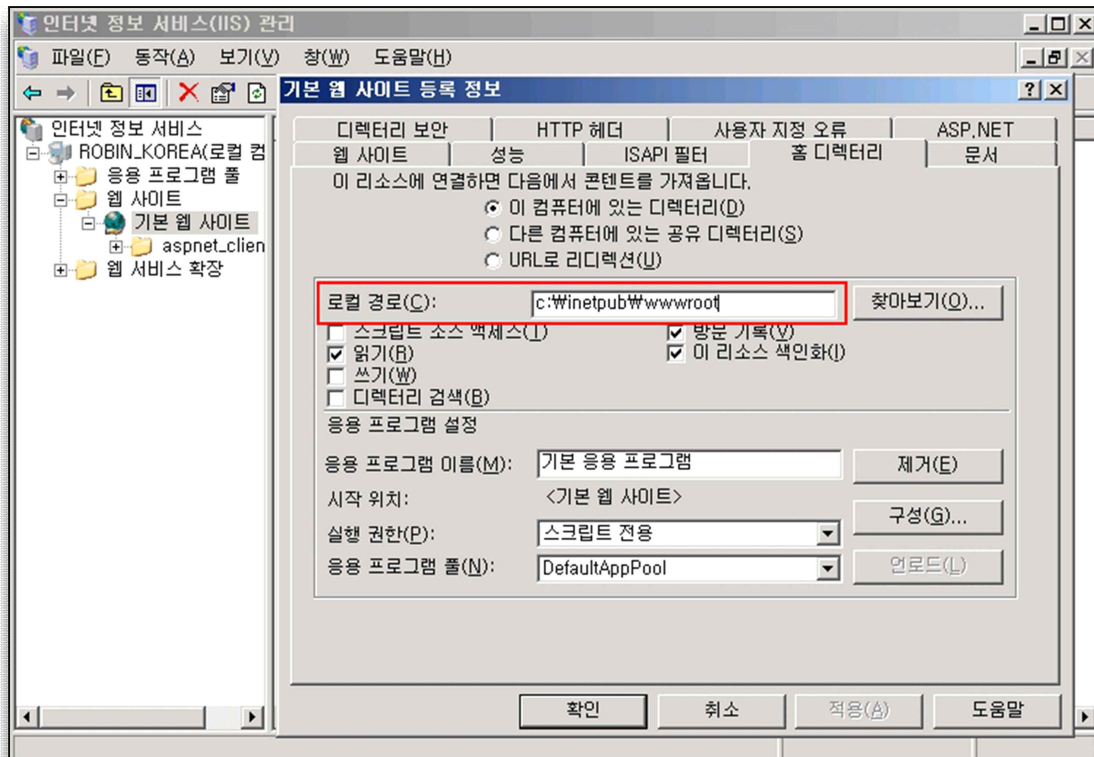
조치 시 영향	일반적으로 영향 없음
---------	-------------

윈도즈 서버

취약점 항목	2.10. IIS 링크 사용금지				
대상 OS	NT, 2000, 2003, 2008	위험도	상	Code	W-28
취약점 개요	공개적인 웹 콘텐츠 디렉터리 안에서 서버의 다른 디렉터리나 파일들에 접근할 수 있는 심볼릭 링크, aliases, 바로가기 등을 사용하지 않도록 하여야 함.				
보안대책					
판단기준	양호: 심볼릭 링크, aliases, 바로가기 등의 사용을 허용하지 않는 경우				
	취약: 심볼릭 링크, aliases, 바로가기 등의 사용을 허용하는 경우				
조치방법	등록된 웹 사이트의 홈 디렉터리에 있는 심볼릭 링크, aliases, 바로가기 파일 삭제				
보안설정방법					

■ IIS 5.0, 6.0

- 인터넷 정보 서비스(IIS) 관리자> 해당 웹 사이트> 속성> [홈 디렉터리] 탭 선택
“로컬 경로”에서 홈 디렉터리 위치 확인

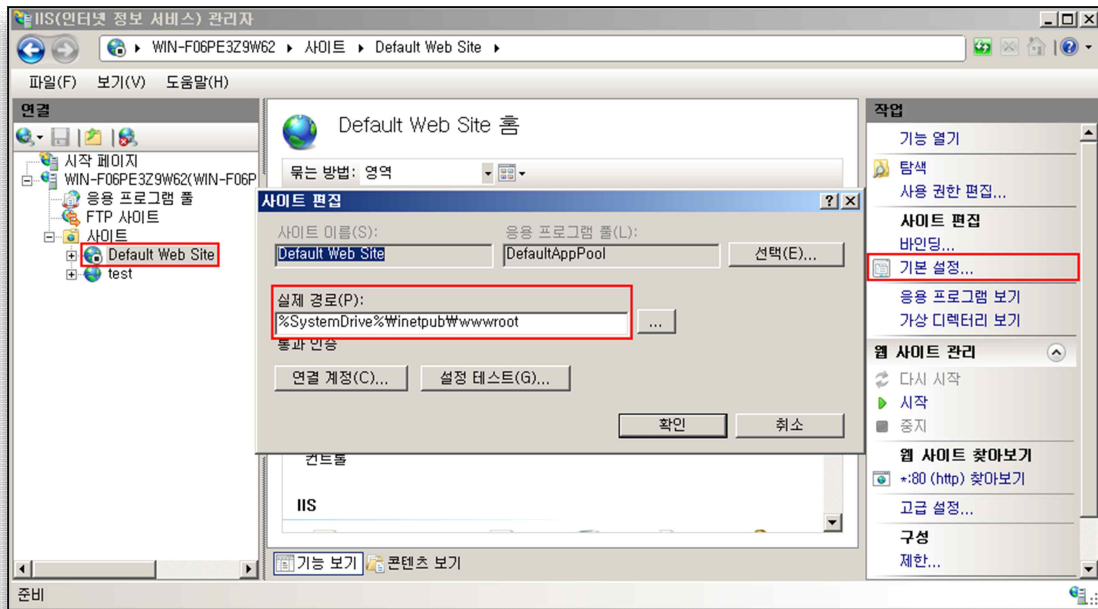


- 로컬 경로에 입력된 홈 디렉터리로 이동하여 바로가기 파일 삭제

■ IIS 7.0

- 인터넷 정보 서비스(IIS) 관리자> 해당 웹 사이트> 기본 설정
“실제 경로”에서 홈 디렉터리 위치 확인

윈도우즈 서버

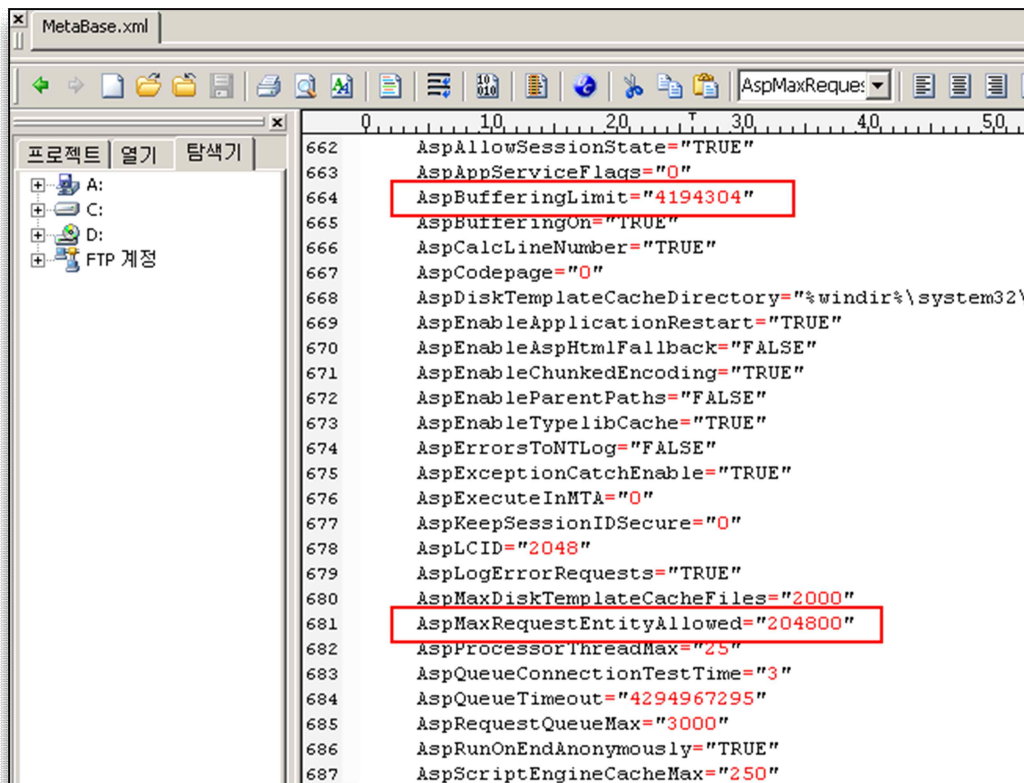


2. 실제 경로에 입력된 홈 디렉터리로 이동하여 바로가기 파일 삭제

조치 시 영향 일반적으로 영향 없음

취약점 항목	2.11. IIS 파일 업로드 및 다운로드 제한				
대상 OS	NT, 2000, 2003, 2008	위험도	상	Code	W-29
취약점 개요	대량의 파일 업로드 및 다운로드에 의하여 서비스 불능상태가 발생할 수 있으므로 불필요한 업로드 및 다운로드의 용량을 제한하여야 함. 또한, 대량의 파일 용량을 허용할 경우 웹 취약점으로 인하여 중요 정보가 대량으로 유출될 위험성이 있음.				
보안대책					
판단기준	양호: 웹 프로세스의 서버 자원 관리를 위해 업로드 및 다운로드 용량을 제한하는 경우				
	취약: 웹 프로세스의 서버 자원을 관리하지 않는 경우 (업로드 및 다운로드 용량 미 제한)				
조치방법	파일 업로드 및 다운로드 용량을 허용할 수 있는 최소 범위로 설정				
보안설정방법					
■ Windows NT, 2000, 2003 1. 시작> 실행> SERVICES.MSC> IISADMIN> 속성> [일반] 탭에서 서비스 중지 2. %systemroot%\system32\inetpub\MetaBase.xml 파일을 찾아 편집기로 OPEN 3. AspMaxRequestEntityAllowed 값을 찾아 파일 업로드 용량을 최소 범위로 제한 4. AspBufferingLimit 값을 찾아 파일 다운로드 용량을 최소 범위로 제한 5. 시작> 실행> SERVICES.MSC> IISADMIN> 속성> [일반] 탭에서 서비스 시작					

윈도우즈 서버



■ Windows 2008

1. 등록된 웹 사이트의 루트 디렉터리에 있는 web.config 파일 내 아래 항목 추가
(web.config 파일이 없으면 사이트 홈 디렉터리에 새로 생성)

```
<configuration>
  <system.webServer>
    <security>
      <requestFiltering>
        <requestLimits maxAllowedContentLength="콘텐츠용량" />
      </requestFiltering>
    </security>
  </system.webServer>
</configuration>
```

%systemroot%\system32\inetsrv\config\applicationhost.config 파일 내 아래 항목 추가

```
<system.webServer>
  <asp>
    <limits bufferingLimit="파일다운로드용량" maxRequestEntityAllowed="파일업로드용량" />
  </asp>
</system.webServer>
```

윈도우즈 서버

※ Default 설정 값

- (1) `maxAllowedContentLength` (콘텐츠 용량) => Default: 30MB
- (2) `MaxRequestEntityAllowed` (파일 업로드 용량) => Default: 200000 byte
- (3) `bufferingLimit` (파일 다운로드 용량) => Default: 4MB(4194304 byte)

조치 시 영향	일반적으로 영향 없음
----------------	-------------

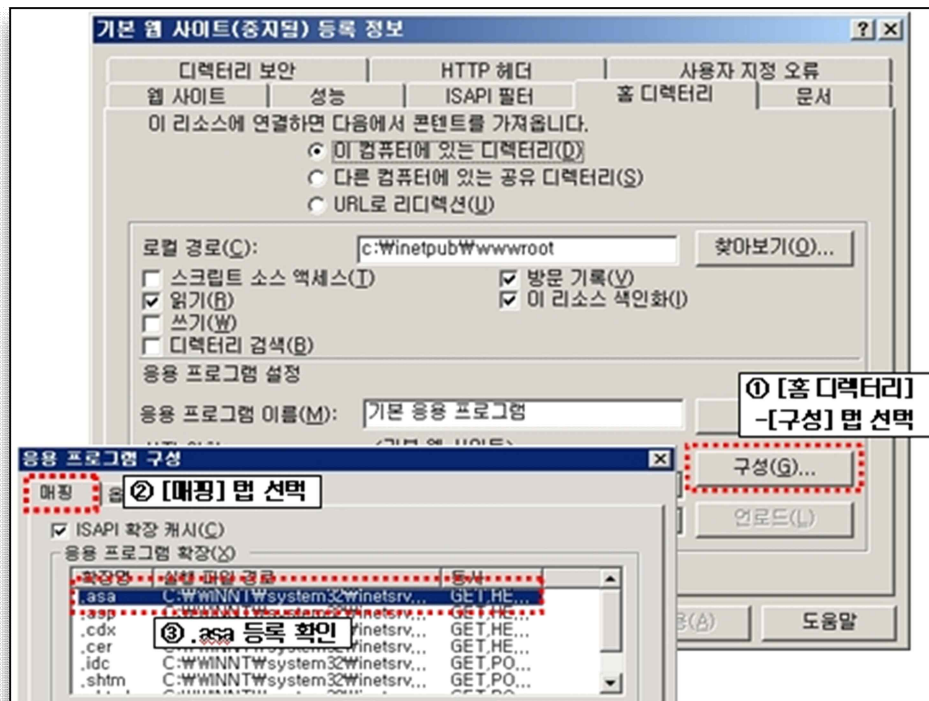
윈도우즈 서버

취약점 항목	2.12. IIS DB 연결 취약점 점검				
대상 OS	NT, 2000, 2003, 2008	위험도	상	Code	W-30
취약점 개요	Global.asa 파일에는 데이터베이스 관련 정보(IP 주소, DB명, 패스워드), 내부 IP 주소, 웹 애플리케이션 환경설정 정보 및 기타 정보 등 보안상 민감한 내용이 포함되어 있으므로 해당 파일이 악의적인 사용자에게 노출될 경우 침해사고로 이어질 수 있음.				
보안대책					
판단기준	양호: .asa 매핑이 존재하는 경우				
	취약: .asa 매핑이 존재하지 않는 경우 ※ 조치 시 마스터 속성과 모든 사이트에 적용함				
조치방법	사용하지 않는 경우 IIS 서비스 중지, 사용할 경우 .asa 매핑을 아래 그림과 같이 추가				
보안설정방법					

■ IIS 5.0, 6.0

1. asa 매핑 등록 확인

인터넷 정보 서비스(IIS) 관리자> 웹 사이트> 해당 웹 사이트> 속성> [홈 디렉터리] 탭에서 구성> [매핑] 탭 선택 후 .asa 매핑이 등록되어 있는지 확인



2. asa 매핑 등록되어 있지 않은 경우 asa 매핑 등록

인터넷 정보 서비스(IIS) 관리자> 웹 사이트> 해당 웹 사이트> 속성> [홈 디렉터리] 탭에서 구성> [매핑] 탭> [추가] 버튼을 클릭하여 asa 매핑 등록

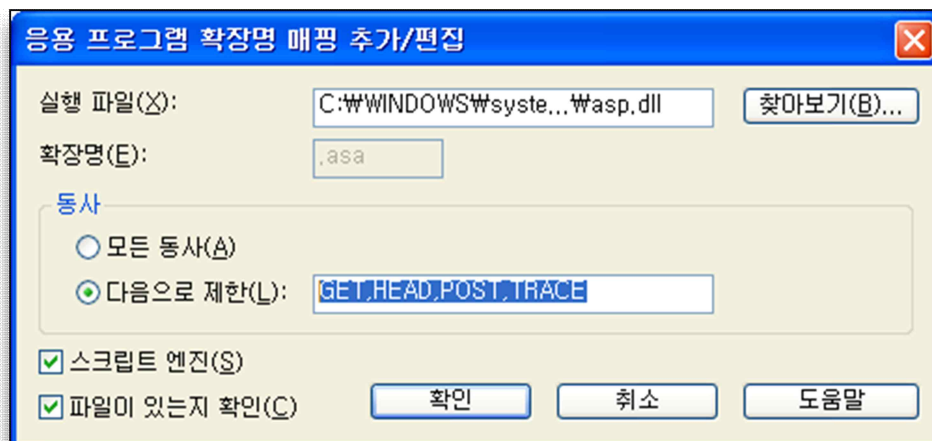
윈도우즈 서버

실행 파일: %SystemRoot%\System32\Inetsrv\asp.dll

확장명: .asa

동사 다음으로 제한: GET,HEAD,POST,TRACE

스크립트 엔진(체크), 파일이 있는지 확인(체크)



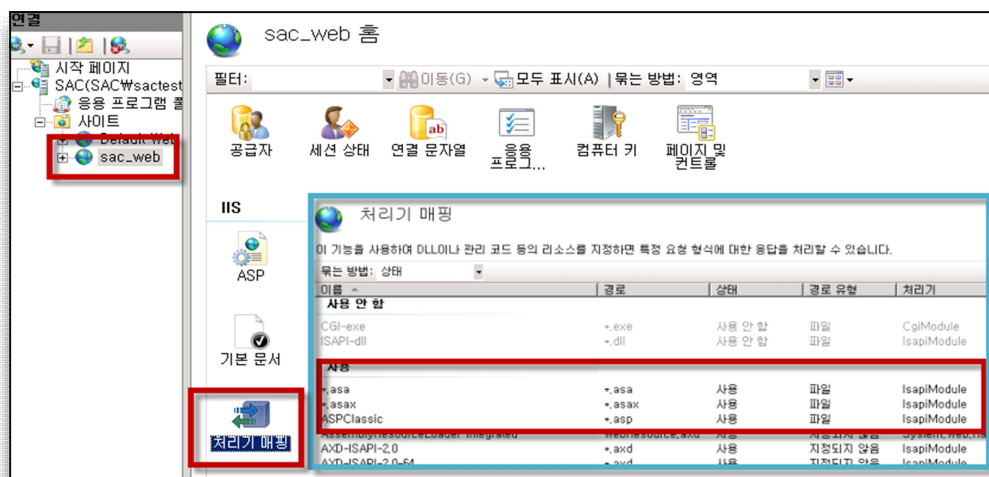
■ IIS 7.0

총 2가지 항목에서 확인 필요

2가지 항목이 모두 아래의 방법(가, 나)과 같이 설정되어 있을 경우 취약하다고 볼 수 있으며, 한 가지 경우라도 설정이 되어있지 않거나 해당 설정이 없을 시 양호하다고 판단함

1. asa / asax 스크립트 매핑 확인

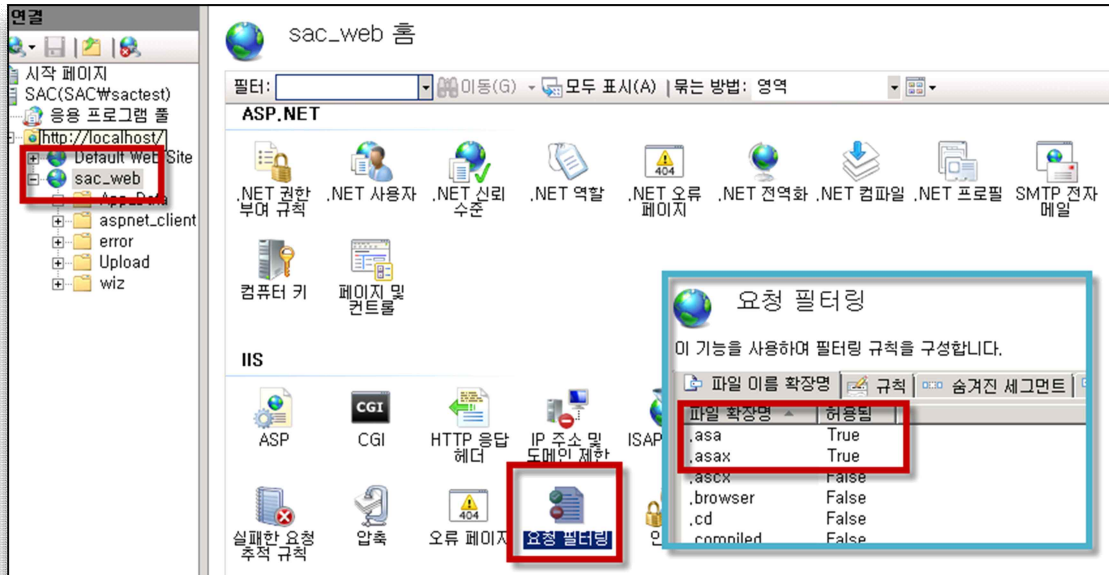
인터넷 정보 서비스(IIS) 관리자> 해당 웹 사이트> IIS> "처리기 매핑" 선택,
사용 항목에 *.asa / *.asax가 사용 상태로 등록되어 있는지 확인



윈도우즈 서버

2. asa / asax 파일 필터링 확인

인터넷 정보 서비스(IIS) 관리자> 해당 웹 사이트> IIS> “요청 필터링” 선택,
.asa / .asax 확장자가 True로 설정되어 있는지 확인



3. 조치방법

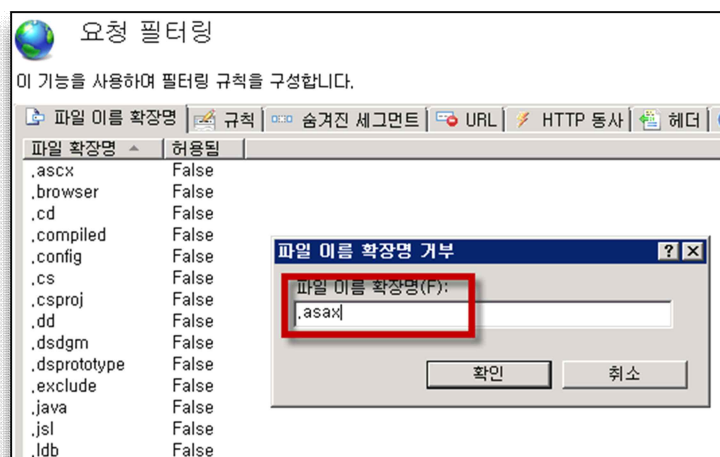
Global.asa / Global.asax 파일을 사용하지 않는 경우 처리기 매핑에서 *.asa / *.asax 파일을 사용 안 함으로 설정, 파일을 사용해야 하는 경우 요청 필터링에서 해당 확장자를 False로 설정

가. asa / asax 스크립트 매핑 해제

인터넷 정보 서비스(IIS) 관리자> 해당 웹 사이트> IIS> “처리기 매핑” 선택,
사용 항목에 *.asa / *.asax를 선택하여 우측 [작업] 탭에서 제거

나. asa / asax 파일 필터링

인터넷 정보 서비스(IIS) 관리자> 해당 웹 사이트> IIS> “요청 필터링” 선택,
우측 [작업] 탭에서 “파일 이름 확장명 거부” 선택하여 .asa / .asax 확장자 등록



조치 시 영향

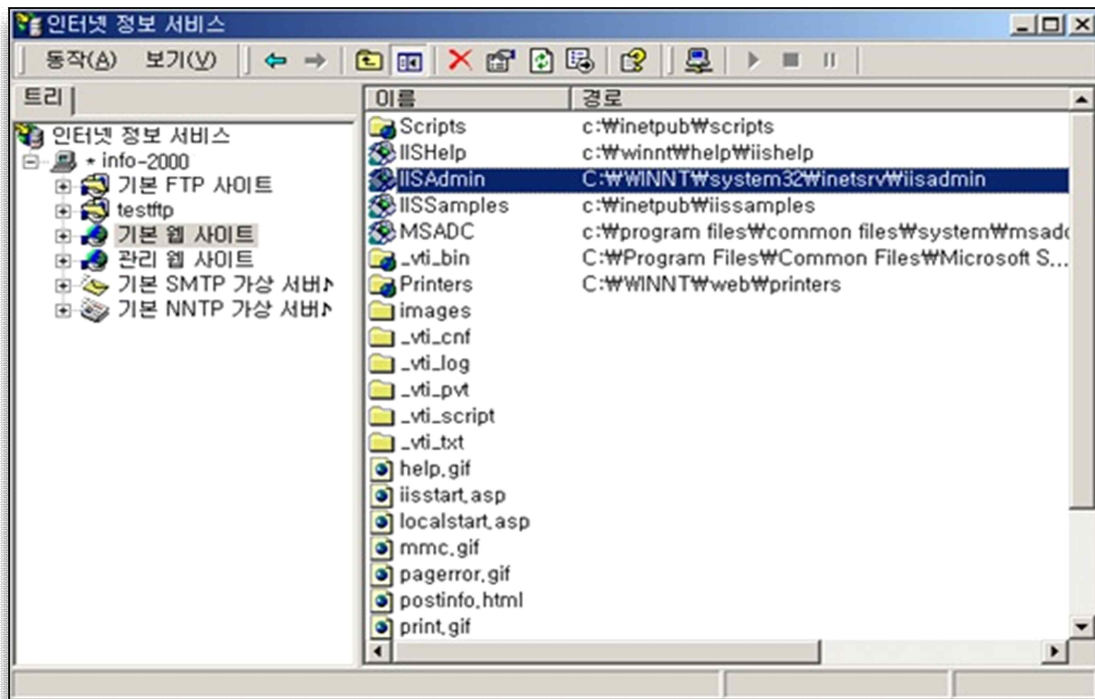
일반적으로 영향 없음

윈도우즈 서버

취약점 항목	2.13. IIS 가상 디렉터리 삭제				
대상 OS	NT, 2000, 2003, 2008	위험도	상	Code	W-31
취약점 개요	IIS 4.0, 5.0 설치 시 기본적으로 /issadmpwd라는 가상 디렉터리를 생성하는데, 이 디렉터리에는 웹 서버를 통하여 패스워드를 변경시켜주는 기능 등을 하는 .HTR 파일이 존재함. 이러한 기능들이 필요하지 않을 경우 /issadmpwd를 제거하고 이 외 존재하는 취약점을 줄이기 위해서 IIS Admin에 관계되는 모든 파일 및 디렉터리를 삭제하여야 함.				
보안대책					
판단기준	양호: 해당 웹 사이트에 IIS Admin, IIS Adminpwd 가상 디렉터리가 존재하지 않는 경우 취약: 해당 웹 사이트에 IIS Admin, IIS Adminpwd 가상 디렉터리가 존재하는 경우 ※ 조치 시 마스터 속성과 모든 사이트에 적용함				
조치방법	사용하지 않는 경우 IIS 서비스 중지, 사용할 경우 IIS Admin, IIS Adminpwd 삭제				
보안설정방법					

■ IIS 5.0

1. 시작> 실행> INETMGR> 웹 사이트> IISAdmin, IISAdminpwd 선택> 삭제



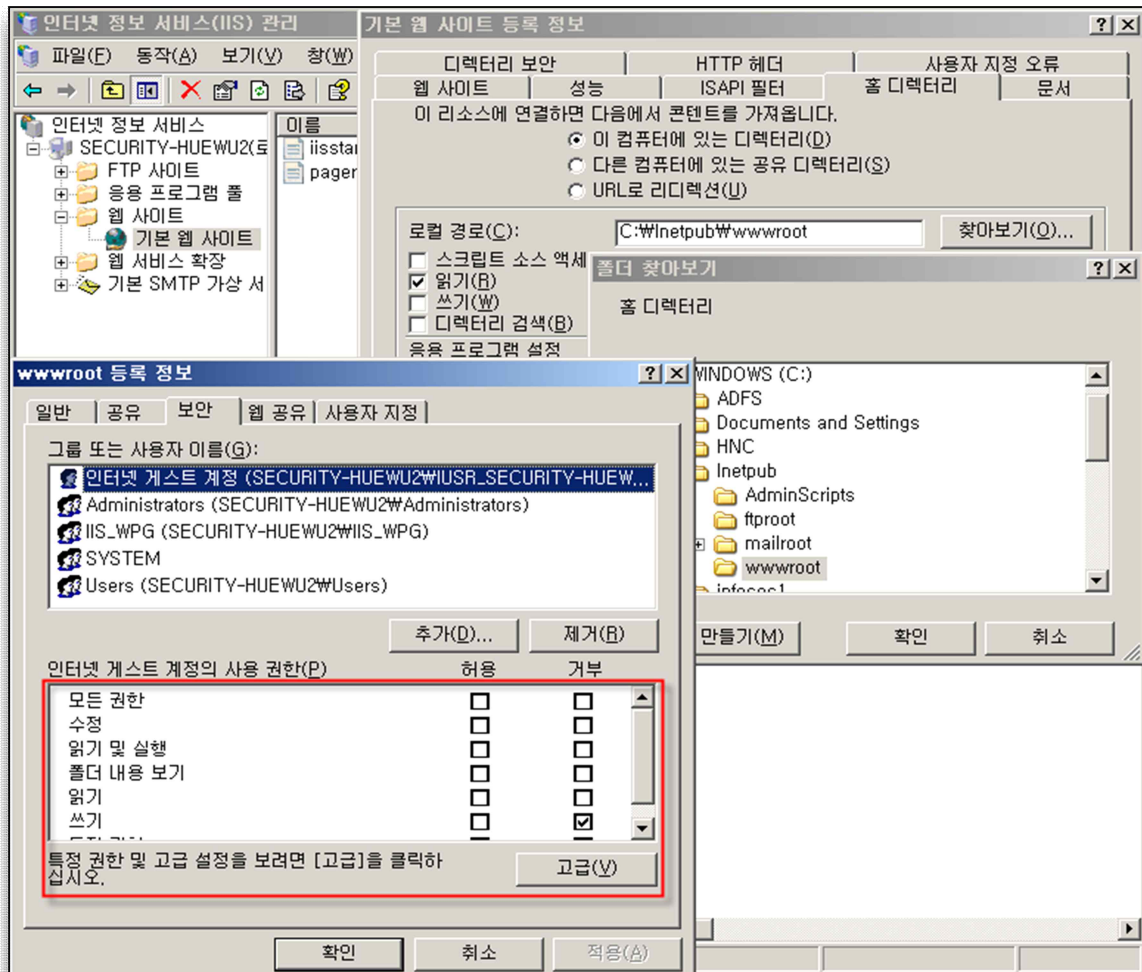
※ IIS 6.0 이상 버전 해당 사항 없음

조치 시 영향	일반적으로 IIS 관리용 페이지를 사용하지 않으므로 영향 없음
---------	------------------------------------

윈도우즈 서버

취약점 항목	2.14. IIS 데이터 파일 ACL 적용				
대상 OS	NT, 2000, 2003, 2008	위험도	상	Code	W-32
취약점 개요	웹 데이터 파일에 *ACL을 부여함으로써 권한 없는 사용자로부터의 실행 및 읽기 제한을 설정할 수 있음. 향후 필요에 의해 IIS를 설치하여 운용한다면 웹 데이터 파일에 대한 ACL을 부여하는 것이 바람직하며 ACL을 설정할 때에는 다음과 같은 사항을 참고하여 설정하여야 함. 1. 가능한 파일의 종류끼리 분류하여 폴더에 저장하는 것이 좋음. 2. 홈 디렉터리(기본: c:\inetpub\wwwroot)내에 적절한 ACL 권한을 부여함. *ACL(Access Control List): 접근이 허가된 주체들과 허가받은 접근 종류들이 기록된 목록.				
보안대책					
판단기준	양호: 홈 디렉터리 내에 있는 하위 파일들에 대해 Everyone 권한이 존재하지 않는 경우 (정적 콘텐츠 파일은 Read 권한만)				
	취약: 홈 디렉터리 내에 있는 하위 파일들에 대해 Everyone 권한이 존재하는 경우 (정적 콘텐츠 파일은 Read 권한 제외) ※ 조치 시 마스터 속성과 모든 사이트에 적용함				
조치방법	IIS 서비스를 사용하지 않는 경우 IIS 서비스 중지, 사용할 경우 홈 디렉터리에 Administrators, System 권한만 설정 후 하위 디렉터리에 존재하는 모든 Everyone 권한 제거 (정적 콘텐츠 파일에 경우 Read 권한 허용)				
보안설정방법					
■ IIS 5.0, 6.0					
1. 시작> 실행> INETMGR> 웹 사이트> 해당 웹 사이트> 속성> 홈 디렉터리					
2. 탐색기를 이용하여 홈 디렉터리의 등록 정보> [보안] 탭에서 권한 확인					
3. 아래와 같은 파일들에 대한 불필요한 Everyone 권한 제어					
파일 형식		액세스 제어 목록			
CGI (.exe, .dll, .cmd, .pl)		모든 사람(X), 관리자/시스템(전체 제어)			
스크립트 파일(.asp)		모든 사람(X), 관리자/시스템(전체 제어)			
포함 파일(.inc, .shtm, .shtml)		모든 사람(X), 관리자/시스템(전체 제어)			
정적 콘텐츠(.txt, .gif, .jpg, .html)		모든 사람(R), 관리자/시스템(전체 제어)			

윈도우즈 서버

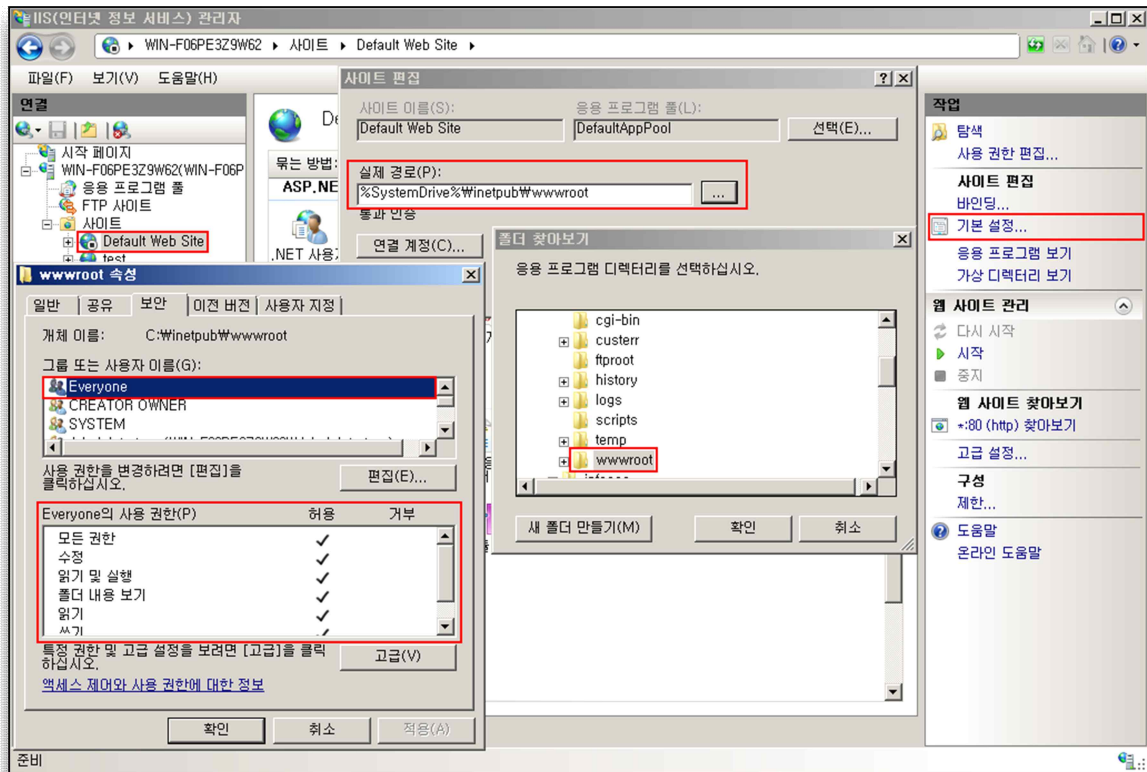


■ IIS 7.0

1. 시작 > 실행 > INETMGR > 사이트 > 해당 웹 사이트 > 기본 설정 > 실제 경로 확인
2. 탐색기를 이용하여 홈 디렉터리의 등록 정보 > [보안] 탭에서 권한 확인
3. 아래와 같은 파일들에 대한 불필요한 Everyone 권한 제어

파일 형식	액세스 제어 목록
CGI (.exe, .dll, .cmd, .pl)	모든 사람(X), 관리자/시스템(전체 제어)
스크립트 파일(.asp)	모든 사람(X), 관리자/시스템(전체 제어)

윈도즈 서버



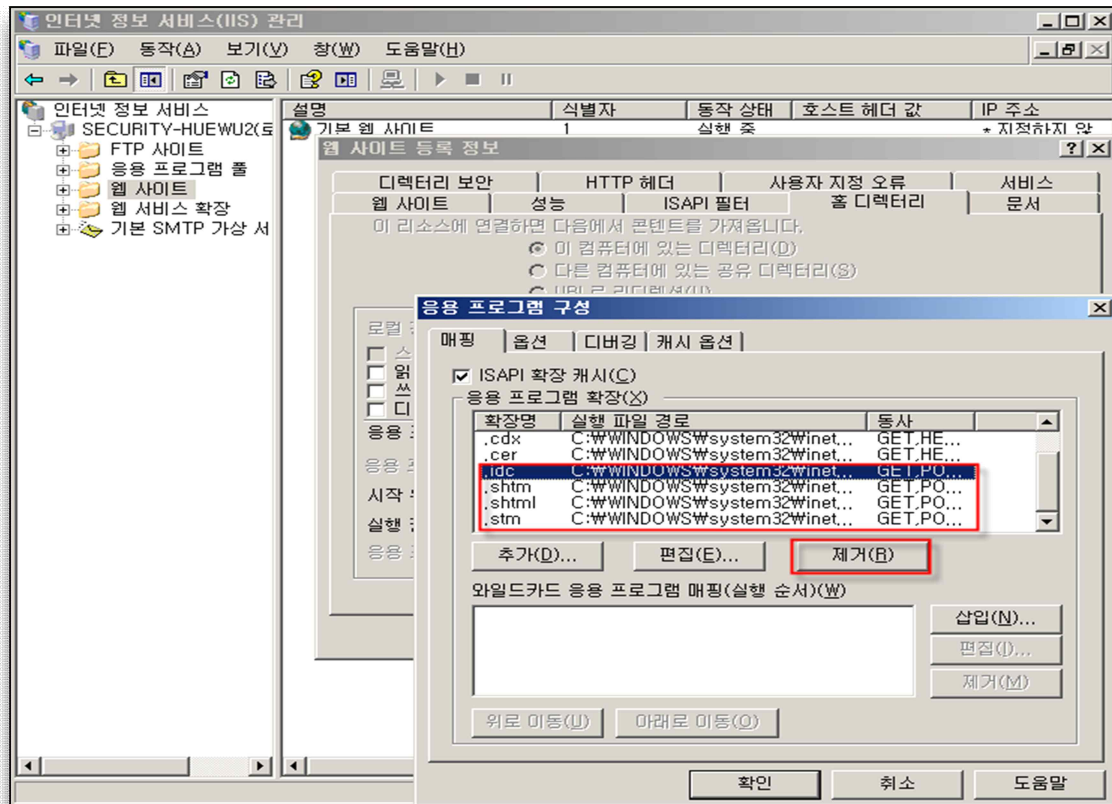
조치 시 영향

IIS에서 홈 디렉터리 내에 있는 데이터 파일 권한 조치에 따른 검증 필요

윈도우즈 서버

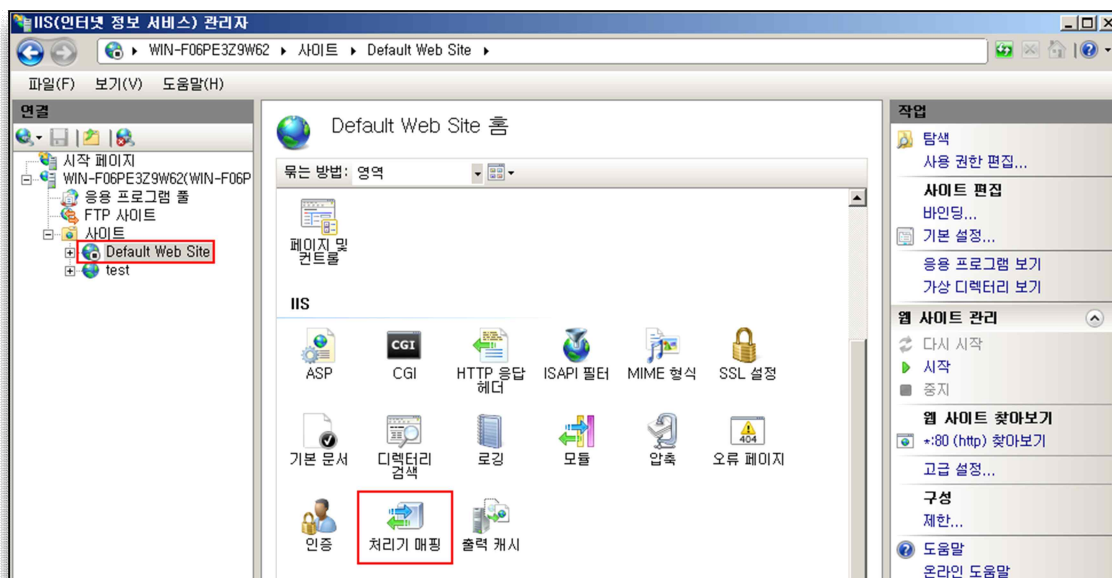
취약점 항목		2.15. IIS 미사용 스크립트 매핑 제거				
대상 OS	NT, 2000, 2003, 2008	위험도	상	Code	W-33	
취약점 개요	사용하지 않는 스크립트 매핑은 보안에 위협이 될 수 있으므로 개발자와 협의하여 불필요한 매핑인지 확인한 후 제거함.					
	.asp나 .shtm 과 같은 확장자들은 특정 DLL 파일과 매핑 되어 있어, 이러한 파일들에 대한 요청이 들어오면 해당 DLL에 의해 처리됨. 이러한 매핑 중 사용되지 않는 것들은 제거하면 보안에 도움이 되며, 특히, .ida, .idc, .idq, .printer, .htr, .htw 확장자는 *버퍼 오버플로우(Buffer Overflow) 공격 위험이 존재하므로 삭제를 권고함.					
	*버퍼 오버플로우(Buffer Overflow): 메모리에 할당된 버퍼의 양을 초과하는 데이터를 입력하여 프로그램의 복귀 주소를 조작, 궁극적으로 해커가 원하는 코드를 실행하는 것.					
보안대책						
판단기준	양호: 취약한 매핑(.htr .idc .stm .shtm .shtml .printer .htw .ida .idq)이 존재하지 않는 경우 취약: 취약한 매핑(.htr .idc .stm .shtm .shtml .printer .htw .ida .idq)이 존재하는 경우 ※ 조치 시 마스터 속성과 모든 사이트에 적용함					
조치방법	사용하지 않는 경우 IIS 서비스 중지, 사용할 경우 취약한 매핑 제거 (아래 표 참고)					
보안설정방법						
■ IIS 5.0, 6.0						
1. 시작> 실행> INETMGR> 웹 사이트> 해당 웹 사이트> 속성> [홈 디렉터리] 탭에서 [구성] 버튼 선택						
2. [매핑] 탭에서 아래와 같은 취약한 매핑 제거						
확장자명	기능		취약점			
asp	Active Server Pages 기능 지원		Buffer Overflow MS02-018 • Win 2000 SP3 이상 양호			
htr	Web-based password reset: Outlook Web Access 등에서 웹 기반 응용 프로그램으로 자신의 사용자 계정 암호 변경		+.htr 소스 공개 취약점 MS01-004 • Win 2000 SP3, NT SP 7.0 이상 양호			
idc	Internet Database Connector: SQL 서버에 연결하기 위한 정보 등을 관리함. asp를 통해 같은 작업을 수행 가능		Web 디렉터리 패스 공개 Q193689 • NT4.0, NT SP6a이상 양호			
stm, stml, shtml	Server-Side Includes		Buffer Overflow MS01-044 • Win 2000 SP3 이상 양호			
printer	Internet Printing : URL을 사용하여 페이지를 프린터로 인쇄할 수 있도록 함 IIS가 인터넷이나 인트라넷을 통해 인쇄 서버 기능 수행		Buffer Overflow MS01-023 • Win 2000 SP2 이상 양호			
ida, idq	Index Server : idq.dll에 매핑되며 인덱스 서버를 쿼리할 때 사용		Buffer Overflow MS01-033 • Win 2000 SP3 이상 양호			
htw	Index Server : webhits.dll에 매핑되며, 인덱스 서버를 쿼리할 때 사용		Webhit 소스 공개 취약점 MS00-006 • Win 2000 SP1 이상 양호			

윈도즈 서버

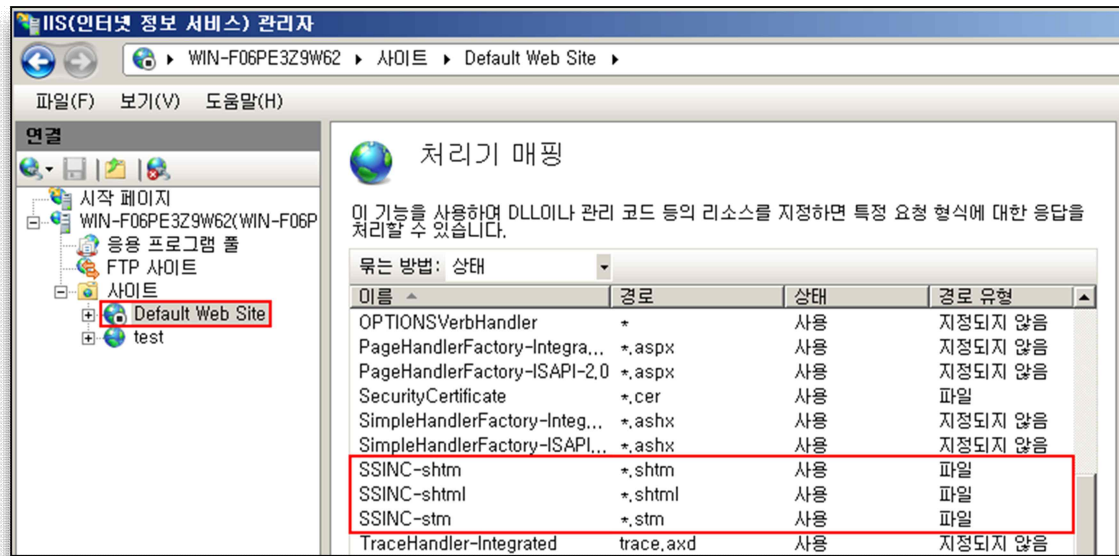


■ IIS 7.0

1. 시작 > 실행 > INETMGR > 웹 사이트 > 해당 웹 사이트 > 처리기 매핑 선택
2. 취약한 매핑 제거 (.httr, .idc, .stm, .shtm, .shtml, .printer, .htw, .ida, .idq)



윈도우즈 서버



조치 시 영향

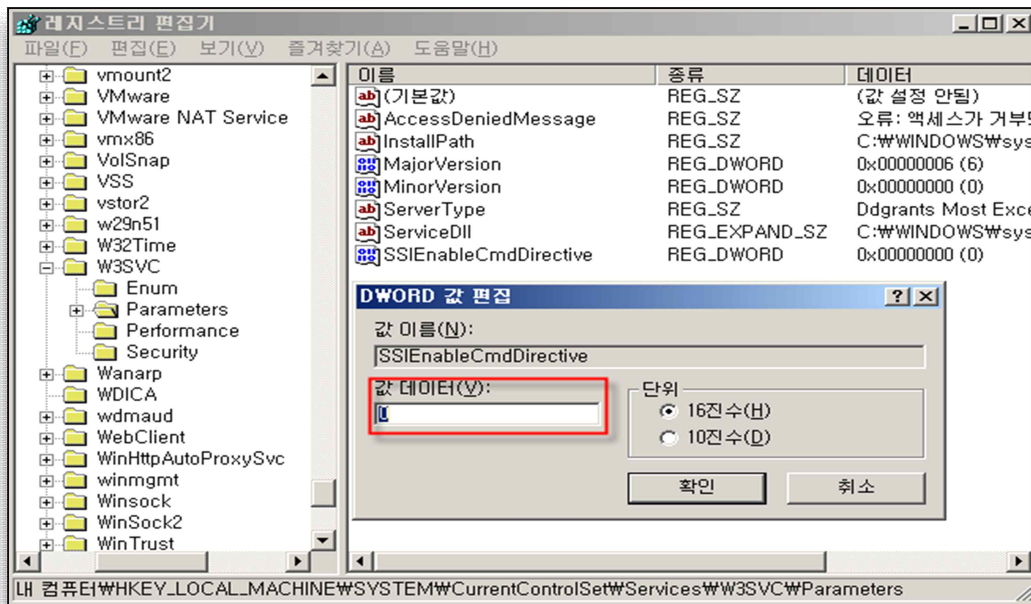
일반적인 경우 영향 없음

윈도우즈 서버

취약점 항목	2.16. IIS Exec 명령어 쉘 호출 진단				
대상 OS	NT, 2000	위험도	상	Code	W-34
취약점 개요	명령어가 Web 서버에서 임의의 명령을 호출하여 허가되지 않은 파일을 실행하도록 사용될 수 있음. 임의의 명령을 호출하도록 설정되어 있다면 아래의 조치 방법에 따라서 설정을 변경하여 주는 것이 안전함.				
보안대책					
판단기준	양호: IIS 5.0 버전에서 해당 레지스트리 값이 0이거나, IIS 6.0 버전 이상인 경우				
	취약: IIS 5.0 버전에서 해당 레지스트리 값이 1인 경우				
조치방법	위의 양호 기준에 맞춰 레지스트리 값 설정				
보안설정방법					

■ Windows NT, 2000

1. 시작> 실행> REGEDIT> HKLM\SYSTEM\CurrentControlSet\Services\W3SVC\Parameters 검색
2. DWORD> SSIEnableCmdDirective 값을 찾아 값을 "0"으로 입력



※ IIS 6.0 이상 버전 해당 사항 없음

조치 시 영향	일반적인 경우 영향 없음
---------	---------------

윈도우즈 서버

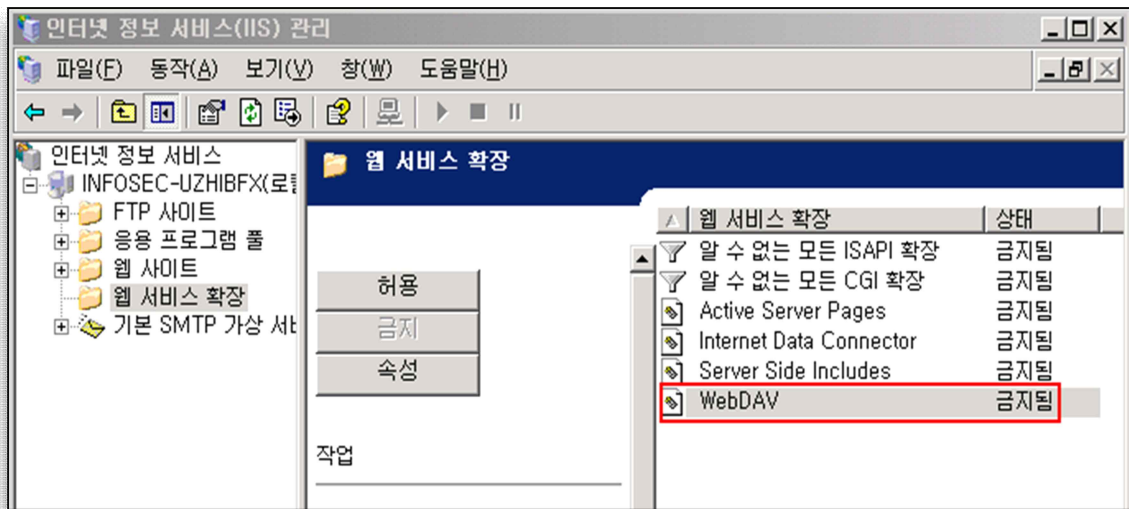
취약점 항목	2.17. IIS WebDAV 비활성화				
대상 OS	NT, 2000, 2003, 2008	위험도	상	Code	W-35
취약점 개요	악의적으로 작성된 요청을 이용하여 특별한 방식으로 인증을 우회할 경우 패스워드로 보호된 *WebDAV의 자원에 접근할 수 있음. 또한, 매개 변수를 정확하게 점검하지 않는 WebDAV에 의해 호출된 구성 요소 중 하나에 결함이 존재하며, 이로 인해 버퍼 오버런이 일어날 수 있음. *WebDAV(Web Distributed Authoring and Versioning): 웹상의 공동개발을 지원하기 위한 IETF 표준안(RFC 2518)으로서, 원격지 사용자들 간에 인터넷상에서 파일을 공동 편집하고 관리할 수 있도록 해줌.				
보안대책					
판단기준	양호: 다음 중 한 가지라도 해당하는 경우 1. IIS 서비스를 사용하지 않는 경우 2. DisableWebDAV 값이 1로 설정되어 있는 경우 3. Windows NT, 2000은 서비스팩 4 이상이 설치되어 있는 경우 4. Windows 2003, Windows 2008은 WebDAV가 금지 되어 있는 경우 취약: 양호 기준에 한 가지라도 해당하지 않는 경우(2003, 2008은 1,4번만)				
조치방법	IIS 서비스를 사용하지 않는 경우 IIS 서비스 중지, 사용할 경우 해당 레지스트리 값을 1로 설정함 (Windows NT, 2000 서비스팩 4 이상 양호, Windows 2003 WebDAV가 금지 시 양호, Windows XP 서비스팩 2이상 양호)				
보안설정방법					
■ Windows NT, 2000 1. 시작> 실행> SERVICES.MSC> World Wide Web Publishing Service> 속성 2. 시작 유형 → 사용 안 함 서비스 상태 → 중지 < IIS를 사용하지만 WebDAV를 사용하지 않는 경우 > 1. 시작> 실행> REGEDIT 실행 2. HKLM\SYSTEM\CurrentControlSet\Services\W3SVC\Parameters 3. 마우스 우클릭> 새로 만들기 DWORD 값을 선택 4. DisableWebDAV 입력 (Default 값인 "0"을 "1"로 변경) < IIS를 사용하고, WebDAV도 필요한 경우 > 1. Windows NT인 경우 - 아래 사이트에서 패치를 받아 설치함 http://211.234.93.190/korea/technet/security/bulletin/MS03-007.asp#top 2. Windows 2000 서비스팩 버전이 2인 경우 - 아래 사이트에서 패치를 받아 설치함 http://211.234.93.190/korea/technet/security/bulletin/MS03-013.asp					

윈도우즈 서버

3. Windows 2000 서비스팩 버전이 3인 경우 - 아래 사이트에서 패치를 받아 설치함
<http://211.234.93.190/korea/technet/security/bulletin/MS03-007.asp#top>
4. Windows 2000 서비스팩 버전이 4인 경우 - 취약점 없음
※ 시스템 재시작 후 적용됨

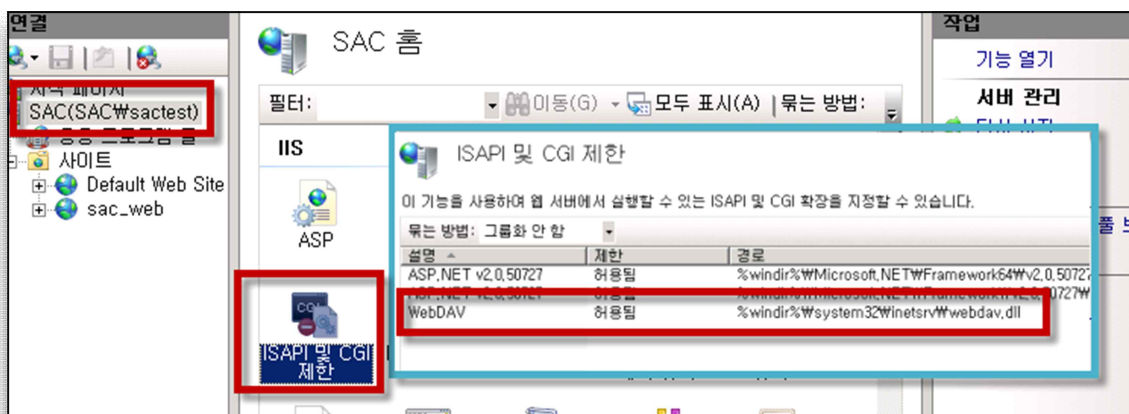
■ Windows 2003

1. 시작> 실행> INETMGR> 웹 사이트> 웹 서비스 확장
2. WebDAV 금지



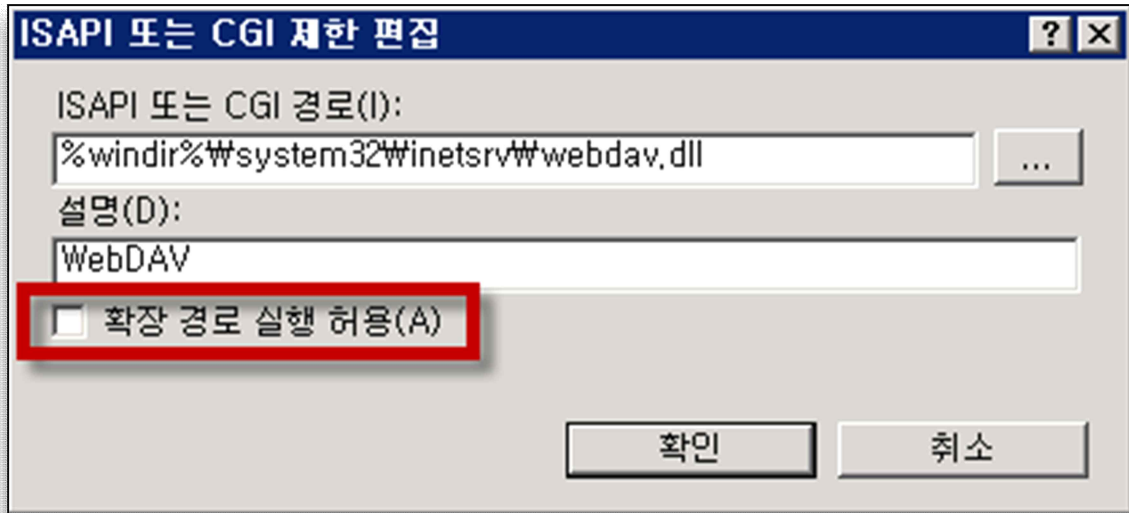
■ Windows 2008

1. 인터넷 정보 서비스(IIS) 관리자> 서버 선택> IIS> "ISAPI 및 CGI 제한" 선택,
WebDAV 사용여부 확인 (허용됨 -> 취약)



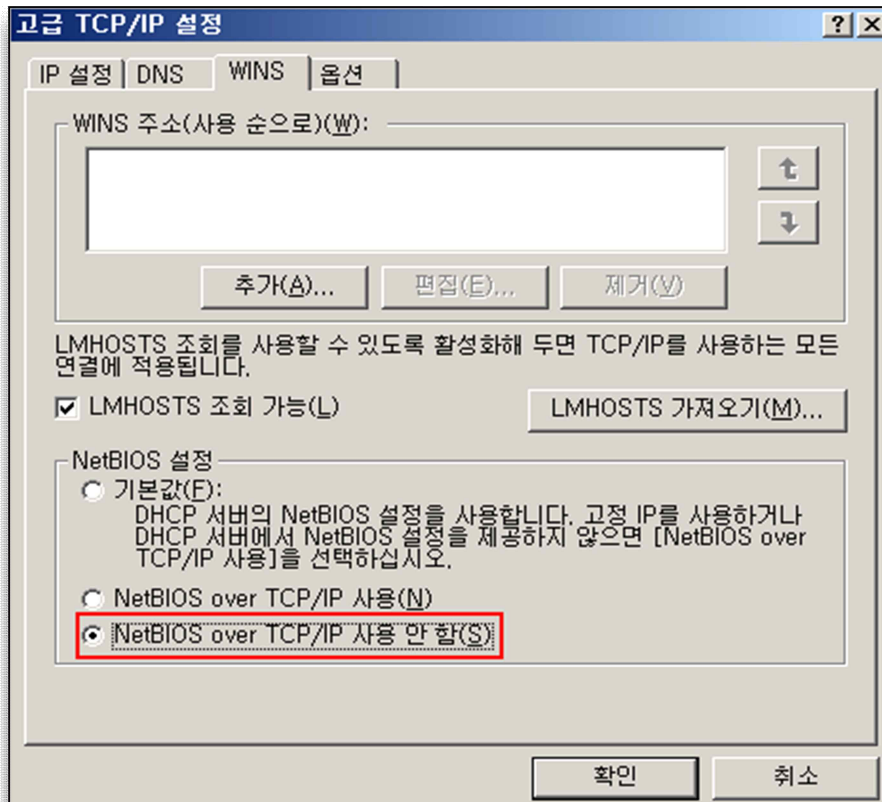
2. 인터넷 정보 서비스(IIS) 관리자> 서버 선택> IIS> "ISAPI 및 CGI 제한" 선택
WebDAV 항목 선택> [작업]에서 제거하거나, 편집> "확장 경로 실행 허용(A)" 체크 해제

윈도우즈 서버



조치 시 영향	일반적으로 사용하지 않는 기능임
---------	-------------------

윈도우즈 서버

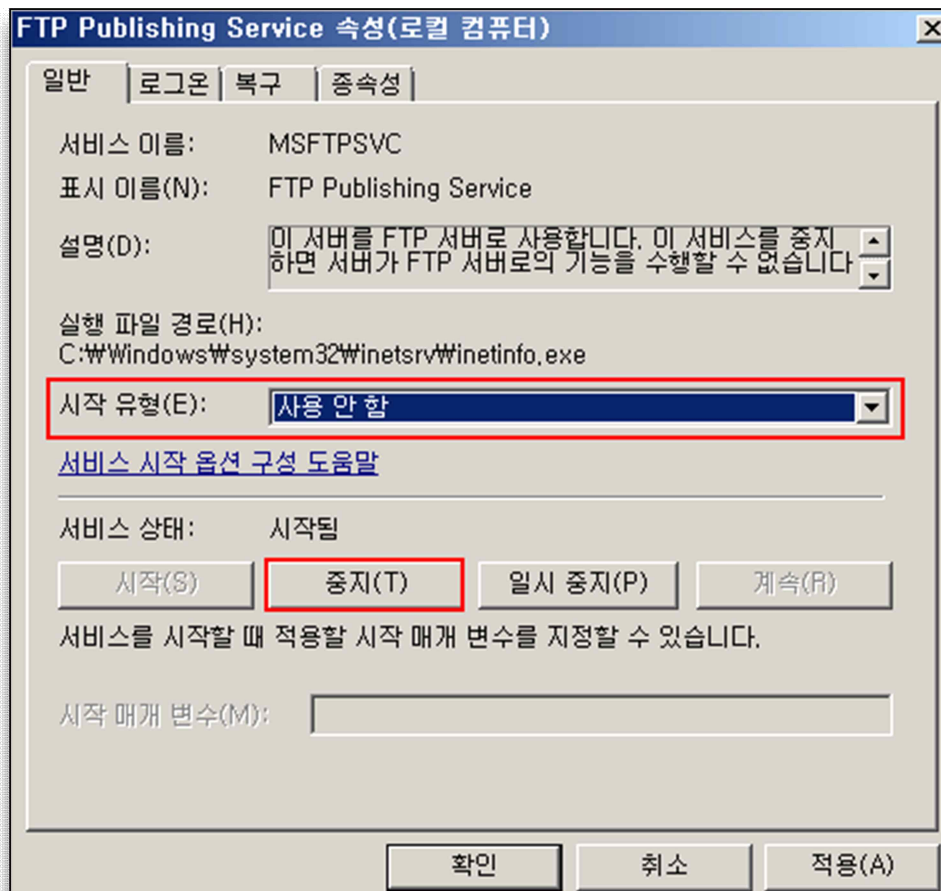
취약점 항목	2.18. NetBIOS 바인딩 서비스 구동 점검				
대상 OS	NT, 2000, 2003, 2008	위험도	상	Code	W-36
취약점 개요	NetBIOS(Network Basic Input/Output System)는 IBM PC를 위한 네트워크 인터페이스 체계로 네임, 세션, 데이터그램의 세 가지 서비스를 제공하고 있음. 윈도우 NT 시스템이 인터넷에 직접 연결되어 있으면 공격자가 쉽게 파일시스템을 사용할 수 있으므로 NetBIOS에 대한 접근 통제가 적용되어야 함.				
보안대책					
판단기준	양호: TCP/IP와 NetBIOS 간의 바인딩이 제거 되어 있는 경우 취약: TCP/IP와 NetBIOS 간의 바인딩이 제거 되어있지 않은 경우				
조치방법	네트워크 제어판을 이용하여 TCP/IP와 NetBIOS 간의 바인딩(binding) 제거				
보안설정방법					
■ Windows NT, 2000, 2003, 2008 1. 시작> 실행> ncpa.cpl> 로컬 영역 연결> 속성> TCP/IP> [일반] 탭에서 [고급] 클릭> [WINS] 탭에서 TCP/IP에서 "NetBIOS 사용 안 함" 또는, "NetBIOS over TCP/IP 사용 안 함" 선택					
					
조치 시 영향	TCP/IP를 거치게 되는 파일 공유 서비스가 제공되지 않음 인터넷에서의 공유 자원에 대한 접근시도가 불가능함 (라우터를 거치지 않은 내부 네트워크에서는 가능함)				

윈도우즈 서버

취약점 항목	2.19. FTP 서비스 구동 점검				
대상 OS	NT, 2000, 2003, 2008	위험도	상	Code	W-37
취약점 개요	기본적인 FTP 서비스는 계정과 패스워드가 암호화되지 않은 채로 전송되어 간단한 *Sniffer에 의해서도 스니핑이 가능하므로 FTP 서비스를 사용하지 않을 것을 권고함. *Sniffer: 네트워크 트래픽을 감시하고 분석하는 프로그램.				
보안대책					
판단기준	양호: FTP 서비스를 사용하지 않는 경우				
	취약: FTP 서비스를 사용하는 경우				
조치방법	FTP 서비스가 필요하지 않다면 서비스 중지				
보안설정방법					

■ Windows NT, 2000, 2003, 2008

1. 시작 > 실행 > SERVICES.MSC > FTP Publishing Service > 속성 > [일반] 탭에서 "시작 유형"을 "사용 안 함"으로 설정한 후, FTP 서비스 중지



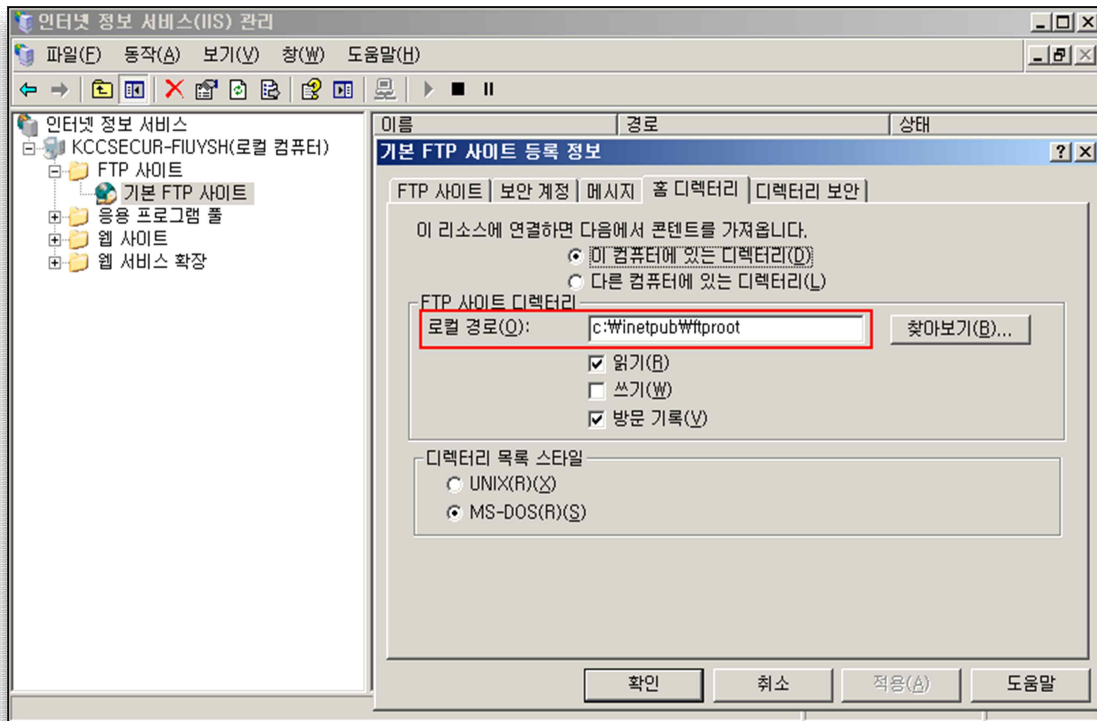
조치 시 영향: 일반적으로 영향 없음

윈도우즈 서버

취약점 항목	2.20. FTP 디렉터리 접근권한 설정				
대상 OS	NT, 2000, 2003, 2008	위험도	상	Code	W-38
취약점 개요	홈 디렉터리에 쓰기 권한이 주어진 경우 임의의 사용자가 쓰기, 수정이 가능하므로 정보유출, 파일 위·변조로 인한 피해가 발생할 수 있음.				
보안대책					
판단기준	양호: FTP 홈 디렉터리에 Everyone 권한이 없는 경우				
	취약: FTP 홈 디렉터리에 Everyone 권한이 있는 경우				
조치방법	FTP 홈 디렉터리에서 Everyone 권한 삭제, 각 사용자에게 적절한 권한 부여				
보안설정방법					

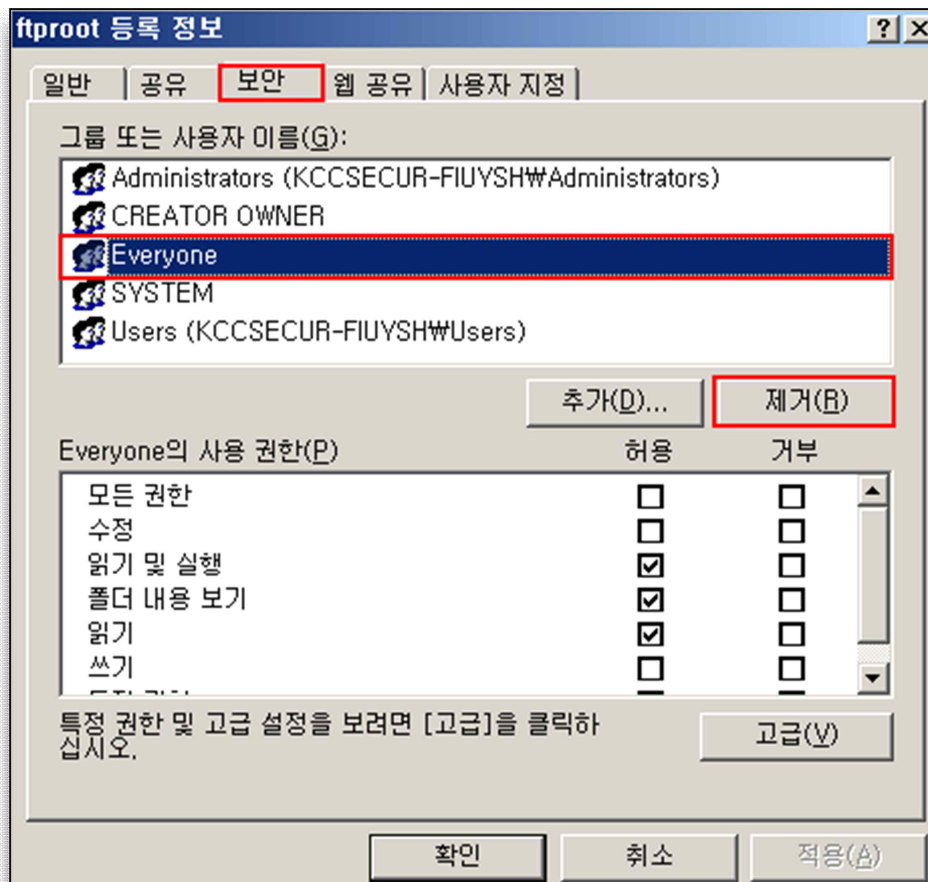
■ Windows NT, 2000, 2003, 2008

1. 인터넷 정보 서비스(IIS) 관리> FTP 사이트> 해당 FTP 사이트> 속성>
[홈 디렉터리] 탭에서 FTP 홈 디렉터리 확인



2. 탐색기> 홈 디렉터리> 속성> [보안] 탭에서 Everyone 권한 제거

윈도우즈 서버



※ IIS 7 이상 버전에서는 FTP 사이트를 별도로 생성하지 않고 기존 웹 사이트에 FTP 사이트를 바인딩 하여 사용함. (관리 도구> 인터넷 정보 서비스(IIS) 6.0 관리자에서 FTP 설정 가능)

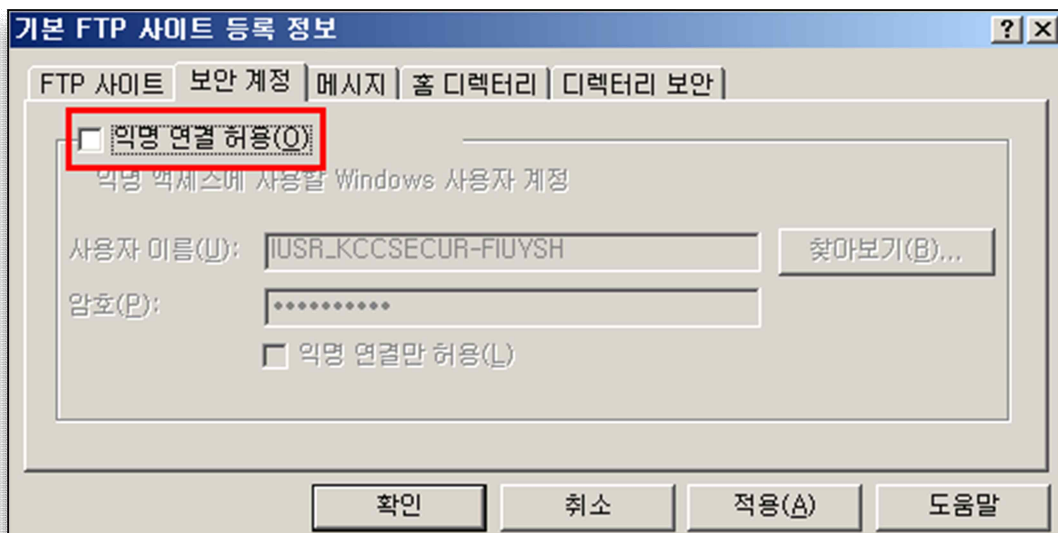
조치 시 영향 | 일반적으로 영향 없음

윈도우즈 서버

취약점 항목	2.21. Anonymous FTP 금지				
대상 OS	NT, 2000, 2003, 2008	위험도	상	Code	W-39
취약점 개요	기본적인 FTP 서비스는 계정과 패스워드가 암호화되지 않은 채로 전송되어 간단한 Sniffer에 의해서도 스니핑이 가능하므로 FTP 서비스를 사용하지 않을 것을 권고. 만약 불가피하게 FTP 서비스를 이용해야 하는 경우 FTP Default 설정이 익명연결 허용을 차단하고, 특정 IP 주소에서 접속하도록 접근제어 설정을 적용하여야 함.				
보안대책					
판단기준	양호: FTP 서비스를 사용하지 않거나, "익명 연결 허용"이 체크되지 않은 경우				
	취약: FTP 서비스를 사용하거나, "익명 연결 허용"이 체크되어 있는 경우				
조치방법	FTP 서비스를 사용하지 않는 경우 서비스 중지, 사용할 경우 "익명 연결 허용" 체크 해제				
보안설정방법					

■ Windows NT, 2000, 2003, 2008

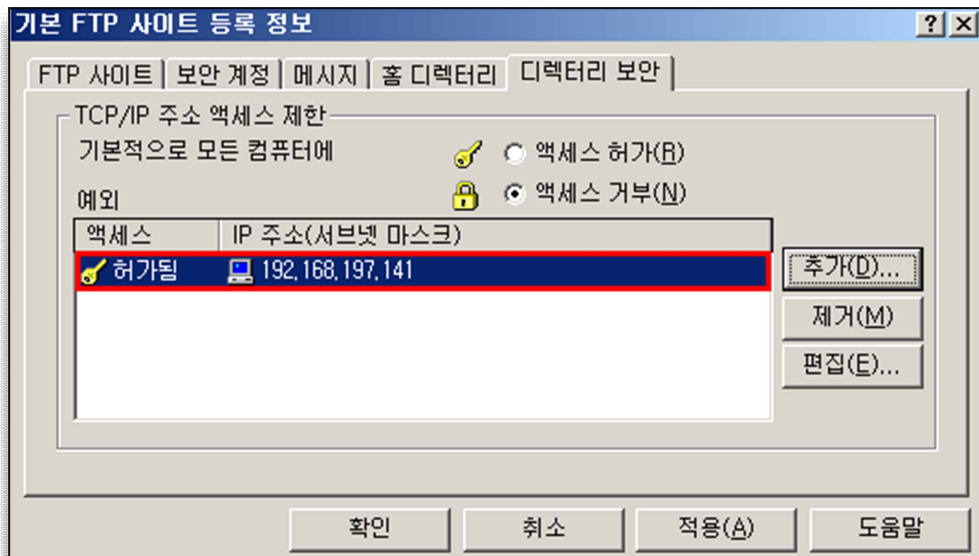
1. 인터넷 정보 서비스(IIS) 관리> FTP 사이트> 속성> [보안 계정] 탭에서 "익명 연결 허용" 체크박스 해제 (만약 개별 FTP 사이트에 적용할 경우 해당 사이트에만 설정이 적용되고, 기본 설정은 적용 받지 않음)



※ IIS 7 이상 버전에서는 FTP 사이트를 별도로 생성하지 않고 기존 웹 사이트에 FTP 사이트를 바인딩 하여 사용함. (관리 도구> 인터넷 정보 서비스(IIS) 6.0 관리자에서 FTP 설정 가능)

조치 시 영향	애플리케이션에서 익명 연결을 사용할 경우를 제외하고, 일반적으로 영향 없음
---------	---

윈도우즈 서버

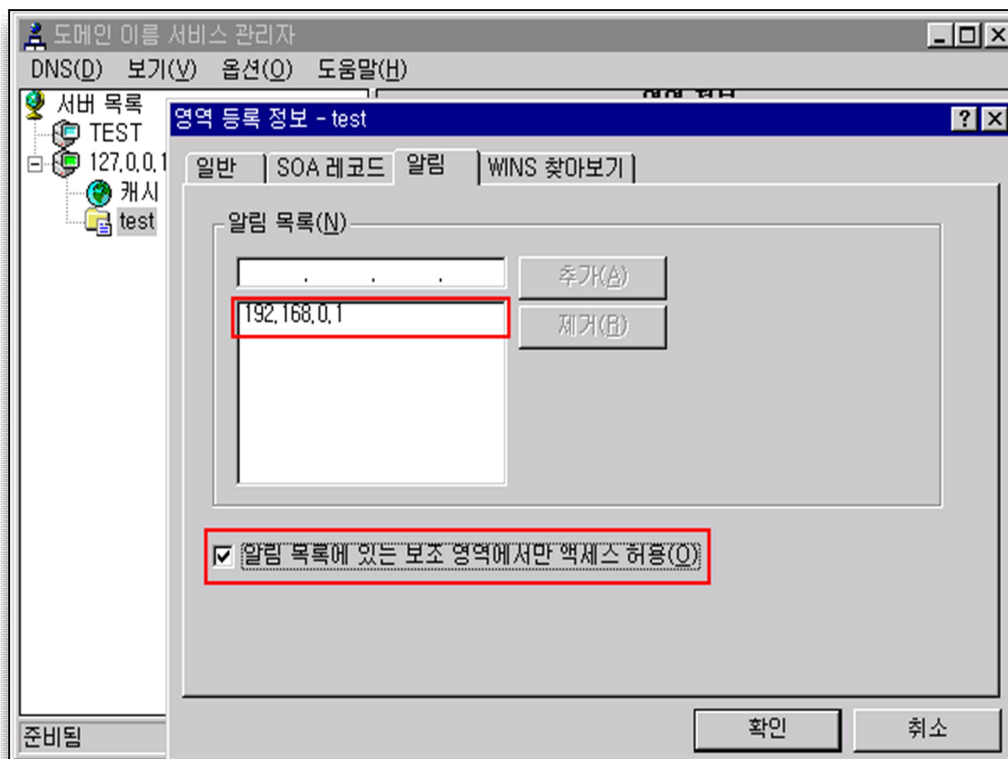
취약점 항목	2.22. FTP 접근 제어 설정				
대상 OS	NT, 2000, 2003, 2008	위험도	상	Code	W-40
취약점 개요	기본적인 FTP 서비스는 계정과 패스워드가 암호화되지 않은 채로 전송되어 간단한 Sniffer에 의해서도 스니핑이 가능하므로 FTP 서비스를 사용하지 않을 것을 권고. 만약 불가피하게 FTP 서비스를 이용해야 하는 경우 특정 IP 주소에 허가된 사용만이 접속할 수 있도록 접근제어 설정을 적용하여야 함.				
보안대책					
판단기준	양호: 특정 IP 주소에서만 FTP 서버에 접속하도록 접근제어 설정을 적용한 경우 취약: 특정 IP 주소에서만 FTP 서버에 접속하도록 접근제어 설정을 적용하지 않은 경우 ※ 조치 시 마스터 속성과 모든 사이트에 적용함				
조치방법	특정 IP 주소에서만 FTP 서버에 접속하도록 접근제어 설정				
보안설정방법					
■ Windows NT, 2000, 2003, 2008 1. 인터넷 정보 서비스(IIS) 관리> FTP 사이트> 속성> [디렉터리 보안] 탭에서 “액세스 거부” 선택 후 접근 가능 IP 주소 추가 (만약 개별 FTP 사이트에 적용할 경우 해당 사이트에만 설정이 적용되고, 기본 설정은 적용 받지 않음)					
					
[참고] 액세스 허가: 모든 액세스를 허용 후 액세스를 거부할 컴퓨터, 그룹, 도메인 추가 액세스 거부: 모든 액세스를 거부 후 액세스를 허용할 컴퓨터, 그룹, 도메인 추가					
※ IIS 7 이상 버전에서는 FTP 사이트를 별도로 생성하지 않고 기존 웹 사이트에 FTP 사이트를 바인딩 하여 사용함 (관리 도구> 인터넷 정보 서비스(IIS) 6.0 관리자에서 FTP 설정 가능)					
조치 시 영향	일반적으로 영향 없음				

윈도우즈 서버

취약점 항목	2.23. DNS Zone Transfer 설정				
대상 OS	NT, 2000, 2003, 2008	위험도	상	Code	W-41
취약점 개요	DNS 서버에 저장되어 있는 도메인 정보를 승인된 DNS서버가 아닌 다른 외부로 유출하는 것은 보안상 바람직하지 않으므로 적절한 보안 설정을 통하여 도메인 정보 전송을 제한하여야 함. 만약, DNS 도메인 정보가 외부로 노출될 경우 악의적인 사용자가 해당 정보를 이용하여 홈페이지 및 하위 URL 정보를 입수하여 웹 애플리케이션 구조를 예측할 수 있음.				
보안대책					
판단기준	양호: 아래 기준에 해당될 경우 1. DNS 서비스를 사용 않는 경우 2. 영역 전송 허용을 하지 않는 경우 3. 특정 서버로만 설정이 되어 있는 경우 취약: 위 3개 기준 중 하나라도 해당 되지 않는 경우				
조치방법	불필요 시 서비스 중지/사용 안 함, 사용하는 경우 영역 전송을 특정 서버로 제한하거나 "영역 전송 허용"에 체크 해제				
보안설정방법					

■ Windows NT

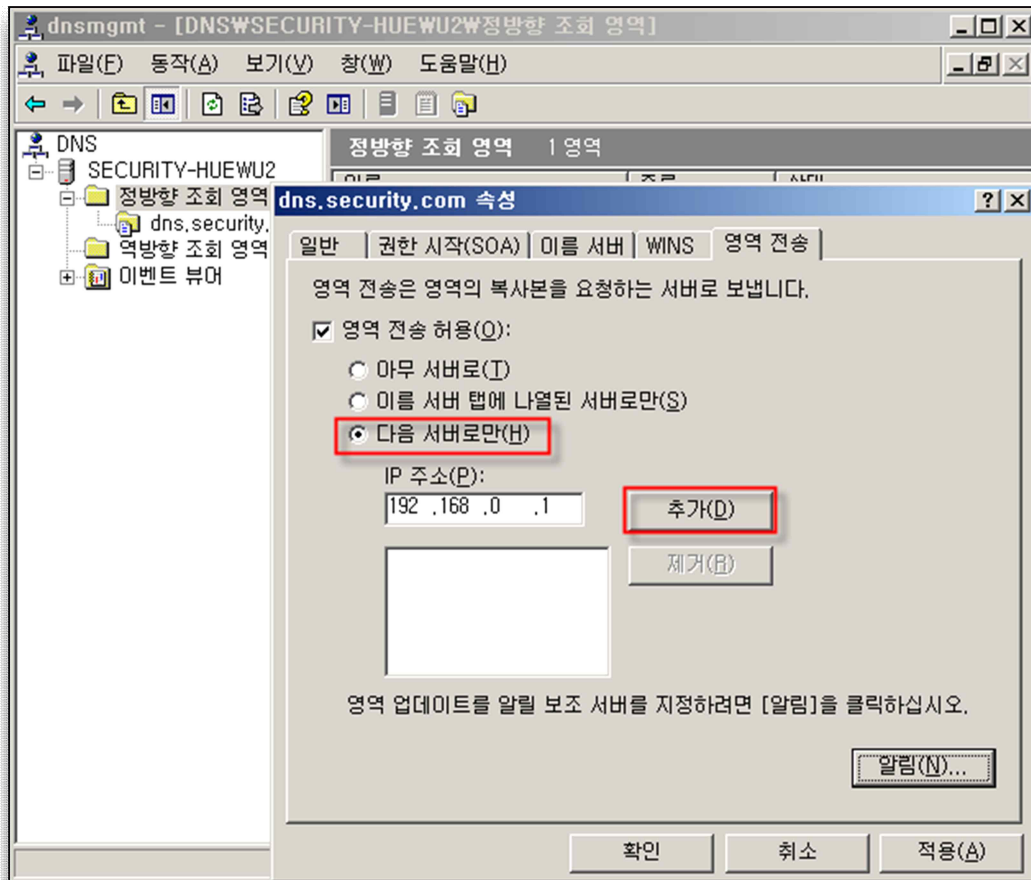
- 시작> 프로그램> 관리 도구> DNS 관리자> 각 조회 영역> 해당 영역> 등록 정보> 알림
- "알림 목록에 있는 보조 영역에서만 액세스 허용" 선택 후 서버 IP 추가



윈도우즈 서버

■ Windows 2000, 2003, 2008

1. 시작> 실행> DNSMGMT.MSC> 각 조회 영역> 해당 영역> 속성> 영역 전송
2. "다음 서버로만" 선택 후 전송할 서버 IP 추가



3. 불필요 시 해당 서비스 제거
시작> 실행> SERVICES.MSC> DNS 서버> 속성 [일반] 탭에서 "시작 유형"을 "사용 안 함"으로 설정한 후, DNS 서비스 중지.

조치 시 영향	영역 전송할 경우 서버를 지정해 주면 영향 없음
----------------	----------------------------

윈도우즈 서버

취약점 항목	2.24. RDS(Remote Data Services) 제거				
대상 OS	NT, 2000, 2003	위험도	상	Code	W-42
취약점 개요	RDS는 MDAC(Microsoft Data Access Components)의 한 컴포넌트로 RDS(Remote Data Services)가 잘못 설정되어 있으면 서비스거부 공격이나 원격에서 관리자 권한으로 임의의 명령을 실행할 수 있는 취약점이 존재함. MDAC 2.7 미만의 버전에서 웹 서버와 웹 클라이언트는 모두 이 취약점으로 인해 위험해질 수 있으므로 RDS가 불필요할 경우 제거하는 것이 안전함.				
보안대책					
판단기준	양호: 다음 중 한 가지라도 해당되는 경우(2008 이상 양호) 1. IIS를 사용하지 않는 경우 2. Windows 2000 서비스팩 4, Windows 2003 서비스팩 2 이상 설치되어 있는 경우 3. 디폴트 웹 사이트에 MSADC 가상 디렉터리가 존재하지 않는 경우 4. 해당 레지스트리 값이 존재하지 않는 경우				
	취약: 양호 기준에 한 가지도 해당되지 않는 경우				
조치방법	사용하지 않는 경우 IIS 서비스 중지/사용 안 함, 사용할 경우 레지스트리 키 값 제거 또는, 관련 패치 적용				
보안설정방법					
■ Windows NT, 2000, 2003 < RDS 제거 방법 > 1. 웹 사이트로부터 “/msadc” 가상 디렉터리 제거 시작> 실행> INETMGR> 웹 사이트 선택 후 오른쪽 디렉터리에서 msadc 제거 2. 다음의 레지스트리 키/디렉터리 제거 HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\W3SVC\Parameters\ADCLaunch\WRDSServer.DataFactory HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\W3SVC\Parameters\ADCLaunch\AdvancedDataFactory HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\W3SVC\Parameters\ADCLaunch\VbBusObj.VbBusObjCls					
조치 시 영향	WAS와 연동될 경우 일부 RDS를 사용하는 경우가 있으며 사용할 경우 레지스트리 키 값 제거				

윈도우즈 서버

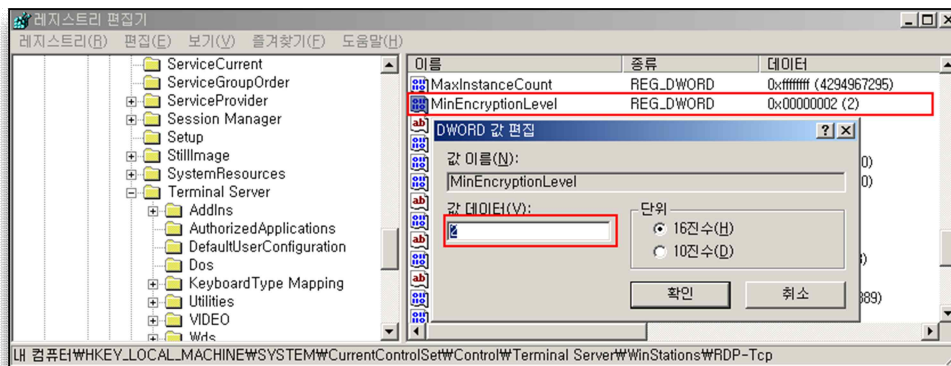
취약점 항목	2.25. 최신 서비스팩 적용																			
대상 OS	NT, 2000, 2003, 2008	위험도	상	Code	W-43															
취약점 개요	서비스팩은 Windows의 안정성을 높이기 위해 응용프로그램, 서비스, 실행 파일 등 여러 수정 파일들을 모아 놓은 업데이트 프로그램이므로 항상 최신 버전으로 유지할 수 있도록 권고함.																			
보안대책																				
판단기준	양호: 최신 서비스팩이 설치되어 있는 경우																			
	취약: 최신 서비스팩이 설치되지 않은 경우																			
조치방법	설치에 따른 영향도 확인 후 최신 서비스팩 설치 (설치 후 시스템 재시작 필요)																			
보안설정방법																				
■ Windows NT, 2000, 2003, 2008																				
1. 시작> 실행> Winver																				
2. 서비스팩 버전 확인 후 최신 버전이 아닌 경우 아래 사이트에서 최신 서비스팩 다운로드 후 설치																				
※ 인터넷 웜(Worm)이 Windows의 취약점을 이용하여 공격하기 때문에 서비스팩 설치 시에는 네트워크와 분리된 상태에서 설치 할 것을 권장																				
[2013년 12월 기준 - 최신 서비스팩 정보]																				
<table><tr><th>운영체제 종류</th><th>최신 서비스팩</th><th>서비스 제공 여부</th></tr><tr><td>Windows NT</td><td>6a</td><td>중단</td></tr><tr><td>Windows Server 2000</td><td>Service Pack 4</td><td>중단</td></tr><tr><td>Windows Server 2003</td><td>Service Pack 2</td><td>중단</td></tr><tr><td>Windows Server 2008</td><td>Service Pack 1</td><td>제공</td></tr></table>						운영체제 종류	최신 서비스팩	서비스 제공 여부	Windows NT	6a	중단	Windows Server 2000	Service Pack 4	중단	Windows Server 2003	Service Pack 2	중단	Windows Server 2008	Service Pack 1	제공
운영체제 종류	최신 서비스팩	서비스 제공 여부																		
Windows NT	6a	중단																		
Windows Server 2000	Service Pack 4	중단																		
Windows Server 2003	Service Pack 2	중단																		
Windows Server 2008	Service Pack 1	제공																		
[보안 패치 사이트]																				
Microsoft Windows Server 제품별 지원																				
http://support.microsoft.com/ph/1163																				
조치 시 영향	설치 후 시스템 재시작이 필요하며 설치에 따른 영향 정도를 확인하여야함																			

윈도즈 서버

취약점 항목	2.26. 터미널 서비스 암호화 수준 설정				
대상 OS	NT, 2000, 2003, 2008	위험도	중	Code	W-44
취약점 개요	터미널 서비스는 원격지에 있는 서버를 관리하기 위한 유용한 도구이지만 취약한 패스워드를 사용하거나 접근제어가 적절하게 설정되어 있지 않은 경우 해킹의 도구로 악용될 수 있으므로 불필요하게 터미널 서비스가 사용되고 있는지 점검하여야 함.				
보안대책					
판단기준	양호: 터미널 서비스를 사용하지 않거나 사용 시 암호화 수준을 “클라이언트와 호환 가능(중간)” 이상으로 설정한 경우				
	취약: 터미널 서비스를 사용하고 암호화 수준이 “낮음” 으로 설정한 경우				
조치방법	불필요 시 서비스 중지/사용 안 함 설정, 사용할 경우 암호화 수준 설정				
보안설정방법					

■ Windows NT

1. 시작> 실행> regedit
2. HKLM\SYSTEM\CurrentControlSet\Control\Terminal Server\WinStations\WDP-Tcp\MinEncryptionLevel 값을 2(중간) 이상으로 설정

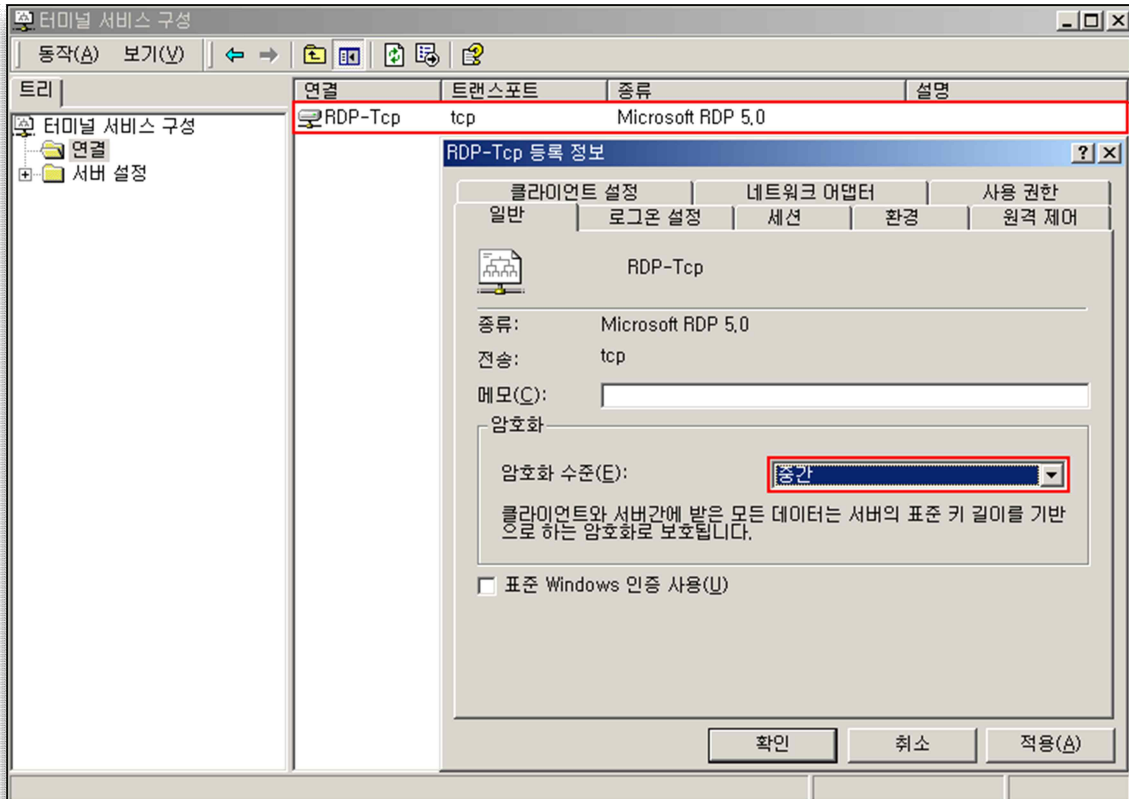


■ Windows 2000

1. 시작> 실행> TSCC.MSC> “해당 서비스” 선택> 속성
2. 암호화 수준 → 중간(Windows 2000) 이상으로 설정

암호화 수준	설 명
낮음	클라이언트에서 서버로 보낸 데이터만 서버의 표준 키 길이를 기반으로 하는 암호화로 보호 서버가 클라이언트로 보낸 데이터는 보호되지 않음
중간	클라이언트와 서버 간에 받은 모든 데이터는 서버의 표준 키 길이를 기반으로 암호화로 보호
높음	클라이언트와 서버 간에 받은 모든 데이터는 서버의 최대 키 길이를 기반으로 암호화로 보호

윈도즈 서버

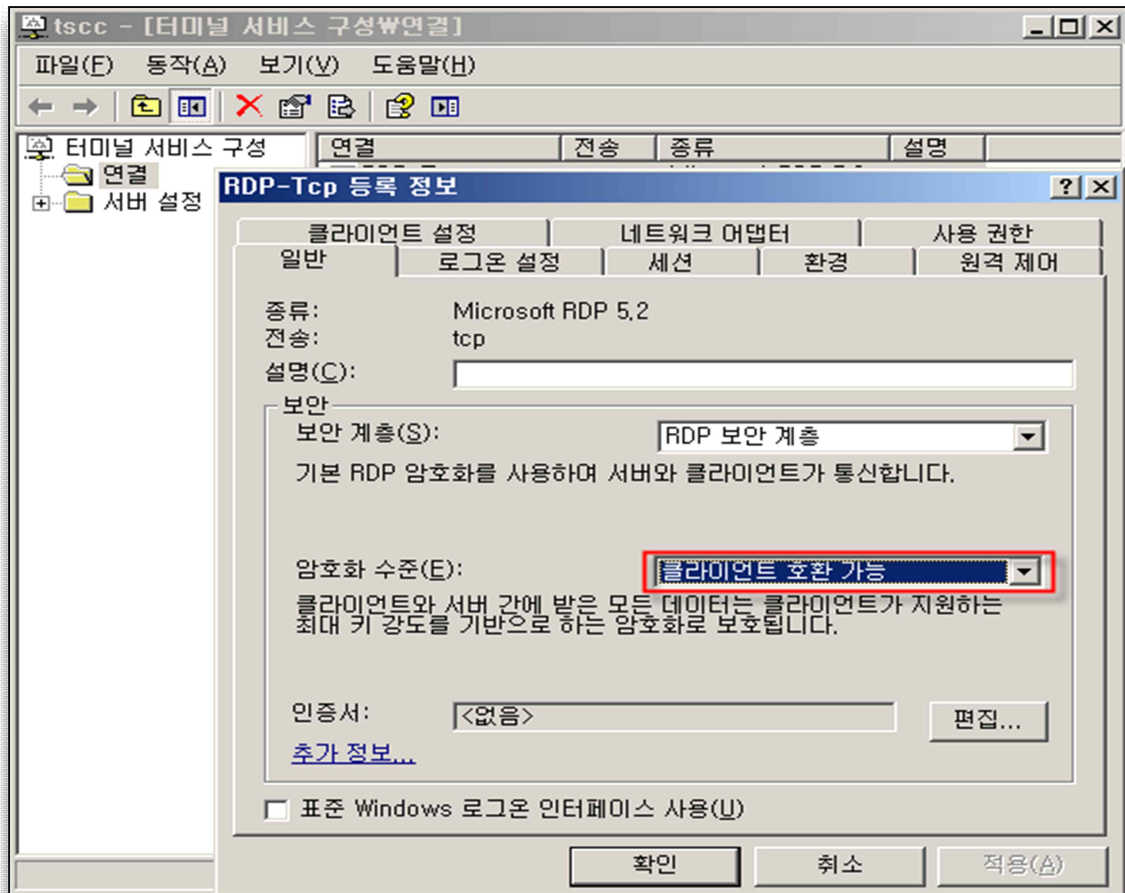


■ Windows 2003, 2008

1. Windows 2003: 시작 > 실행 > TSCC.MSC > “해당 서비스” 선택 > 속성
Windows 2008: 시작 > 관리 도구 > 터미널 서비스 > 터미널 서비스 구성 > RDP-Tcp 속성
2. 암호화 수준 설정 → 클라이언트 호환 가능(Windows 2003), 중간(Windows 2000) 이상

암호화 수준	설 명
낮음	클라이언트에서 서버로 보내는 모든 데이터는 클라이언트가 지원하는 최대 키 강도를 기반으로 하는 암호화로 보호
클라이언트 호환 가능	클라이언트와 서버 간에 받은 모든 데이터는 클라이언트가 지원하는 최대 키 강도를 기반으로 하는 암호화로 보호
높음	클라이언트와 서버 간에 받은 모든 데이터는 서버의 최대 키 강도를 기반으로 하는 암호화로 보호 이 암호화 수준을 지원하지 않는 클라이언트는 연결할 수 없음
FIS 규격	클라이언트에서 서버로 보내는 모든 데이터를 Federal Information Processing Standard 140-1 유효 암호화 방법을 사용하여 보호

윈도우즈 서버



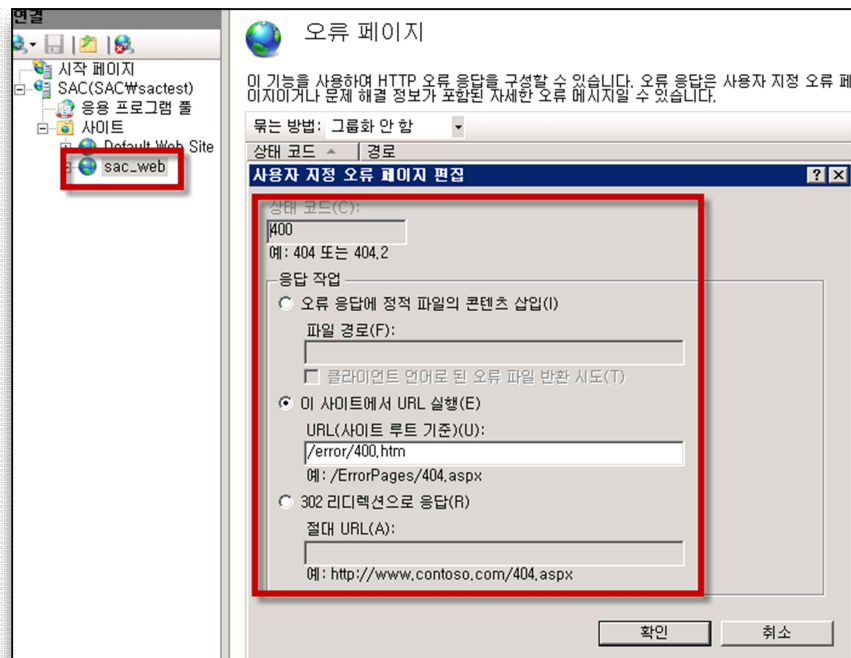
※ 터미널 서비스가 필요한 경우 추가 보안 대책

1. 관리자 이외의 일반 사용자의 터미널 서비스 접속을 허용하지 않음
2. 방화벽에서 터미널 서비스 포트(3389)의 사용을 관리자 컴퓨터의 IP로 제한

조치 시 영향	암호화 수준 변경 시 일반적으로 영향 없음
----------------	-------------------------

인터넷 정보 서비스(IIS) 관리자> 해당 웹 사이트> [오류 페이지]에서 400, 401, 403, 404, 500 등 웹 서비스 에러에 대해 별도의 페이지를 지정

윈도우즈 서버

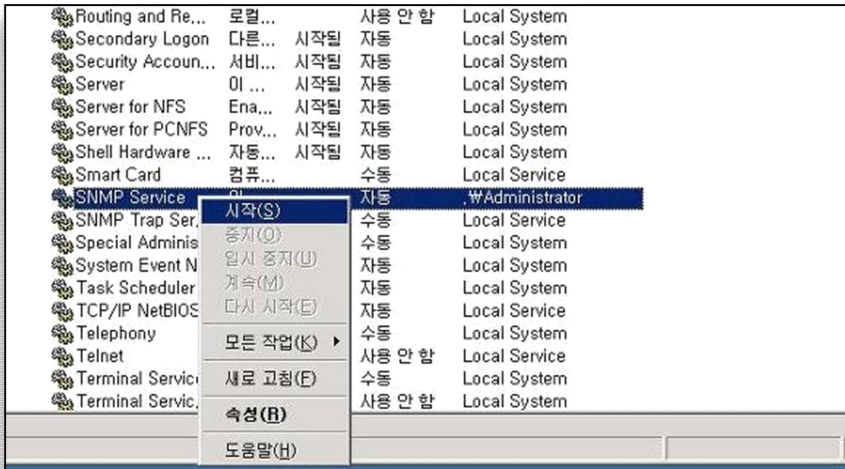


2. 오류 페이지 설정 편집

인터넷 정보 서비스(IIS) 관리자> 해당 웹 사이트> 오류 페이지> [기능 설정 편집]에서
 “서버오류 발생 시 다음 반환” 항목을 “사용자 지정 오류 페이지”로 설정

조치 시 영향	일반적으로 영향 없음
---------	-------------

윈도우즈 서버

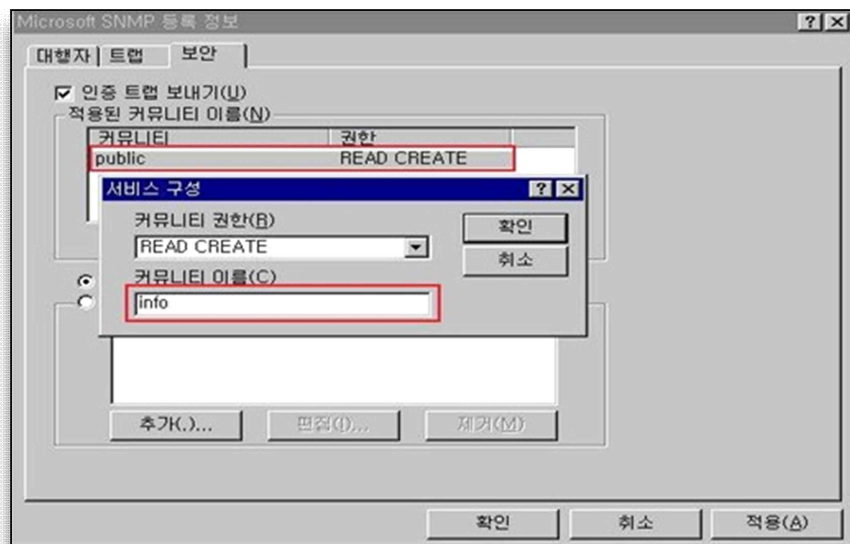
취약점 항목	2.28. SNMP 서비스 구동 점검					
대상 OS	NT, 2000, 2003, 2008		위험도	중	Code	W-46
취약점 개요	SNMP 서비스는 시스템 상태를 실시간으로 파악하거나 설정하기 위해 사용하는 서비스이므로 시스템의 주요정보 유출 및 불법수정을 방지하기 위해 사용하지 않는 경우 중지하여야 함.					
보안대책						
판단기준	양호: SNMP 서비스를 사용하지 않는 경우					
	취약: SNMP 서비스를 사용하는 경우					
조치방법	불필요 시 서비스 중지/사용 안 함					
보안설정방법						
■ Windows 2000, 2003, 2008						
1. 시작> 실행> SERVICES.MSC> SNMP Service> 속성> 보안						
2. 불필요 시 해당 서비스 제거						
시작> 실행> SERVICES.MSC> SNMP Service> 속성에서 "시작 유형"을 "사용 안 함"으로 설정한 후, SNMP 서비스를 중지함						
						
조치 시 영향	*NMS 또는, 별도의 툴에서 SNMP 서비스를 이용하여 서버를 모니터링 하는 경우, 통신하고자 하는 Server/Client에 모두 같은 Community 이름을 사용하여야 함 (서비스> SNMP> 등록 정보> 종속성 참고)					
*NMS(Network Management System): 네트워크 관리 시스템						

윈도우즈 서버

취약점 항목	2.29. SNMP 서비스 커뮤니티스트링의 복잡성 설정				
대상 OS	NT, 2000, 2003, 2008	위험도	중	Code	W-47
취약점 개요	SNMP 서비스는 시스템 상태를 실시간으로 파악하고, 설정하기 위해 사용되는 서비스로 시스템 정보를 송수신하기 위해 일종의 패스워드인 Community String 값을 사용함. 하지만 대부분의 시스템에서 Community String 설정을 public, private 등 Default 설정 값으로 사용하는 경우 많은데, 이를 변경하지 않을 경우 Community String 값을 이용하여 비인가자가 시스템의 주요 정보 및 설정 상황을 파악할 수 있음.				
보안대책					
판단기준	양호: SNMP 서비스를 사용하지 않거나 Community 이름이 public, private이 아닌 경우				
	취약: SNMP 서비스를 사용하며, Community 이름이 public, private인 경우				
조치방법	불필요 시 서비스 중지/사용 안 함, 사용 시 Default Community 이름(public) 변경				
보안설정방법					

■ Windows NT

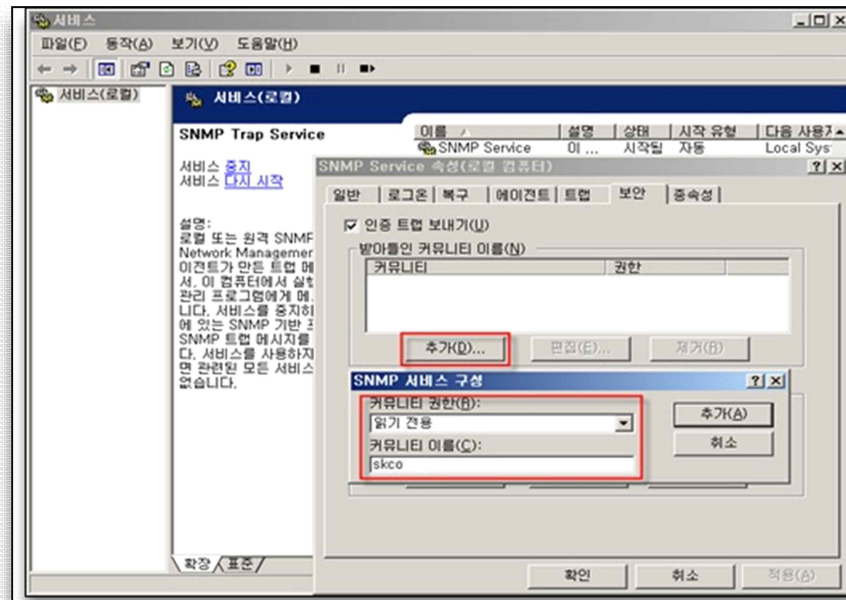
1. 바탕화면> 네트워크 환경> 등록 정보> 서비스/SNMP Service> 등록 정보> 보안



■ Windows 2000, 2003, 2008

1. 시작> 실행> SERVICES.MSC> SNMP Service> 속성> 보안
2. 쓰기 권한이 필요하지 않다면 커뮤니티 이름을 읽기 전용으로 Public/Private이 아닌 이름을 추가 (NT의 경우 시작> 제어판> 서비스에서 설정)

윈도우즈 서버



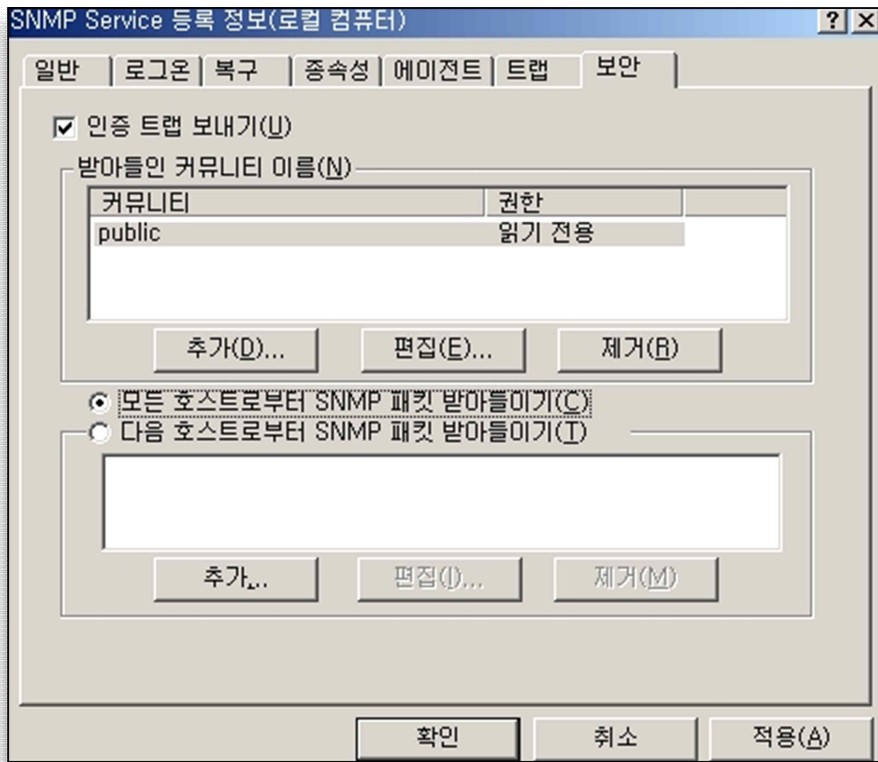
3. 불필요 시 해당 서비스 제거

시작 > 실행 > SERVICES.MSC > SNMP Service > 속성 [일반] 탭에서 "시작 유형"을 "사용 안 함"으로 설정한 후, SNMP 서비스 중지.

조치 시 영향

NMS 또는, 별도의 툴에서 SNMP 서비스를 이용하여 서버를 모니터링 하는 경우, 통신하고자 하는 Server/Client에 모두 같은 Community 이름을 사용하여야 함. (서비스 > SNMP > 등록 정보 > 종속성 참고)

윈도우즈 서버

취약점 항목	2.30. SNMP Access control 설정				
대상 OS	NT, 2000, 2003, 2008	위험도	중	Code	W-48
취약점 개요	SNMP v1의 가장 큰 취약점은 보안 기능이 없어 단순히 Community name 확인 절차만 거치면 Network가 불가능하게 되는 문제점 등이 발견되었는데 이를 SNMP v2를 통해 보완함. 인증 절차에 대한 보안 M5 알고리즘과 Partymib를 이용한 사용자에게만 특정 객체를 이용하거나 못하게 하는 접근 통제 기능이 추가되어 보안요소가 높아짐.				
보안대책					
판단기준	양호: 특정 호스트로부터 SNMP 패킷 받아들이기로 설정되어 있는 경우				
	취약: 모든 호스트로부터 SNMP 패킷 받아들이기로 설정되어 있는 경우				
조치방법	불필요 시 서비스 중지/사용 안 함, 사용 시 Default Community 이름(public) 변경				
보안설정방법					
■ Windows 2000, 2003, 2008					
1. 시작> 실행> SERVICES.MSC> SNMP Service> 속성> 보안					
2. "인증 트랩 보내기" 및 "다음 호스트로부터 SNMP 패킷 받아들이기" 선택					
3. SNMP 호스트 등록					
					
조치 시 영향	일반적으로 영향 없음				

윈도우즈 서버

취약점 항목	2.31. DNS 서비스 구동 점검				
대상 OS	NT, 2000, 2003, 2008	위험도	중	Code	W-49
취약점 개요	동적 업데이트는 DNS 정보에 변경 사항이 있을 때마다 DNS 클라이언트 컴퓨터가 자신의 리소스 레코드(zone 파일)를 DNS 서버에 자동으로 업데이트하는 기능으로 영역 레코드 수동 관리 작업을 줄일 수 있음. 하지만 동적 업데이트를 사용할 경우 악의적인 사용자에게 의해 신뢰할 수 없는 데이터가 받아들여질 수 있으므로 동적 업데이트 사용을 제한하여야 함.				
보안대책					
판단기준	양호: DNS 서비스를 사용하지 않거나 동적 업데이트 "없음(아니오)"으로 설정되어 있는 경우 취약: 서비스를 사용하며 동적 업데이트가 설정되어 있는 경우				
조치방법	일반적으로 동적 업데이트 기능이 필요 없으나 확인 필요				
보안설정방법					
■ Windows 2000, 2003, 2008 - 시작> 실행> DNSMGMT.MSC> 각 조회 영역> 해당 영역> 속성> 일반 - 동적 업데이트 → 없음(또는, 아니오) 선택					
불필요 시 해당 서비스 제거 시작> 실행> SERVICES.MSC> DNS 서버> 속성 [일반] 탭에서 "시작 유형"을 "사용 안 함"으로 설정한 후, DNS 서비스 중지.					
조치 시 영향	일반적으로 동적 업데이트 기능이 필요 없지만 확인 필요				

윈도우즈 서버

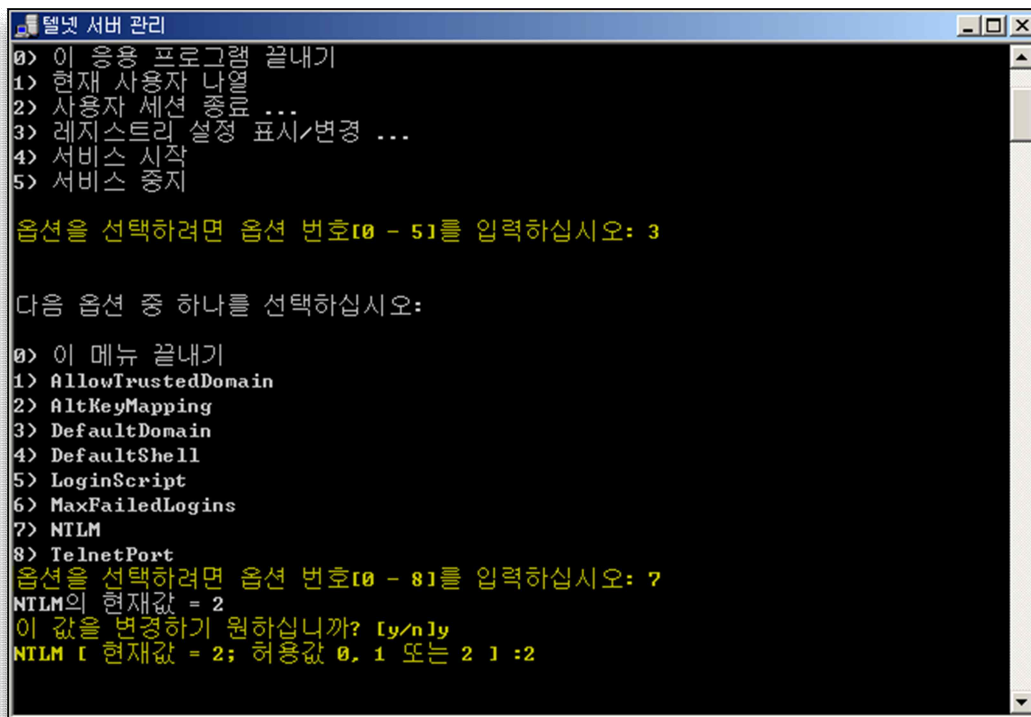
취약점 항목	2.32. HTTP/FTP/SMTP 배너 차단				
대상 OS	NT, 2000, 2003, 2008	위험도	하	Code	W-50
취약점 개요	임의의 사용자가 HTTP, FTP, SMTP 접속 시도 시 보이는 접속 배너 정보를 수집하여 해킹에 사용할 수 있음.				
보안대책					
판단기준	양호: HTTP, FTP, SMTP 접속 시 배너 정보가 보이지 않는 경우				
	취약: HTTP, FTP, SMTP 접속 시 배너 정보가 보여지는 경우				
조치방법	사용하지 않는 경우 IIS 서비스 중지/사용 안 함, 사용 시 속성 값 수정				
보안설정방법					
■ HTTP w3svc.dll, w3core.dll를 Hex 편집기로 불러온 다음 "Microsoft-IIS/4.0", "Microsoft-IIS/5.0", "Microsoft-IIS/6.0", "Microsoft-IIS/7.5" 부분을 수정 ※ dll파일이 메모리에 로드되어 있어 편집이 불가능하므로 윈도우를 명령 프롬프트만 나타나도록 부팅한 후 해당 파일을 변경 ■ FTP ftpsvc2.dll를 Hex편집기로 불러온 다음 "Microsoft FTP Service" 부분을 찾아 수정 ※ dll파일이 메모리에 로드되어 있어 편집이 불가능하므로 윈도우를 명령 프롬프트만 나타나도록 부팅한 후 해당 파일을 변경 ■ SMTP 1. IIS 관리자에서 서버 개체를 우클릭 하여 선택한 다음 속성을 선택 2. 메타베이스 직접 편집 허용 확인란 선택 ※ Exchange System Manager에서 사용할 수 없는 매개변수를 변경하려는 경우 메타베이스 설정을 직접 편집 가능함 (예) 다음과 같이 SMTP 통신에서 Exchange 관련 버전 정보를 공개하지 못하도록 기본 SMTP 가상 서버 구성 개체(<IISsmtpServerLocation="/LM/SmtpSvc/1">)에 ConnectResponse 속성 값을 추가하여 SMTP 서버의 SMTP 배너를 변경할 수 있음 <IISsmtpServer Location ="/LM/SmtpSvc/1"> AdminACL="4963... ..a472" ClusterEnabled="FALSE" ConnectionTimeout="600"					
조치 시 영향	일반적으로 영향 없음				

윈도우즈 서버

취약점 항목	2.33. Telnet 보안 설정				
대상 OS	NT, 2000, 2003, 2008	위험도	중	Code	W-51
취약점 개요	Telnet 서비스는 평문으로 데이터를 송수신하기 때문에 Password 방식으로 인증을 수행할 경우 ID 및 Password가 외부로 노출될 위험성이 있음. 따라서 Telnet 이용 시 네트워크상으로 패스워드를 전송하지 않는 NTLM 인증만 사용하여야 함. ※ Windows 서버의 Telnet 서비스는 NTLM 인증과 Password 인증 방법을 제공함. • NTLM 인증: 암호를 전송하지 않고 negotiate/challenge/response 절차로 인증을 수행함. • Password 인증: 관리자 및 TelnetClients 그룹에 포함된 ID/PWD로 인증 절차를 수행함.				
보안대책					
판단기준	양호: Telnet 서비스가 구동 되어 있지 않거나 인증 방법이 NTLM인 경우				
	취약: Telnet 서비스가 구동 되어 있으며 인증 방법이 NTLM이 아닌 경우				
조치방법	불필요 시 서비스 중지/사용 안 함 설정, 사용 시 인증 방법으로 NTLM만 사용				
보안설정방법					

■ Windows NT, 2000

1. 시작> 설정> 제어판> 관리 도구> 텔넷 서버 설정
2. NTLM 인증 방식만 사용

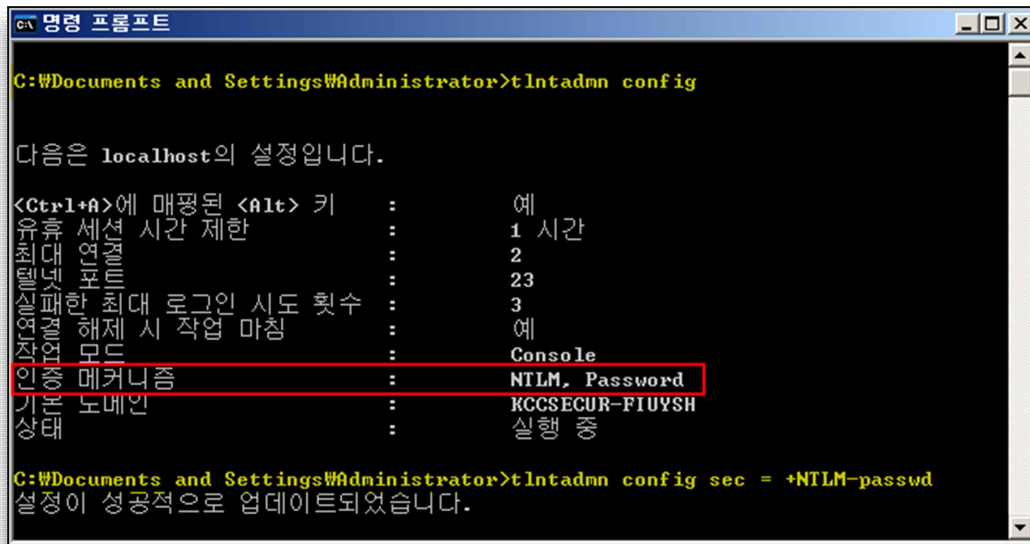


■ Windows 2003, 2008

1. 시작> 실행> cmd> tlntadmn config

윈도즈 서버

2. tlntadmn config sec = +NTLM-passwd (passwd 인증 방식을 제외하고 NTLM 인증 방식만 사용)



3. 불필요 시 해당 서비스 제거

시작 > 실행 > SERVICES.MSC > Telnet > 속성 [일반] 탭에서 "시작 유형"을 "사용 안 함"으로 설정한 후 Telnet 서비스 중지

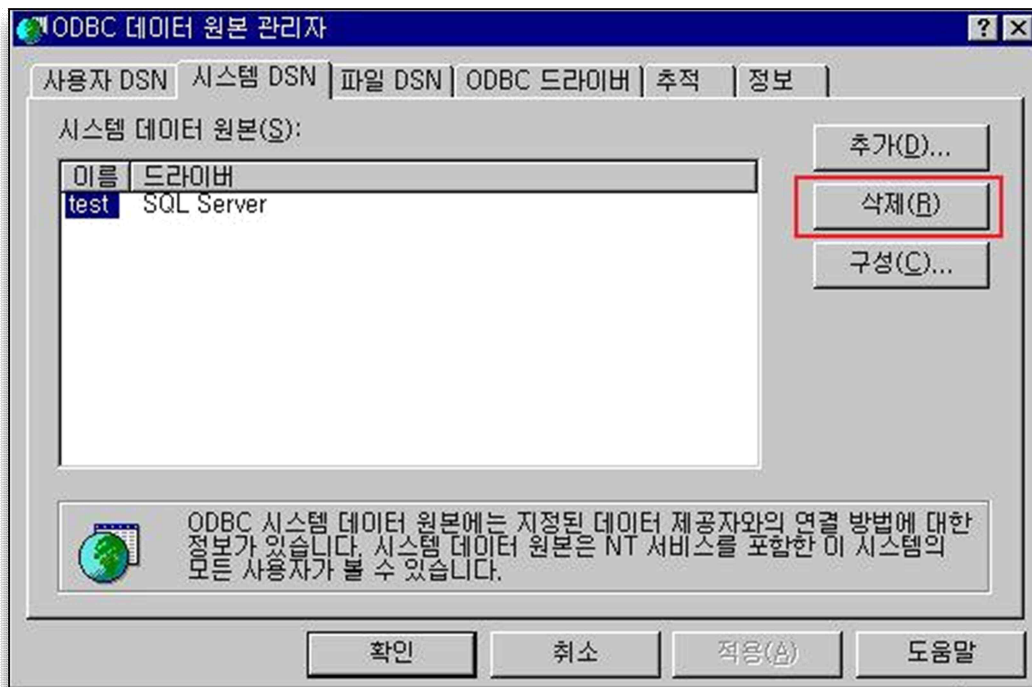
조치 시 영향	일반적으로 영향 없음
---------	-------------

윈도우즈 서버

취약점 항목	2.34. 불필요한 ODBC/OLE-DB 데이터 소스와 드라이브 제거				
대상 OS	NT, 2000, 2003, 2008	위험도	중	Code	W-52
취약점 개요	특정 샘플 애플리케이션은 샘플 데이터베이스를 위해 ODBC 데이터 소스를 설치하거나 불필요한 ODBC/OLE-DB 데이터베이스 드라이브를 설치하므로 불필요한 데이터 소스나 드라이버는 ODBC 데이터 소스 관리자 도구를 이용해서 제거하는 것이 바람직함.				
보안대책					
판단기준	양호: 시스템 DSN 부분의 Data Source를 현재 사용하고 있는 경우				
	취약: 시스템 DSN 부분의 Data Source를 현재 사용하고 있지 않은 경우				
조치방법	사용하지 않는 불필요한 ODBC 데이터 소스 제거				
보안설정방법					

■ Windows NT

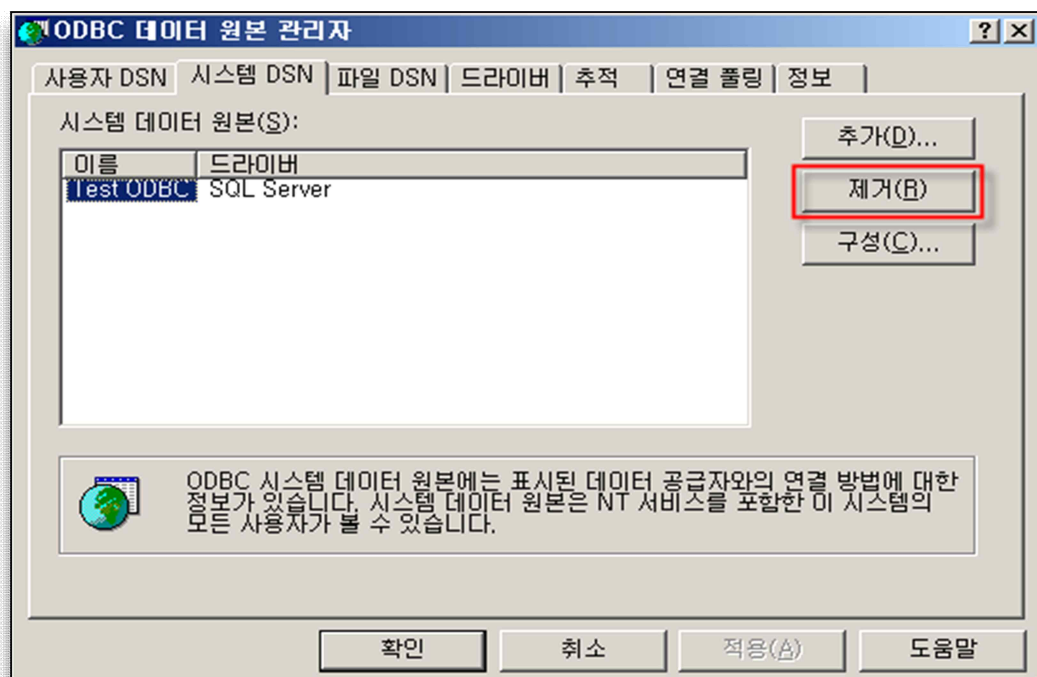
1. 시작> 설정> 제어판> 데이터 원본(ODBC)> 시스템 DSN> 해당 드라이브 클릭
2. 사용하지 않는 데이터 소스 제거



■ Windows 2000, 2003, 2008

1. 시작> 설정> 제어판> 관리 도구> 데이터 원본(ODBC)> 시스템 DSN> 해당 드라이브 클릭
2. 사용하지 않는 데이터 소스 제거

윈도우즈 서버



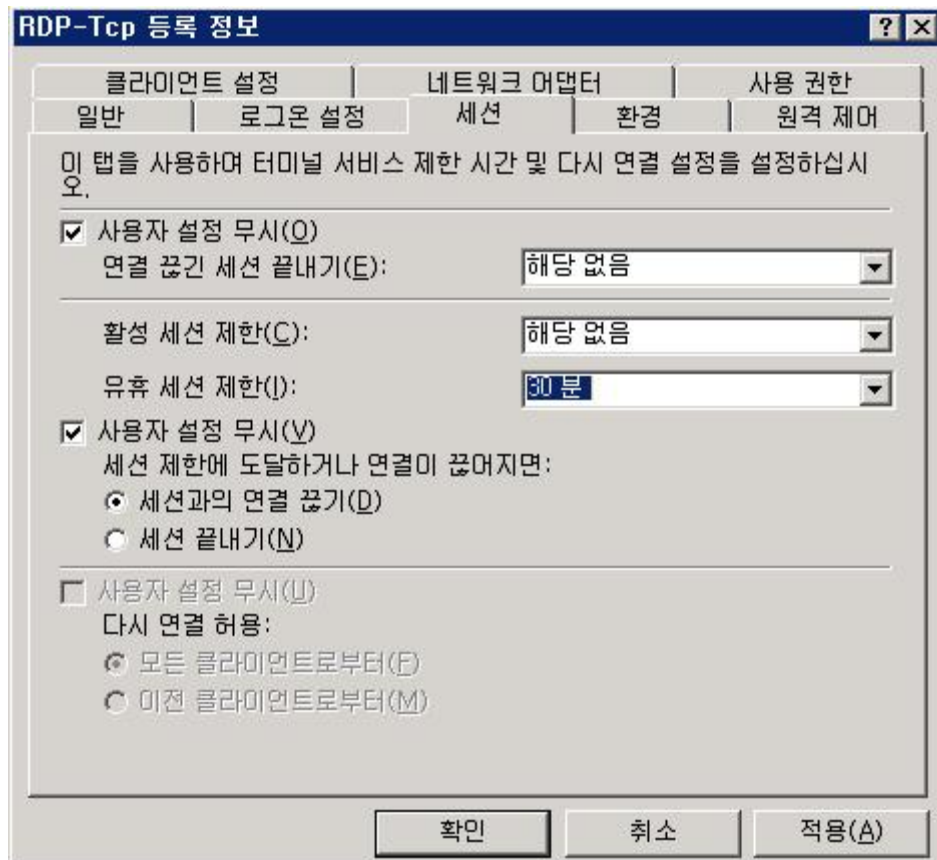
조치 시 영향 애플리케이션에서 사용할 경우 양호

윈도우즈 서버

취약점 항목	2.35. 원격터미널 접속 타임아웃 설정				
대상 OS	NT, 2000, 2003, 2008	위험도	중	Code	W-53
취약점 개요	일반적으로 웹 서비스 이용 시 사용자의 브라우저에서 어떠한 이벤트도 발생하지 않는다면 웹 서버에서 보안상 자동으로 세션을 끊는 경우가 있음. 이와 같은 방식으로 원격제어를 이용하여 터미널에 접속 후 일정 시간 동안 이벤트가 발생시키지 않는다면 세션을 종료시키기 위해 Timeout 설정을 해주어야 함.				
보안대책					
판단기준	양호: 원격제어 시 Timeout 제어 설정을 적용한 경우				
	취약: 원격제어 시 Timeout 제어 설정을 적용하지 않은 경우				
조치방법	Timeout 제어 설정 적용				
보안설정방법					

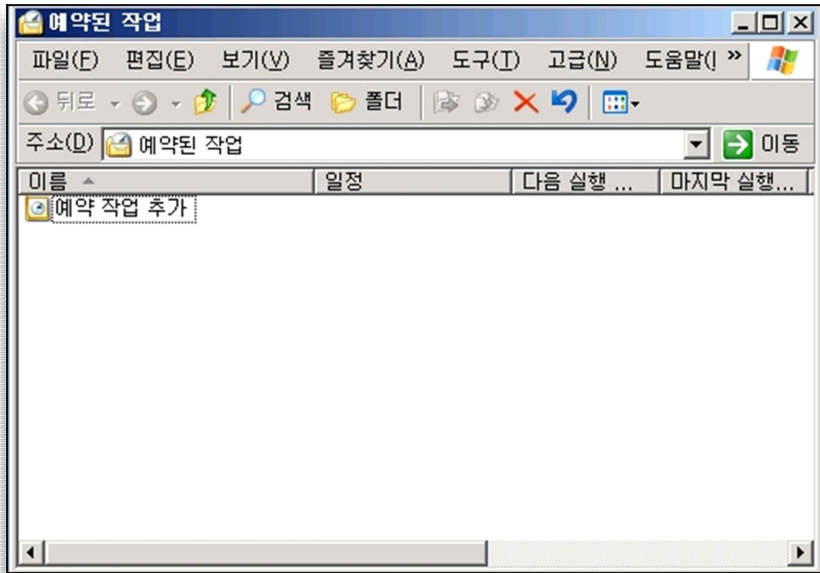
■ Windows 2000, 2003, 2008

1. 시작> 실행> 열기> tscc.msc 실행
(Windows 2008은 tsconfig.msc)
2. RDP-Tcp connection에서 우클릭> 속성 실행
3. [세션] 탭에서 아래 Override user settings(사용자 설정 무시)을 체크하고
Idle session time 세션이 끊어지도록(유휴 세션 제한) 원하는 시간을 설정함



조치 시 영향 애플리케이션에서 사용할 경우는 양호

윈도우즈 서버

취약점 항목	2.36. 예약된 작업에 의심스러운 명령이 등록되어 있는지 점검				
대상 OS	NT, 2000, 2003, 2008	위험도	중	Code	W-54
취약점 개요	일정 시간마다 미리 설정해둔 프로그램을 실행할 수 있는 예약된 작업은 시작프로그램과 더불어서 해킹과 트로이 목마, 백도어를 설치하여 공격하기 좋은 루트로 사용될 수 있으므로 예약된 작업을 수시로 확인하는 것을 권장함.				
보안대책					
판단기준	양호: 예약된 작업에 접속하여 불필요한 명령어나 파일이 있는지 확인한 경우				
	취약: 예약된 작업에 접속을 하지 않아 확인을 하지 않거나, 방치하고 있는 경우				
조치방법	예약 작업에 대한 주기적인 확인				
보안설정방법					
■ Windows 2000, 2003, 2008					
< GUI 확인 방법 >					
1. 시작> 설정> 제어판> 예약된 작업 확인					
2. 등록된 예약 작업을 선택하여 상세내역 확인					
3. 불필요한 파일 존재 시 삭제					
					
< CLI 확인 방법 >					
1. 시작> 실행> cmd 입력					
2. cmd 창에서 C:\>at 명령어를 실행하여 확인					
조치 시 영향	예약 작업을 주기적으로 확인				

윈도우즈 서버

3. 패치 관리

취약점 항목	3.1. 최신 HOT FIX 적용				
대상 OS	NT, 2000, 2003, 2008	위험도	상	Code	W-55
취약점 개요	Hot Fix는 즉시 교정되어야만 하는 주요한 취약점(주로 보안과 관련된)을 패치하기 위해 배포되는 프로그램으로 각각의 서비스팩이 발표된 이후 패치가 추가될 필요가 있을 때 별도로 발표됨. 때론, Hot Fix보다 취약성을 이용한 공격도구가 먼저 출현할 수 있으므로 Hot Fix는 발표 후 가능한 한 빨리 설치할 것을 권장함.				
보안대책					
판단기준	양호: 최신 Hotfix 또는,PMS(Patch Management System) Agent가 설치되어 있는 경우 취약: 최신 Hotfix 또는, PMS(Patch Management System) Agent가 설치되어 있지 않은 경우				
조치방법	최신 Hotfix 설치				
보안설정방법					
1. 아래의 패치 리스트를 조회하여, 서버에 필요한 패치를 선별하여 수동으로 설치함 http://www.microsoft.com/korea/technet/security/current.asp					
2. Windows 자동 업데이트 기능을 이용한 설치 수동 업데이트의 부담을 덜어주기 위하여 Microsoft에서는 자동으로 시스템에 필요한 Hot Fix 및 소프트웨어 업그레이드를 보여주고 다운로드 및 적용을 쉽게 하기 위한 사이트를 마련해 놓고 있음 Internet Explorer 도구 메뉴 중 "Windows Update"를 선택하면 자동으로 Windows Update 사이트로 이동하게 되며, 다음의 URL을 직접 주소 입력 창에 입력 가능함 http://windowsupdate.microsoft.com/?IE					
3. PMS(Patch Management System) Agent를 설치하여 자동으로 업데이트되도록 설정함					
※ 주의: 보안 패치 및 Hot Fix 경우 적용 후 시스템 재시작을 요하는 경우가 대부분이므로 관리자는 서비스에 지장이 없는 시간대에 적용할 것을 권장함. 일부 Hot Fix는 수행되고 있는 OS 프로그램이나 개발용 Application 프로그램에 영향을 줄 수 있으므로 패치 적용 전 Application 프로그램을 구분하고, 필요하다면 OS 벤더 또는, Application 엔지니어에게 확인 작업을 거친 후 패치를 수행하여야 함					
조치 시 영향	설치 후 시스템 재시작이 필요한 경우가 존재하며 설치에 따른 영향도 필요함				

윈도우즈 서버

취약점 항목	3.2. 백신 프로그램 업데이트				
대상 OS	NT, 2000, 2003, 2008	위험도	상	Code	W-56
취약점 개요	계속되는 신종 바이러스의 출현으로 인해 백신 프로그램의 설치만으로는 그 효과를 볼 수 없으므로 바이러스 정보에 대한 주기적인 업데이트를 통해 최신의 바이러스까지 치료할 수 있는 기능이 필요함.				
보안대책					
판단기준	양호: 바이러스 백신 프로그램의 최신 엔진 업데이트가 설치되어 있는 경우				
	취약: 바이러스 백신 프로그램의 최신 엔진 업데이트가 설치되어 있지 않은 경우				
조치방법	담당자를 통해 바이러스 백신을 설치 후 엔진 업데이트를 설정하도록 권고				
보안설정방법					
1. 긴급한 경우 수시로 업데이트 진행 (백신 종류마다 다소 차이는 있으나 매주 업데이트가 이뤄짐) 2. 정기적인 업데이트를 통해 검색엔진을 최신 버전으로 유지하고, 백신사에서 발표하는 경보 주시 3. 백신 프로그램의 자동 업데이트 기능을 이용하면 온라인을 통해 변동 사항을 자동으로 업데이트하여 알 수 있음 • 안철수 연구소, 하우리: 매주 수요일 정기업데이트 • 시만텍코리아, 트랜드마이크로: 매주 목요일 정기업데이트 (미국 시간으로 수요일) ※ 4개 백신 업체 모두 긴급 시 수시 업데이트 및 실시간 업데이트 기능 제공.					
조치 시 영향	일반적으로 영향 없음				

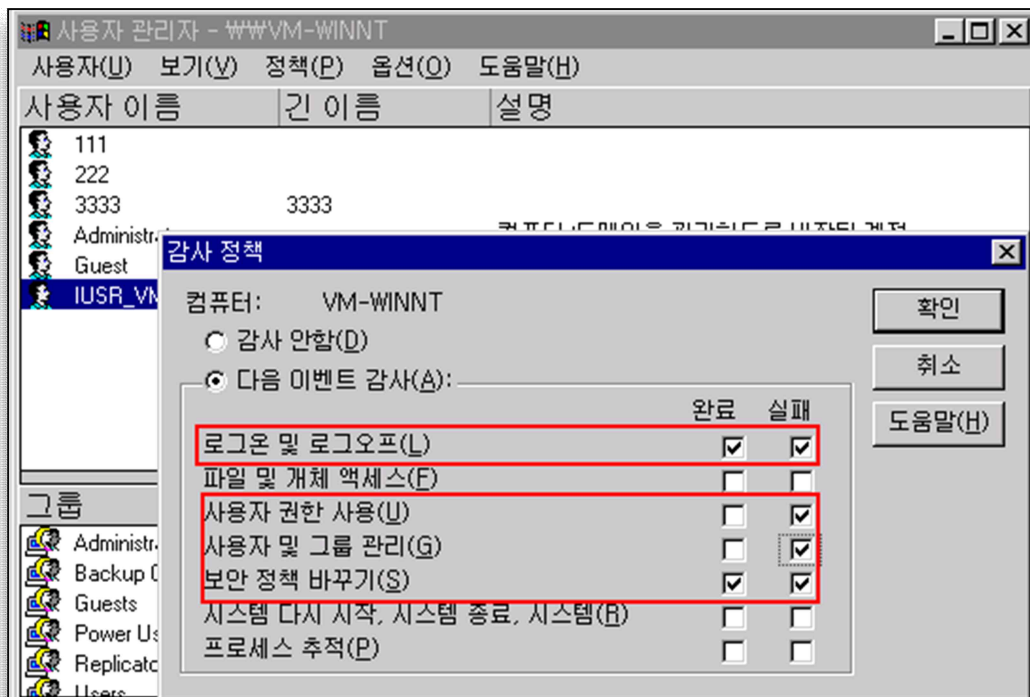
윈도즈 서버

취약점 항목	3.3. 정책에 따른 시스템 로깅 설정				
대상 OS	NT, 2000, 2003, 2008	위험도	중	Code	W-57
취약점 개요	감사 설정이 구성되어 있지 않거나 감사 설정 수준이 너무 낮으면 보안 관련 문제 발생 시 원인을 파악하기 어려우며 법적 대응을 위한 충분한 증거로 사용될 수도 없음. 그러나 감사 설정이 너무 높으면 보안 로그에 불필요한 항목이 많이 기록되므로 매우 중요한 항목과 혼동할 수 있으며 시스템 성능에도 심각한 영향을 줄 수 있기 때문에 법적 요구 사항과 조직의 정책에 따라 필요한 로그를 남기도록 설정하여야 함.				
보안대책					
판단기준	양호: 아래와 같은 이벤트에 대한 감사 설정이 되어 있는 경우 - 로그온 이벤트, 계정 로그온 이벤트, 정책 변경: 성공/실패 감사 - 계정 관리, 디렉터리 서비스 액세스, 권한 사용: 실패 감사				
	취약: 아래와 같은 이벤트에 대한 감사 설정이 되어 있지 않은 경우				
조치방법	위와 같은 이벤트에 대한 추가적인 감사 설정				
보안설정방법					

■ Windows NT

1. 시작> 프로그램> 관리 도구> 도메인 사용자 관리자> 정책> 감사

- 로그온 및 로그오프, 보안 정책 바꾸기: 성공/실패 감사
- 사용자 권한 사용, 사용자 및 그룹 관리: 실패 감사

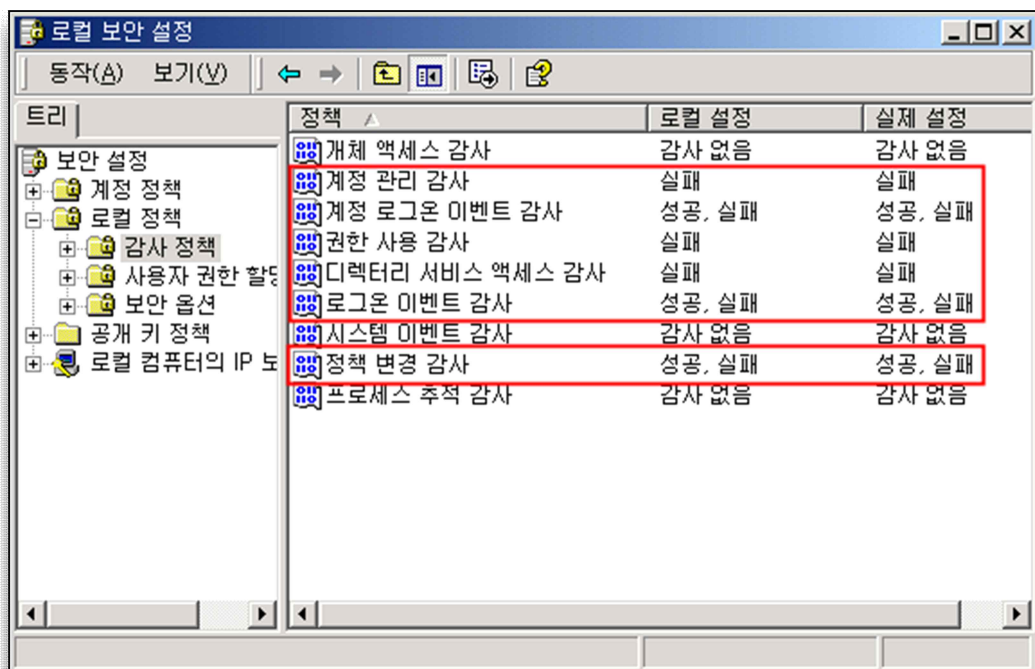


윈도우즈 서버

■ Windows 2000, 2003, 2008

1. 시작 > 실행 > SECPOL.MSC > 로컬 정책 > 감사 정책

- 로그인 및 로그오프, 보안 정책 바꾸기: 성공/실패 감사
- 사용자 권한 사용, 사용자 및 그룹 관리: 실패 감사



윈도우즈 서버

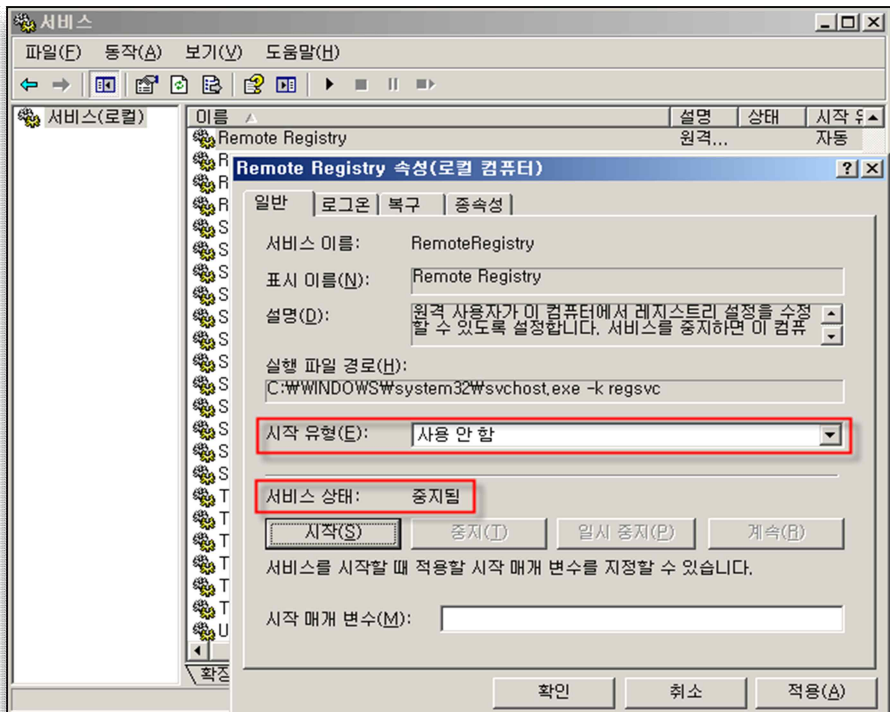
정 책	설 명
로그온 이벤트	사용자가 컴퓨터에 로그인하거나 로그오프 할 때마다 로그인 시도된 컴퓨터의 보안 로그에 이벤트 생성
계정 로그인 이벤트	사용자가 도메인에 로그인하면 도메인 컨트롤러에 로그인 시도 기록
계정 관리	사용자나 그룹이 작성, 변경 또는, 삭제된 시간을 판단하는데 사용
개체 액세스	시스템 액세스 컨트롤 목록(SACL)이 있는 Windows 2000 기반 네트워크의 모든 개체에 대한 감사 활성화 보안 로그에 이벤트를 표시하려면 먼저 개체 액세스 감사를 활성화한 후 감사할 각 개체에 대해 SACL 정의
디렉터리 서비스 액세스	Active Directory 개체의 SACL에 나열된 사용자가 해당 개체에 액세스를 시도할 때 감사 항목 생성
권한 사용	권한 사용의 성공 및 실패를 감사할 경우 사용자 권한을 이용하려고 할 때마다 이벤트 생성
프로세스 추적	실행되는 프로세스에 대한 자세한 추적 정보를 감사하는 경우 이벤트 로그에 프로세스를 작성하고 종료하려고 한 시도 확인
시스템 이벤트	사용자나 프로세스가 컴퓨터 환경을 변경하면 시스템 이벤트가 생성되고, 시스템 이벤트를 감사할 경우 보안 로그 삭제 시간 감사
정책 변경	감사 정책 변경의 성공 및 실패를 감사함
조치 시 영향	일반적인 경우 영향 없음

윈도우즈 서버

4. 로그 관리

취약점 항목	4.1. 로그의 정기적 검토 및 보고				
대상 OS	NT, 2000, 2003, 2008	위험도	상	Code	W-58
취약점 개요	로그를 정기적으로 분석하여 침입 유무를 파악하고, 침입 시도 의심 사례를 분석하여 사전에 해당 장비에 대한 접근을 차단하는 등 체계적인 로그 관리 작업이 이루어져야 함.				
보안대책					
판단기준	양호: 로그 기록에 대해 정기적으로 검토, 분석, 리포트 작성 및 보고 등의 조치가 이루어지는 경우				
	취약: 로그 기록에 대해 정기적으로 검토, 분석, 리포트 작성 및 보고 등의 조치가 이루어 지지 않는 경우				
조치방법	로그 기록 검토 및 분석을 시행하여 리포트를 작성하고 정기적으로 보고함				
보안설정방법					
■ Windows NT, 2000, 2003, 2008 1. 로그 기록에 대한 정기적 검토 및 분석 실시 (1) 시작> 제어판> 관리 도구> 이벤트 뷰어 (2) 응용 프로그램 로그, 보안 로그, 시스템 로그 분석 (3) OS 구성에 따라 디렉터리 서비스 로그, 파일 복제 서비스 로그, DNS 서버 로그 등 분석 ※ 이벤트 로그를 확인하기 위해서 Windows 서버의 이벤트 뷰어를 사용하여 진행함 2. 로그 분석 결과에 대한 일일·월간 보고서 작성 및 보고					
조치 시 영향	일반적인 경우 영향 없음				

윈도우즈 서버

취약점 항목	4.2. 원격으로 액세스할 수 있는 레지스트리 경로				
대상 OS	NT, 2000, 2003, 2008	위험도	상	Code	W-59
취약점 개요	Windows에 의해 사용되는 모든 초기화 및 환경설정 정보가 레지스트리에 저장되므로 레지스트리에 대한 철저한 보안이 요구됨. 레지스트리 편집기는 원격접속으로도 그 키를 바꿀 수 있지만, 대단히 위험하므로 네트워크를 통한 레지스트리 접속을 차단하여야 함. 원격에서 레지스트리로의 접근을 위해서는 관리자의 권한 또는, 원격에서 접근하기 위한 특별한 계정이 필요함. 윈도우에서는 원격에서 레지스트리 접근에 대한 요구를 다루기 위해 원격 레지스트리 서비스를 제공하고 있는데, 이 서비스를 중지시키면 레지스트리에 대한 어떠한 원격 접근도 막을 수 있으므로 불가피한 경우를 제외하고는 사용을 중지할 것을 권고함.				
보안대책					
판단기준	양호: Remote Registry Service가 중지되어 있는 경우 취약: Remote Registry Service가 사용 중인 경우				
조치방법	불필요 시 서비스 중지 및 사용 안 함으로 설정				
보안설정방법					
■ Windows NT, 2000, 2003, 2008					
1. 시작> 실행> SERVICES.MSC> Remote Registry> 속성					
2. 시작 유형 → 사용 안 함					
서비스 상태 → 중지					
					
조치 시 영향	Remote Registry Service를 사용하는지 확인 필요 (서비스> Remote Registry Service> 등록 정보> 종속성 참고)				

윈도우즈 서버

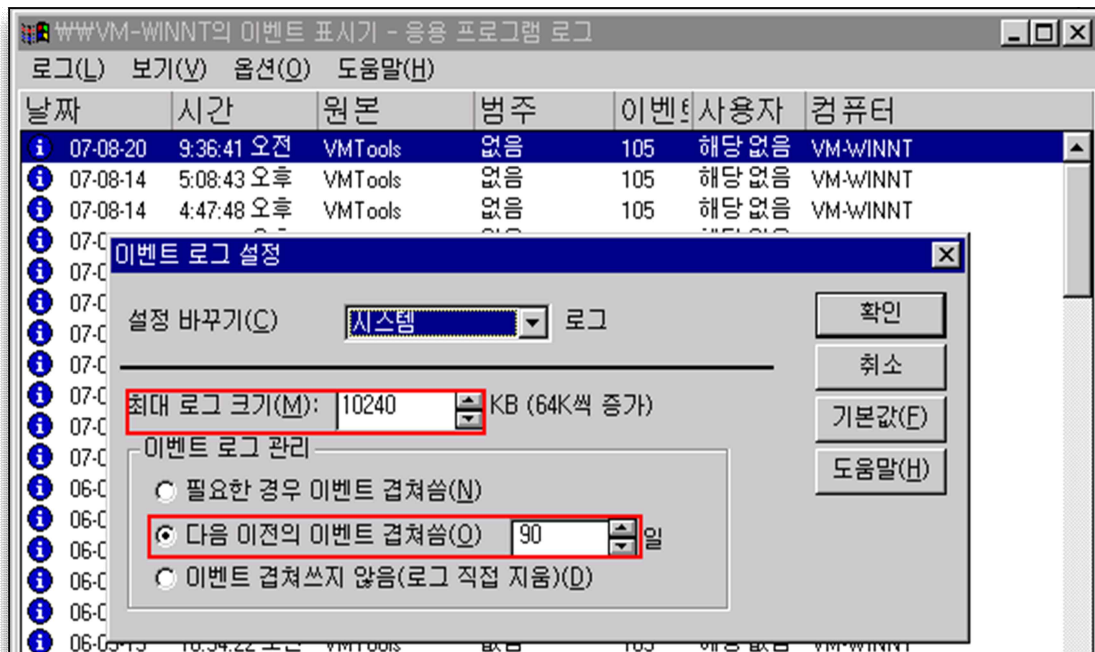
취약점 항목	4.3. 이벤트 로그 관리 설정				
대상 OS	NT, 2000, 2003, 2008	위험도	하	Code	W-60
취약점 개요	최대 로그 크기는 "10,240Kb 이상"으로 설정하여 충분한 로그가 저장될 수 있는 공간을 확보하고, 이벤트 로그 관리는 "이벤트 겹쳐 쓰지 않음"으로 설정하여 로그가 자동으로 덮어 씌워짐으로써 과거의 로그가 삭제되는 일이 발생하지 않도록 확인함.				
보안대책					
판단기준	양호: 최대 로그 크기 "10,240Kb 이상"으로 설정, "90일 이후 이벤트 덮어쓰" 을 설정한 경우				
	취약: 최대 로그 크기 "10,240Kb 미만"으로 설정, 이벤트 덮어쓰 기간이 "90일 이하"로 설정된 경우				
조치방법	최대 로그 크기 "10204KB", "90일 이후 이벤트 덮어쓰" 설정				
보안설정방법					

■ Windows NT

1. 프로그램 > 관리 도구 > 이벤트 표시기 > 로그 > 로그 설정

2. 최대 로그 크기 → 10240

다음 이전의 이벤트 겹쳐 씌움 → 90일



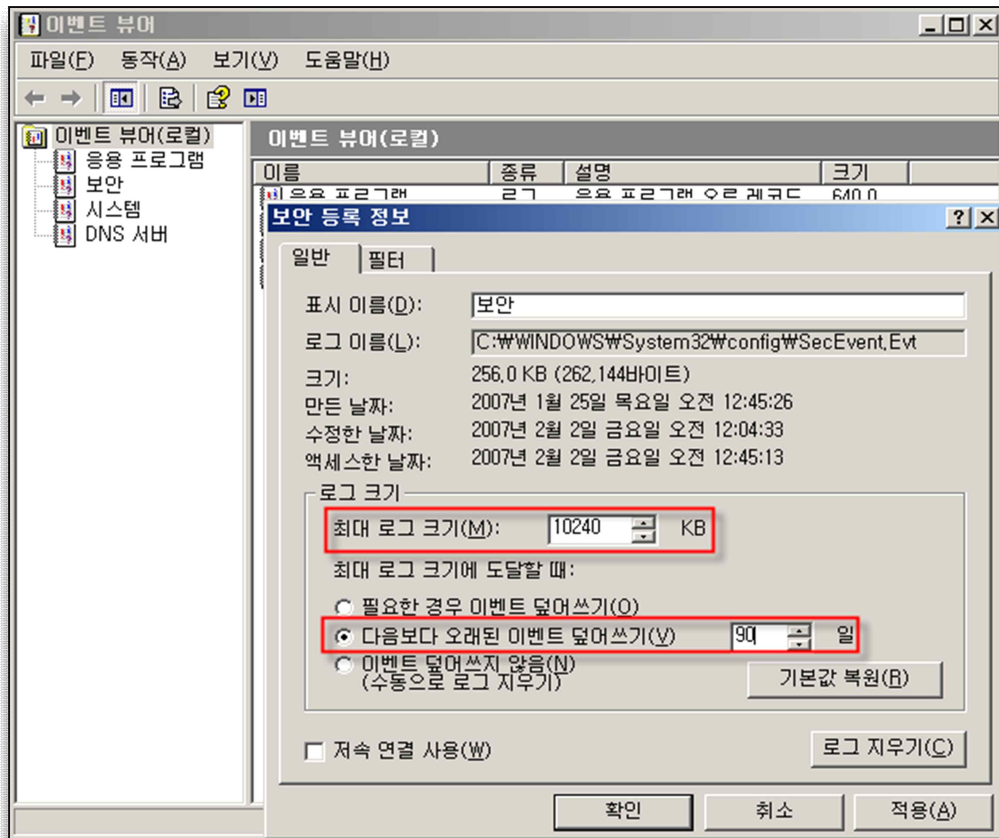
윈도우즈 서버

■ Windows 2000, 2003, 2008

1. 시작 > 실행 > EVENTVWR.MSC > 해당 로그 > 속성 > 일반

2. 최대 로그 크기 → 10240

최대 로그 크기에 도달할 때: 다음보다 오래된 이벤트 덮어쓰기 → 90일

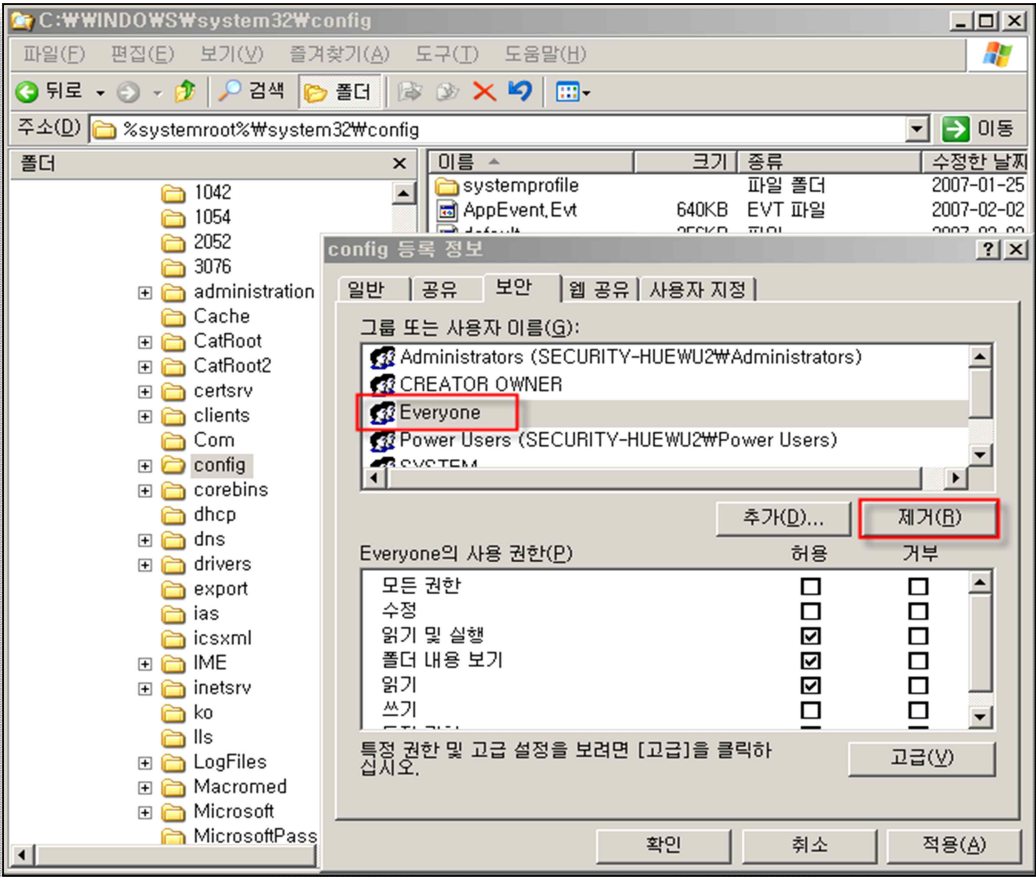


※ Windows 2008 서버의 경우 덮어쓰기 날짜 지정 불가능

조치 시 영향	일반적인 경우 영향 없음
---------	---------------

취약점 항목	4.4. 원격에서 이벤트 로그 파일 접근 차단				
대상 OS	NT, 2000, 2003, 2008	위험도	중	Code	W-61
취약점 개요	익명으로 중요 "시스템 로그' 파일 및 '애플리케이션 로그" 파일에 접근할 수 있어 중요 보안 감사 정보의 변조·삭제·유출의 위험이 존재하므로 원격 익명 사용자의 시스템 로그 접근을 제한하여야 함. ※ 일반적으로 시스템 로그는C:\winnt\system32\config 파일에 저장되지만. 애플리케이션 로그 파일은 각각의 애플리케이션마다 로그 저장 위치가 다름. 웹 서버에 많이 사용하는 IIS 경우, C:\winnt\system32\LogFiles에 저장됨.				
보안대책					
판단기준	양호: 로그 디렉터리의 권한에 Everyone 권한이 없는 경우				

윈도우즈 서버

	취약: 로그 디렉터리의 접근권한이 Everyone 권한이 있는 경우 • 시스템 로그 디렉터리: %systemroot%\system32\config • IIS 로그 디렉터리: %systemroot%\system32\LogFiles
조치방법	로그 디렉터리의 접근권한에 Everyone 제거
보안설정방법	
■ Windows NT, 2000, 2003, 2008	
1. 탐색기> 로그 디렉터리> 속성> 보안	
2. Everyone 제거	
 The screenshot shows a Windows Explorer window with the address bar set to %systemroot%\system32\config. The left pane shows a tree view of folders, with 'config' selected. The right pane shows a list of files and folders. A 'config' folder's security properties dialog box is open, showing the 'Everyone' group selected in the list. The 'Remove' button is highlighted.	
조치 시 영향	일반적인 경우 영향 없음

윈도우즈 서버

5. 보안 관리

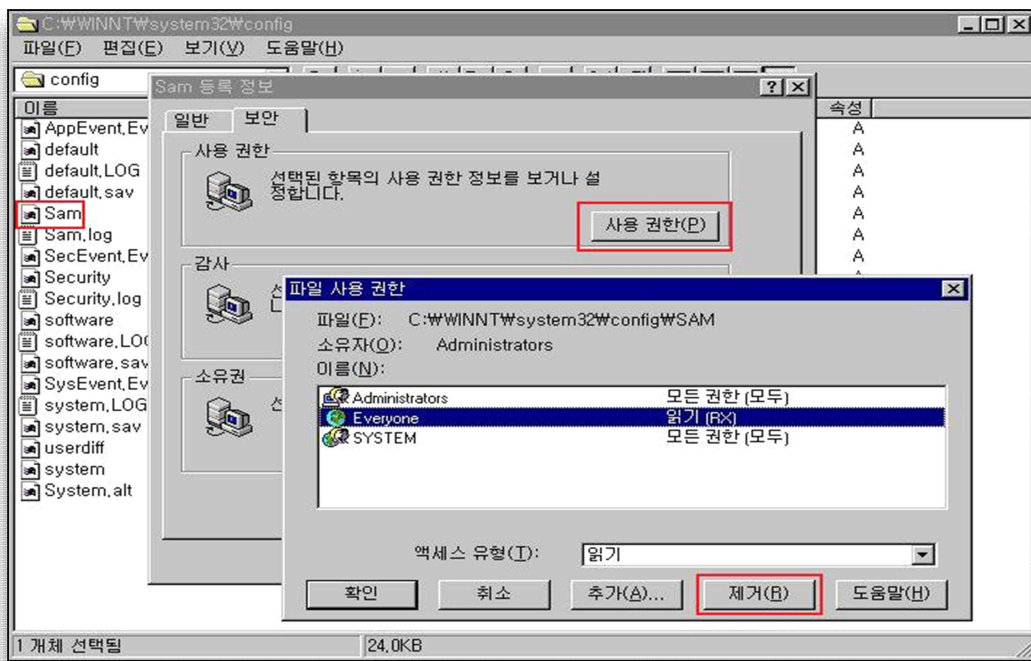
취약점 항목	5.1. 백신 프로그램 설치				
대상 OS	NT, 2000, 2003, 2008	위험도	상	Code	W-62
취약점 개요	*웜, *트로이목마 등의 악성 바이러스로 인한 피해규모가 커지고 있으므로 이에 대한 피해를 최소화하기 위해 반드시 바이러스 백신 프로그램을 설치 및 운영하여야 함. 바이러스 백신 프로그램은 바이러스 감염 여부 진단 및 치료뿐만 아니라 파일 보호를 통한 예방 조치도 가능함. *웜: 악의적인 목적을 가지고 자기 자신의 복제해 전파시키며 주로 네트워크 공유 폴더나 메일로 전파됨. *트로이목마: 고의적으로 악의적 목적이 있는 파일, 주로 다른 악성코드나 위장된 프로그램으로 전파되거나 인터넷을 통해 다운로드 됨.				
보안대책					
판단기준	양호: 바이러스 백신 프로그램이 설치되어 있는 경우				
	취약: 바이러스 백신 프로그램이 설치되어 있지 않은 경우				
조치방법	담당자를 통해 바이러스 반드시 설치하여야 하도록 함				
보안설정방법					
- 안철수 연구소: http://www.ahnlab.com - 하우리: http://www.hauri.co.kr - 시만텍코리아: http://www.symantec.co.kr - 한국트렌드마이크로: http://www.trendmicro.co.kr/					
조치 시 영향	일반적으로 영향 없음				

윈도즈 서버

취약점 항목	5.2. SAM 파일 접근 통제 설정				
대상 OS	NT, 2000, 2003, 2008	위험도	상	Code	W-63
취약점 개요	SAM(Security Account Manager) 파일은 사용자와 그룹 계정의 패스워드를 관리하고, LSA(Local Security Authority)를 통한 인증을 제공함. 따라서 SAM 파일에 대한 패스워드 공격 시도로 인해 패스워드 데이터베이스 정보가 노출될 수 있으므로 Administrator 및 System 그룹 외에는 SAM 파일에 대한 접근을 제한하여야 함.				
보안대책					
판단기준	양호: SAM 파일 접근권한에 Administrator, System 그룹만 모든 권한으로 설정되어 있는 경우				
	취약: SAM 파일 접근권한에 Administrator, System 그룹 외 다른 그룹에 권한이 설정되어 있는 경우				
조치방법	SAM 파일 권한 확인 후 Administrator, System 그룹 외 다른 그룹에 설정된 권한 제거				
보안설정방법					

■ Windows NT

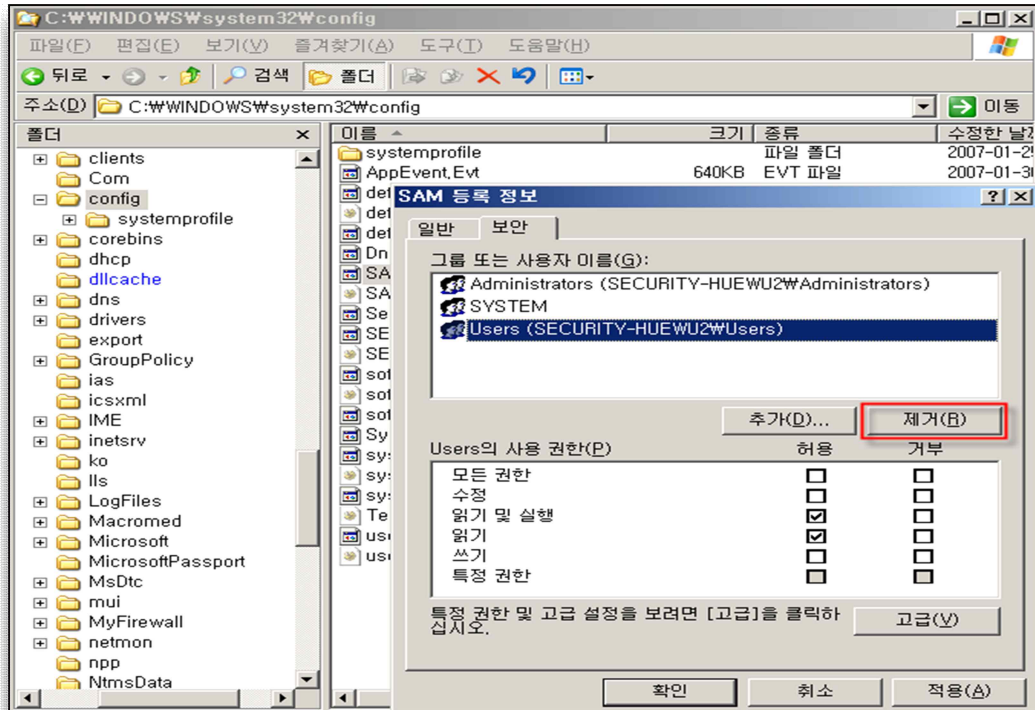
1. %systemroot%\system32\config\SAM> 속성> 보안
2. Administrator, System 그룹 외 다른 사용자 및 그룹 권한 제거



윈도우즈 서버

■ Windows 2000, 2003, 2008

1. %systemroot%\system32\config\SAM> 속성> 보안
2. Administrator, System 그룹 외 다른 사용자 및 그룹 권한 제거



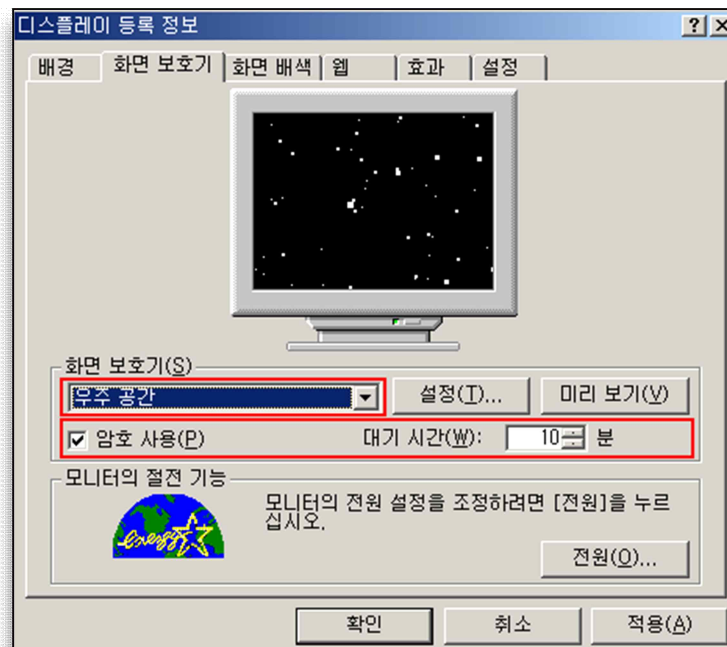
조치 시 영향 일반적으로 영향 없음

윈도우즈 서버

취약점 항목	5.3. 화면 보호기 설정				
대상 OS	NT, 2000, 2003, 2008	위험도	상	Code	W-64
취약점 개요	사용자가 일정 시간 동안 아무런 작업을 수행하지 않을 경우 자동으로 로그오프 되거나 워크스테이션이 잠기도록 설정하여야 함. 해당 기능을 설정하지 않은 경우 사용자가 자리를 비운 사이에 임의의 사용자가 해당 시스템에 접근하여 중요 정보를 유출 하거나, 악의적인 행위를 통해 시스템 운영에 악영향을 미칠 수 있음.				
보안대책					
판단기준	양호:	화면 보호기를 설정하고 대기 시간이 10분 이하의 값으로 설정되어 있으며, 화면 보호기 해제를 위한 암호를 사용하는 경우			
	취약:	화면 보호기가 설정되지 않았거나 암호를 사용하지 않은 경우 또는, 화면 보호기 대기 시간이 10분을 초과한 값으로 설정되어 있는 경우			
조치방법	화면 보호기 사용, 대기 시간 10분, 암호 사용				
보안설정방법					

■ Windows NT, 2000

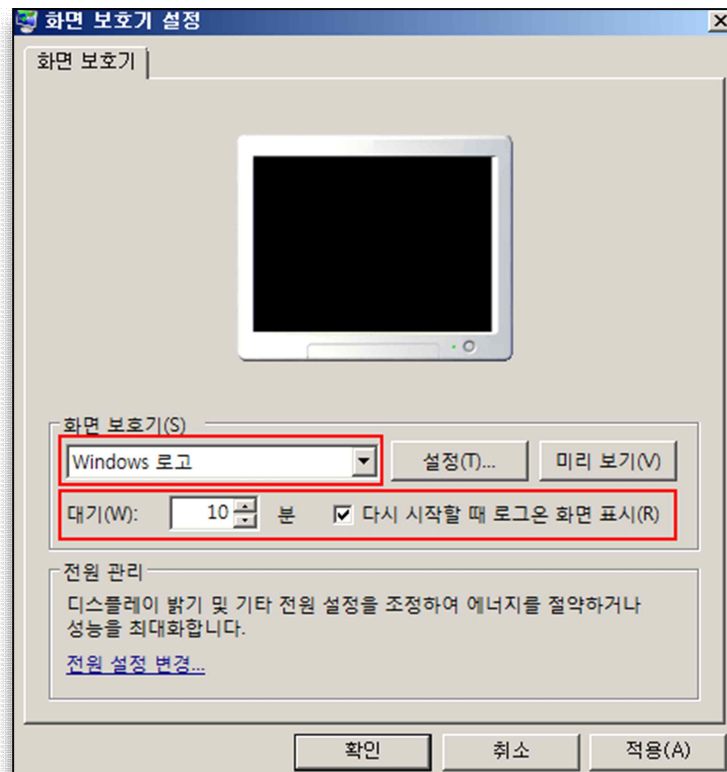
1. 바탕화면> 등록 정보> 화면 보호기> “암호 사용” 체크, 대기 시간 “10분” 설정



■ Windows 2003, 2008

1. 제어판> 개인 설정> 화면 보호기> “다시 시작할 때 로그인 화면 표시” 체크, 대기 시간 “10분” 설정

윈도우즈 서버



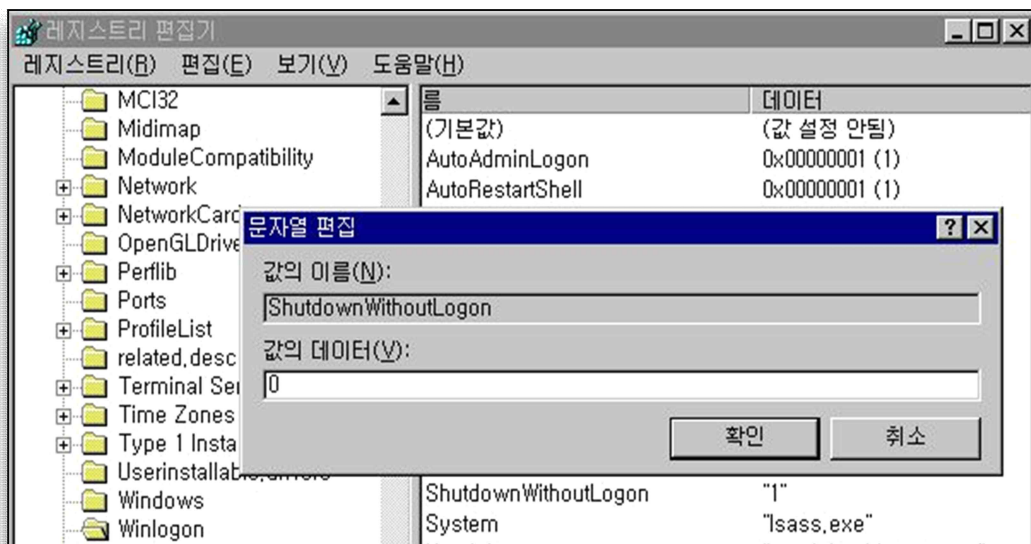
조치 시 영향	일반적인 경우 영향 없음
---------	---------------

윈도우즈 서버

취약점 항목	5.4. 로그인 하지 않고 시스템 종료 허용				
대상 OS	NT, 2000, 2003, 2008	위험도	상	Code	W-65
취약점 개요	로그온 창에 “시스템 종료” 버튼이 활성화되어 있으면 로그인을 하지 않고도 불법적인 시스템 종료가 가능하여 정상적인 서비스 운영이 불가능할 수 있음. 시스템 종료 버튼을 비활성화 시킴으로써 허가되지 않은 사용자가 시스템 종료를 하는 위협을 방지할 수 있음.				
보안대책					
판단기준	양호: “로그온 하지 않고 시스템 종료 허용”이 “사용 안 함”으로 설정되어 있는 경우				
	취약: “로그온 하지 않고 시스템 종료 허용”이 “사용”으로 설정되어 있는 경우				
조치방법	시스템 종료: 로그인 하지 않고 시스템 종료 허용 → 사용 안 함				
보안설정방법					

■ Windows NT

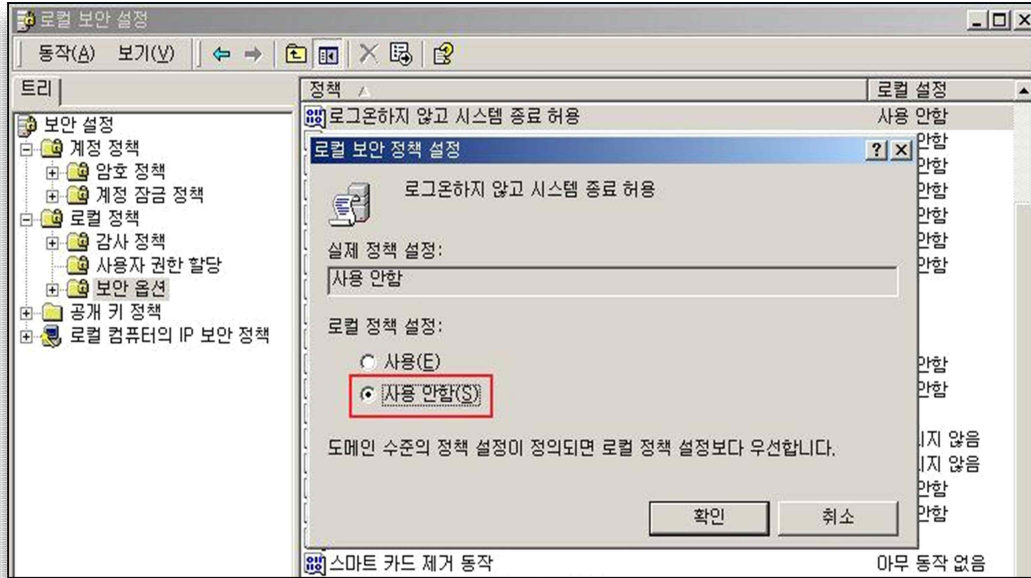
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\ShutdownWithoutLogon = 0



윈도우즈 서버

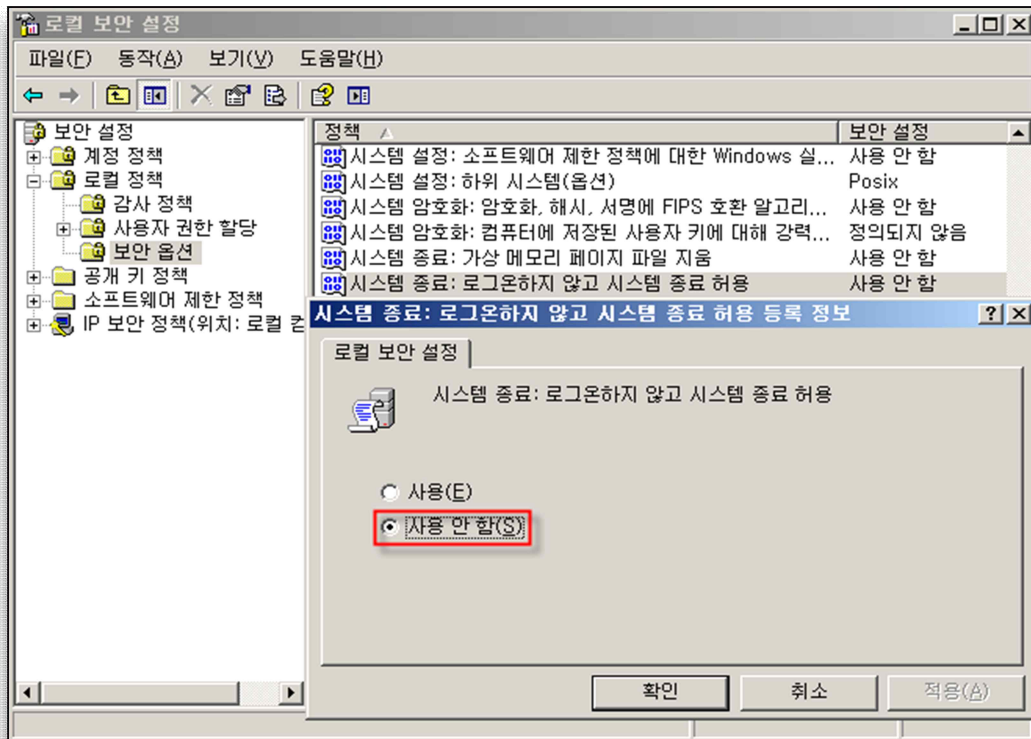
■ Windows 2000

1. 시작 > 실행 > SECPOL.MSC > 로컬 정책 > 보안 옵션
2. "로그온 하지 않고 시스템 종료 허용"을 "사용 안함"으로 설정



■ Windows 2003, 2008

1. 시작 > 실행 > SECPOL.MSC > 로컬 정책 > 보안 옵션
2. "시스템 종료: 로그인 하지 않고 시스템 종료 허용"을 "사용 안 함"으로 설정



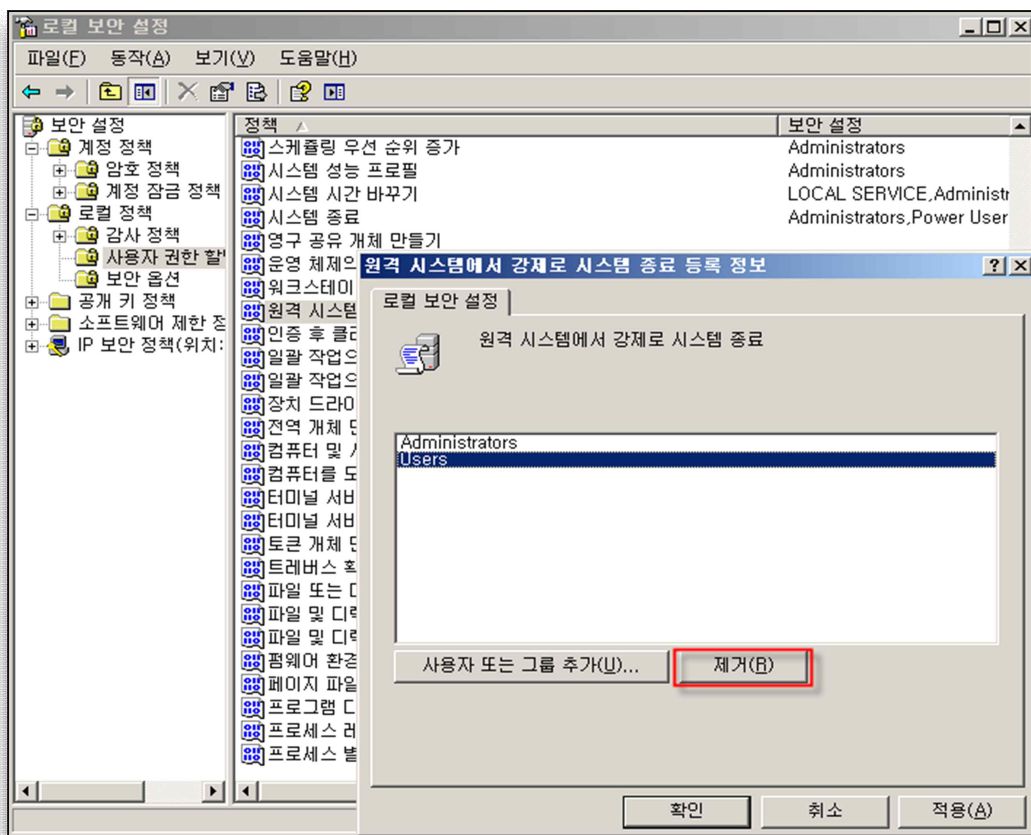
조치 시 영향 | 일반적인 경우 영향 없음

윈도우즈 서버

취약점 항목	5.5. 원격 시스템에서 강제로 시스템 종료				
대상 OS	NT, 2000, 2003, 2008	위험도	상	Code	W-66
취약점 개요	원격에서 네트워크를 통하여 운영 체제를 종료할 수 있는 사용자나 그룹을 결정하여 특정 사용자만 제어할 수 있도록 설정함. 만약 해당 권한 부여가 부적절할 경우 서비스 거부 공격에 악용될 수 있음.				
보안대책					
판단기준	양호: “원격 시스템에서 강제로 시스템 종료” 정책에 “Administrators”만 존재하는 경우				
	취약: “원격 시스템에서 강제로 시스템 종료” 정책에 “Administrators” 외 다른 계정 및 그룹이 존재하는 경우				
조치방법	원격 시스템에서 강제로 시스템 종료 → Administrators				
보안설정방법					

■ Windows NT, 2000, 2003, 2008

1. 시작 > 실행 > SECPOL.MSC > 로컬 정책 > 사용자 권한 할당
2. “원격 시스템에서 강제로 시스템 종료” 정책에 Administrators 외 다른 계정 및 그룹 제거



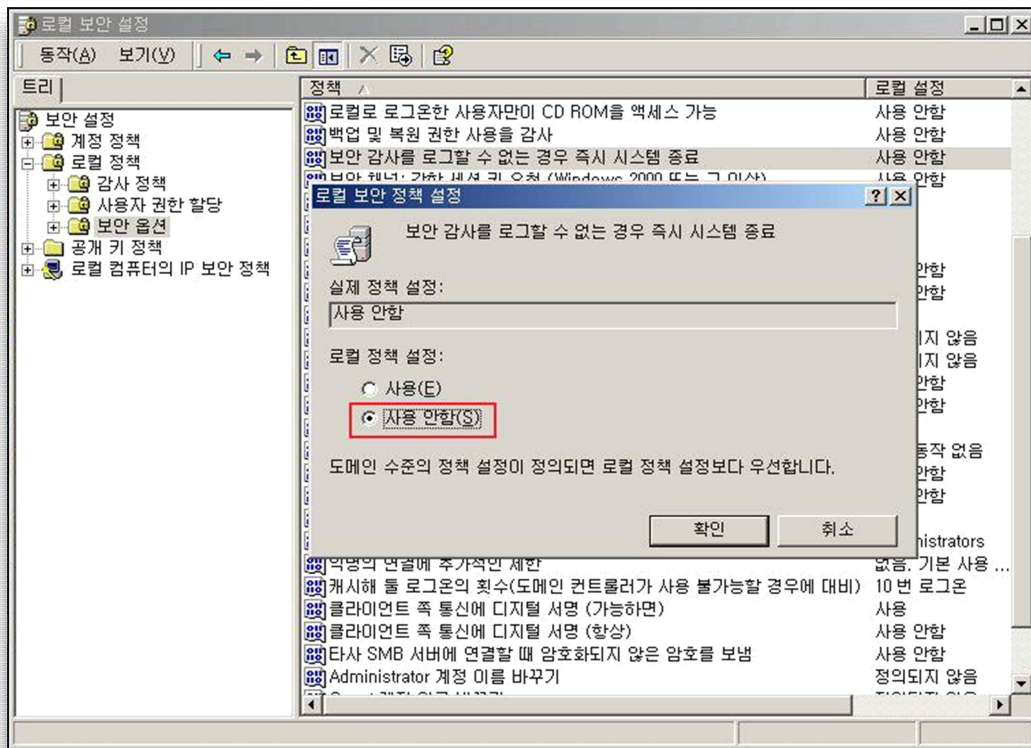
조치 시 영향 일반적으로 영향 없음

윈도우즈 서버

취약점 항목	5.6. 보안 감사를 로그할 수 없는 경우 즉시 시스템 종료				
대상 OS	NT, 2000, 2003, 2008	위험도	상	Code	W-67
취약점 개요	보안 감사를 로그할 수 없는 경우 즉시 시스템 종료 여부 설정으로 보안 이벤트를 기록할 수 없는 경우 컴퓨터를 종료할 것인지 결정함. 이 정책을 사용 시 서비스 거부 공격에 악용될 수 있으며, 비정상적인 시스템 종료로 인하여 시스템 및 데이터에 손상을 입힐 수 있음.				
보안대책					
판단기준	양호: "보안 감사를 로그할 수 없는 경우 즉시 시스템 종료" 정책이 "사용 안 함"으로 되어 있는 경우				
	취약: "보안 감사를 로그할 수 없는 경우 즉시 시스템 종료" 정책이 "사용"으로 되어 있는 경우				
조치방법	Windows 2000: 보안 감사를 로그할 수 없는 경우 즉시 시스템 종료 → 사용 안 함 Windows 2003: 감사: 보안 감사를 로그할 수 없는 경우 즉시 시스템 종료 → 사용 안 함 Windows 2008: 감사: 보안 감사를 로그할 수 없는 경우 즉시 시스템 종료 → 사용 안 함				
보안설정방법					

■ Windows NT, 2000

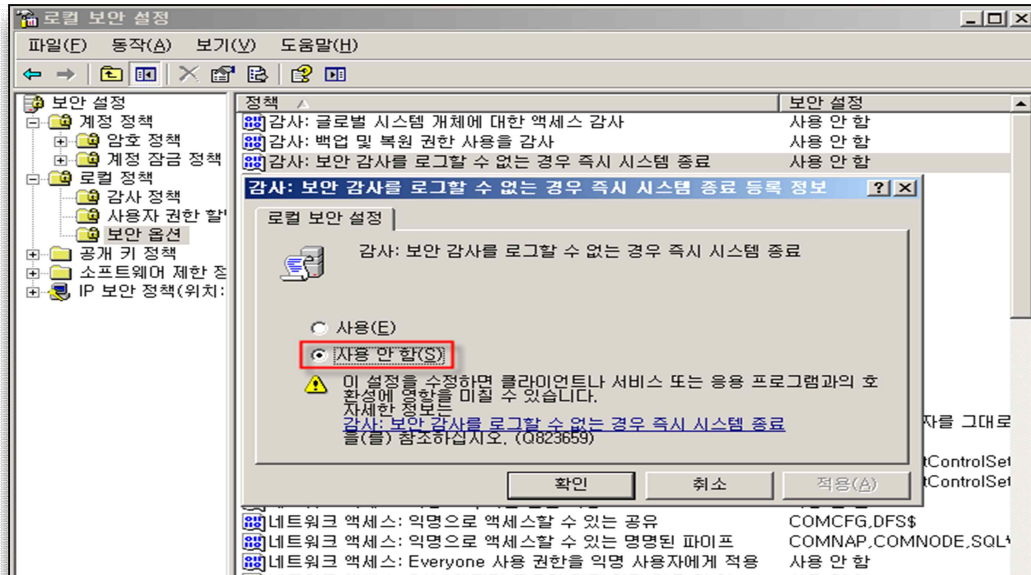
1. 시작> 실행> SECPOL.MSC> 로컬 정책> 보안 옵션
2. "보안 감사를 로그할 수 없는 경우 즉시 시스템 종료" 정책을 "사용 안 함" 으로 설정



윈도즈 서버

■ Windows 2003, 2008

1. 시작> 실행> SECPOL.MSC> 로컬 정책> 보안 옵션
2. "감사: 보안 감사를 로그할 수 없는 경우 즉시 시스템 종료" 정책을 "사용 안 함" 으로 설정



조치 시 영향

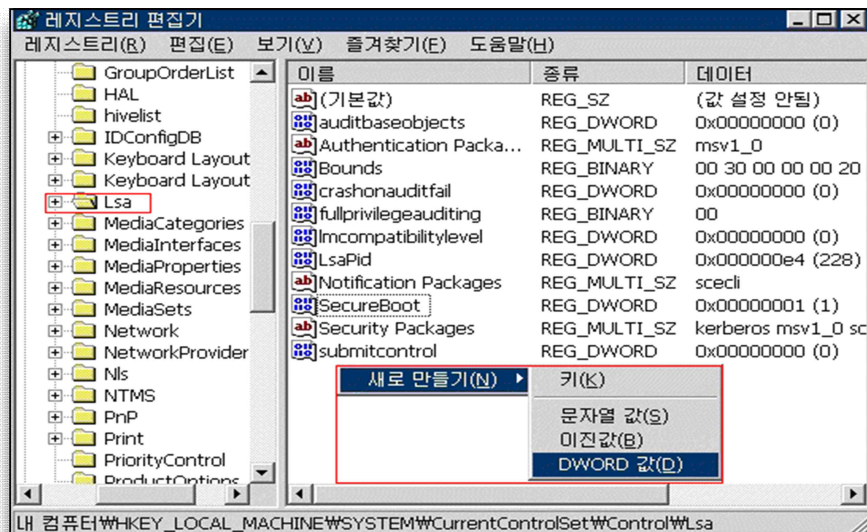
일반적으로 영향 없음

윈도우즈 서버

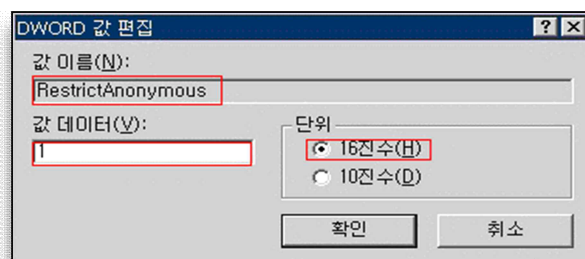
취약점 항목	5.7. SAM 계정과 공유의 익명 열거 허용 안 함				
대상 OS	NT, 2000, 2003, 2008	위험도	상	Code	W-68
취약점 개요	Windows에서는 익명의 사용자가 도메인 계정(사용자, 컴퓨터 및 그룹)과 네트워크 공유 이름의 열거 작업을 수행할 수 있으므로 SAM(보안계정관리자) 계정과 공유의 익명 열거가 허용될 경우 악의적인 사용자가 계정 이름 목록을 확인하고 이 정보를 사용하여 암호를 추측하거나 사회 공학적 공격기법을 수행할 수 있음.				
보안대책					
판단기준	양호: 해당 보안 옵션 값이 설정 되어 있는 경우				
	취약: 해당 보안 옵션 값이 설정 되어 있지 않는 경우				
조치방법	레지스트리 값 또는, 로컬 보안 정책 설정				
보안설정방법					

■ Windows NT

1. 시작> 실행> regedit
2. HKLM\SYSTEM\CurrentControlSet\Control\Lsa 레지스트리 검색
3. 우클릭 후 새로 만들기> DWORD 값 선택



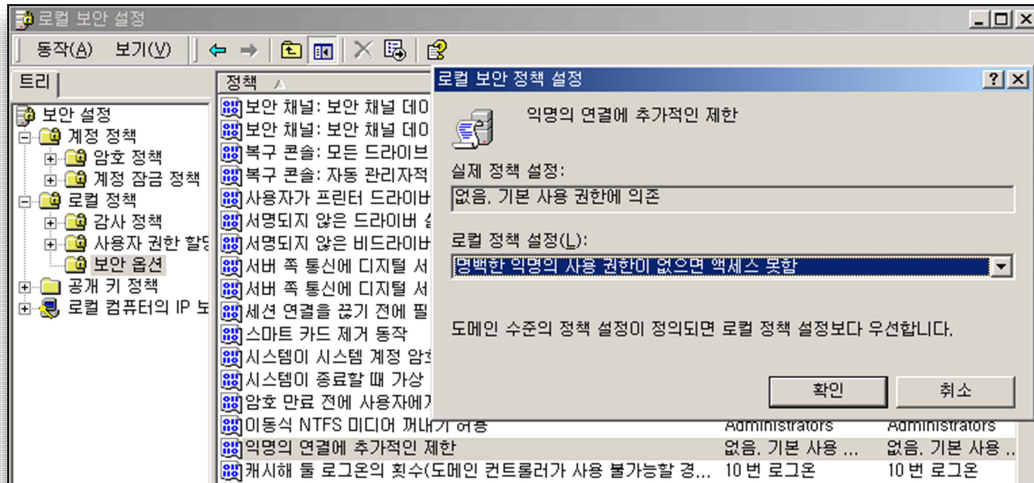
4. RestrictAnonymous를 입력 후 데이터 Default 값인 "0"을 "1"로 변경



윈도우즈 서버

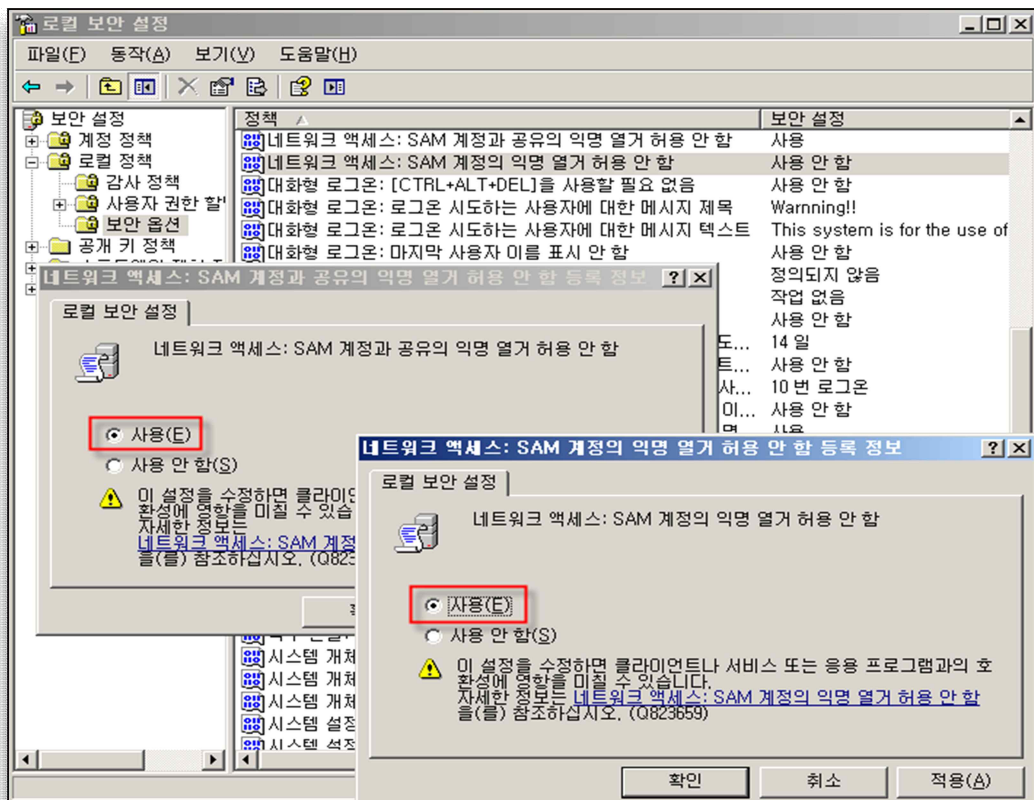
■ Windows 2000

1. 시작> 실행> SECPOL.MSC> 로컬 정책> 보안 옵션
2. “익명의 연결에 추가적인 제한”에 “명백한 익명의 사용 권한이 없으면 액세스 제한” 선택



■ Windows 2003, 2008

1. 시작> 실행> SECPOL.MSC> 로컬 정책> 보안 옵션
2. “SAM 계정과 공유의 익명 열거 허용 안 함”과 “SAM 계정의 익명 열거 허용 안 함”에 “사용” 선택



윈도우즈 서버

- 방화벽과 라우터에서 135~139(TCP, UDP)포트 차단을 통해 외부로부터의 위협을 차단함
- 원천적으로 봉쇄
- 네트워크 및 전화 접속 연결> 로컬 영역> 등록 정보> 고급> 고급 설정> Microsoft 네트워크 파일 및 프린트 공유를 해제하여야 함

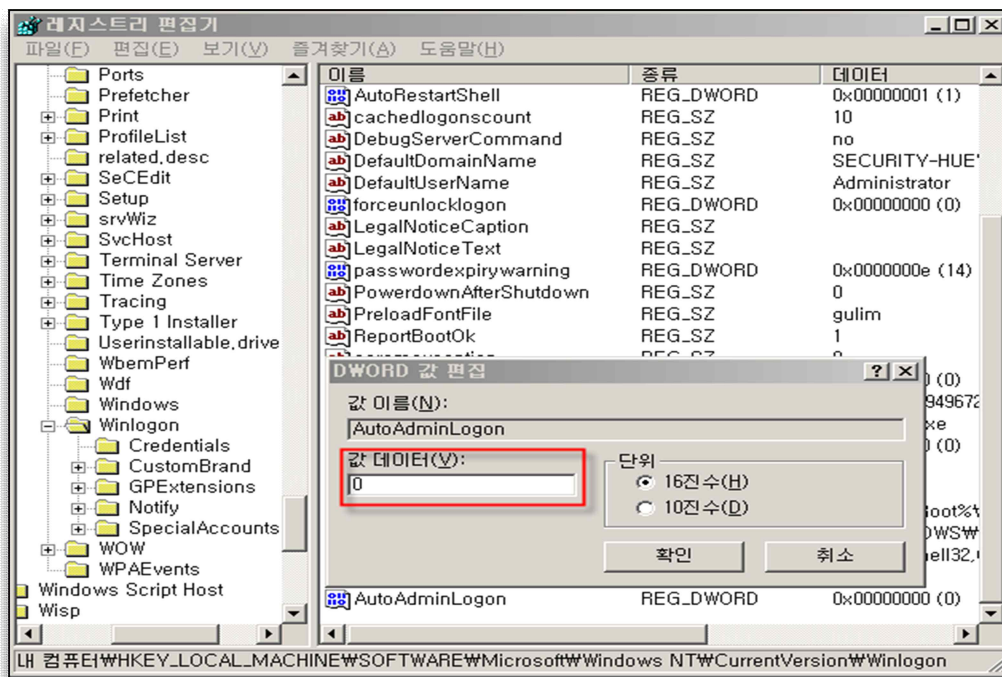
조치 시 영향	Active Directory, Clustered system 에서는 적용 시 영향 있음
----------------	---

윈도우즈 서버

취약점 항목	5.8. Autologon 기능 제어				
대상 OS	NT, 2000, 2003, 2008	위험도	상	Code	W-69
취약점 개요	*Autologon 기능을 사용하면 침입자가 해킹 도구를 이용하여 레지스트리에서 로그인 계정 및 암호를 확인할 수 있으므로 Autologon 기능을 사용하지 않도록 설정함. *Autologon: 레지스트리에 암호화 되어 저장된 대체 증명을 사용하여 자동으로 로그인하는 기능.				
보안대책					
판단기준	양호: AutoAdminLogon 값이 없거나 0으로 설정되어 있는 경우				
	취약: AutoAdminLogon 값이 1로 설정되어 있는 경우				
조치방법	해당 레지스트리 값이 존재하는 경우 0으로 설정				
보안설정방법					

■ Windows NT, 2000, 2003

1. 시작> 실행> REGEDIT> HKLM\SOFTWARE\Microsoft\WindowsNT\CurrentVersion\Winlogon
2. "AutoAdminLogon 값"을 "0"으로 설정
3. DefaultPassword 엔트리가 존재한다면 삭제



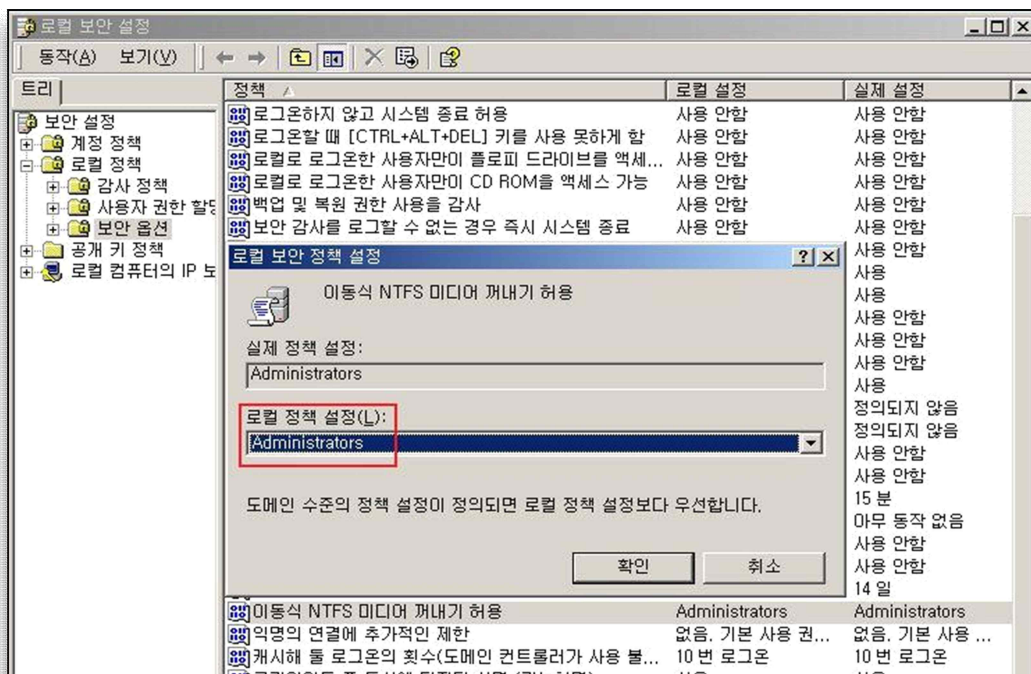
조치 시 영향 반드시 자동 로그인을 사용하여야 할 경우를 제외하고는 일반적으로 영향 없음

윈도우즈 서버

취약점 항목	5.9. 이동식 미디어 포맷 및 꺼내기 허용				
대상 OS	NT, 2000, 2003, 2008	위험도	상	Code	W-70
취약점 개요	이동식 미디어의 NTFS 포맷 및 꺼내기가 허용되는 사용자를 제한함으로써 사용자가 관리 권한을 갖고 있는 임의의 컴퓨터로만 이동식 디스크의 데이터를 이동하고, 파일에 대한 소유권을 얻어 파일을 보거나 수정할 수 있도록 함.				
보안대책					
판단기준	양호: "이동식 미디어 포맷 및 꺼내기 허용" 정책이 "Administrator"로 되어 있는 경우				
	취약: "이동식 미디어 포맷 및 꺼내기 허용" 정책이 "Administrator"로 되어 있지 않은 경우				
조치방법	이동식 미디어 포맷 및 꺼내기 허용 → Administrator				
보안설정방법					

■ Windows NT, 2000

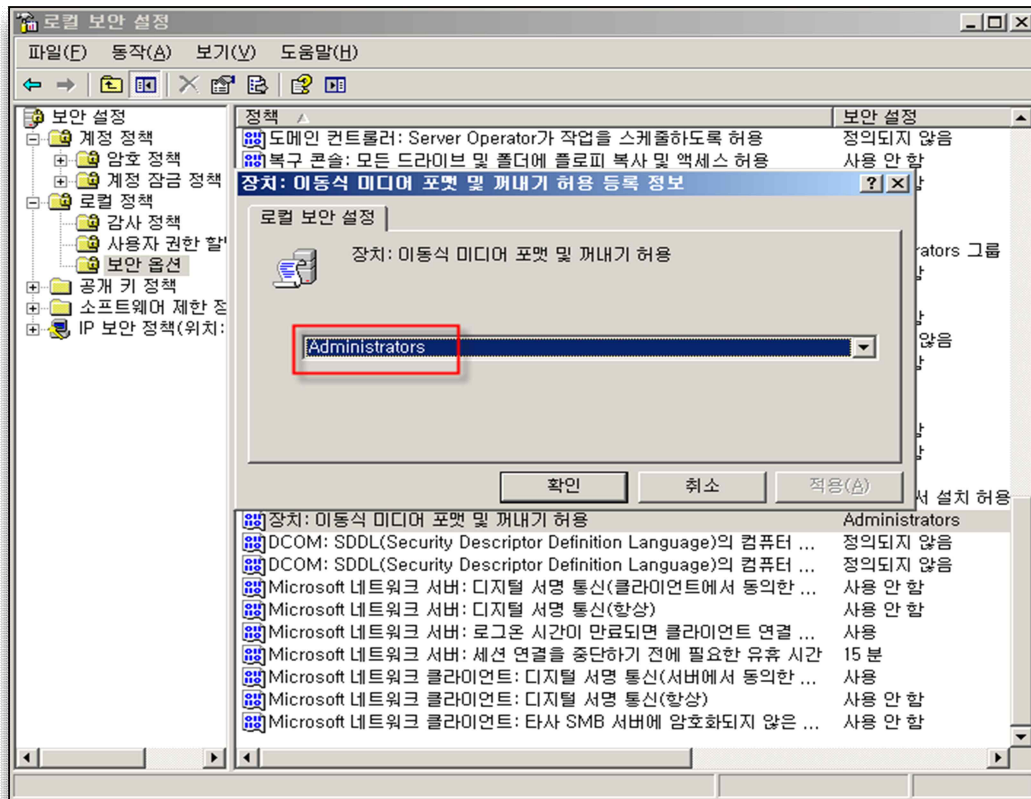
1. 시작> 실행> SECPOL.MSC> 로컬 정책> 보안 옵션
2. "이동식 NTFS 미디어 꺼내기 허용" 정책을 "Administrators" 로 설정



■ Windows 2003, 2008

1. 시작> 실행> SECPOL.MSC> 로컬 정책> 보안 옵션
2. "이동식 미디어 포맷 및 꺼내기 허용" 정책을 "Administrators" 로 설정

윈도우즈 서버



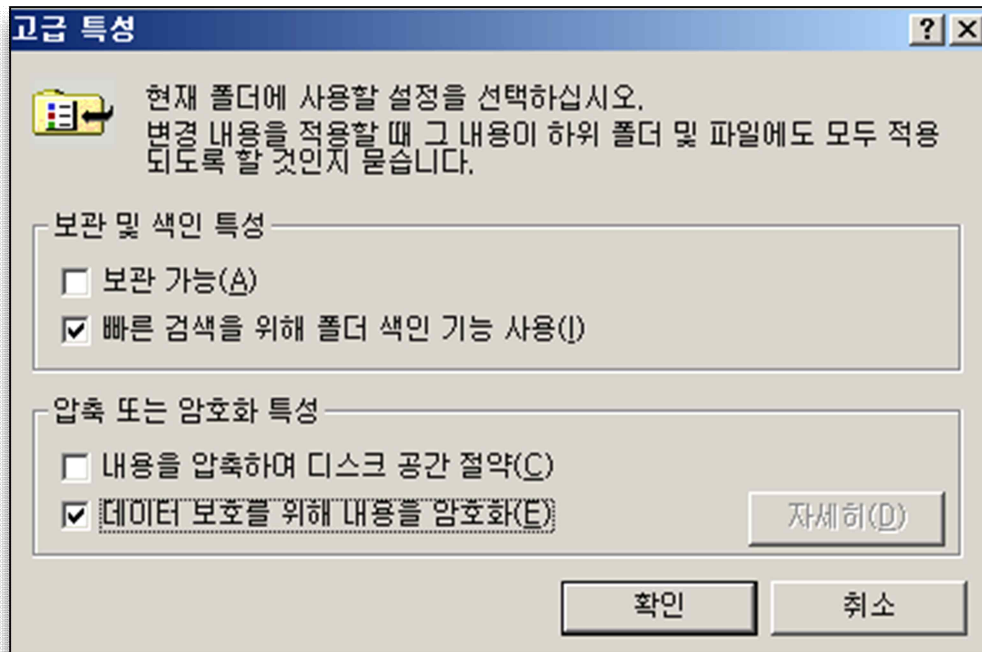
조치 시 영향	일반적으로 영향 없음
---------	-------------

윈도우즈 서버

취약점 항목	5.10. 디스크볼륨 암호화 설정				
대상 OS	2000, 2003	위험도	상	Code	W-71
취약점 개요	디스크 볼륨이 암호화 되어 있지 않은 경우 비인가자가 데이터를 열람할 수 있음				
보안대책					
판단기준	양호: "데이터 보호를 위해 내용을 암호화 "정책이 선택된 경우				
	취약: "데이터 보호를 위해 내용을 암호화 "정책이 선택되어 있지 않은 경우				
조치방법	EFS(Encrypting File System) 활성화				
보안설정방법					

■ Windows 2000, 2003

1. 폴더 선택 > 속성 > [일반] 탭 > 고급 > 고급 특성 > "데이터 보호를 위해 내용을 암호화" 선택



조치 시 영향 복호키 분실 시 데이터복구 어려움

윈도우즈 서버

취약점 항목		5.11. Dos공격 방어 레지스트리 설정			
대상 OS	NT, 2000, 2003	위험도	중	Code	W-72
취약점 개요	Dos(서비스 거부 공격)은 네트워크 사용자가 컴퓨터나 컴퓨터의 특정 서비스를 사용할 수 없도록 만들기 위한 네트워크 공격으로, TCP/IP 스택(Stack)을 강화하는 레지스트리 값 변경을 통하여 Dos 공격을 방어할 수 있음. 만약 Dos 방어 레지스트리를 설정하지 않은 경우 Dos 공격에 의한 시스템 다운으로 서비스 제공이 중단될 수 있음.				
보안대책					
판단기준	양호: DOS 방어 레지스트리 값이 아래와 같이 설정되어 있는 경우				
	취약: DOS 방어 레지스트리 값이 아래와 같이 설정되어 있지 않은 경우 • SynAttackProtect = REG_DWORD 0(False) -> 1 이상 • EnableDeadGWDetect = REG_DWORD 1(True) -> 0 • KeepAliveTime = REG_DWORD 7,200,000(2시간) -> 300,000(5분) • NoNameReleaseOnDemand = REG_DWORD 0(False) -> 1				
조치방법	위에 명시된 레지스트리 값을 추가 또는, 변경하여 적용함				
보안설정방법					
레지스트리 값 이름		설명			
SynAttackProtect		SYN-ACK 패킷의 기다리는 시간을 줄여 SYN 공격에 대한 방어 기능 기능을 설정할 수 있음 • 0 => SynAttack 프로텍션을 사용하지 않음 • 1 => 재전송 시도를 줄이고, route 캐쉬 엔트리를 지연시킴 • 2 => 1의 기능 외에도 Winsock에 대한 지시(indication)를 지연시킴			
EnableDeadGWDetect		EnableDeadGWDetect를 0으로 설정하지 않으면 서버가 강제로 원하지 않는 Gateway로 전환될 수 있음 • 0 => (False) 작동하지 않는 Gateway를 검색할 수 없음 • 1 => (True) 작동하지 않는 Gateway를 검색할 수 있음			
KeepAliveTime		idle connection을 확인하기 위하여 얼마나 자주 Keep-alive 패킷을 보낼지를 결정하는 값임 • 기본 값 => 7,200,000(2시간) • 권장 값 => 300,000(5분)			
NoNameReleaseOnDemand		컴퓨터가 이름 해제 요청을 받을 때 NetBIOS 이름 해제 여부를 결정하는 설정으로 이 값은 관리자가 악의적인 이름 해제 공격으로부터 컴퓨터를 보호할 수 있음. • 0 => (False) 해당 기능 사용 안 함 • 1 => (True) 해당 기능 사용			

윈도우즈 서버

■ Windows NT, 2000, 2003

1. 시작 > 실행 > REGEDIT
2. HKLM\System\CurrentControlSet\Services\Tcpip\Parameters\ 검색
3. 다음의 DOS 방어 레지스트리 값 추가 또는, 변경

레지스트리 값 이름	값 종류	유효 범위	권장 설정 값
SynAttackProtect	REG_DWORD	0, 1, 2	1 또는, 2
EnableDeadGWDetect	REG_DWORD	0, 1 (False, True)	0 (False)
KeepAliveTime	REG_DWORD	1 - 0xFFFFFFFF	300,000(5분)으로 변경
NoNameReleaseOnDemand	REG_DWORD	0, 1 (False, True)	1 (True)

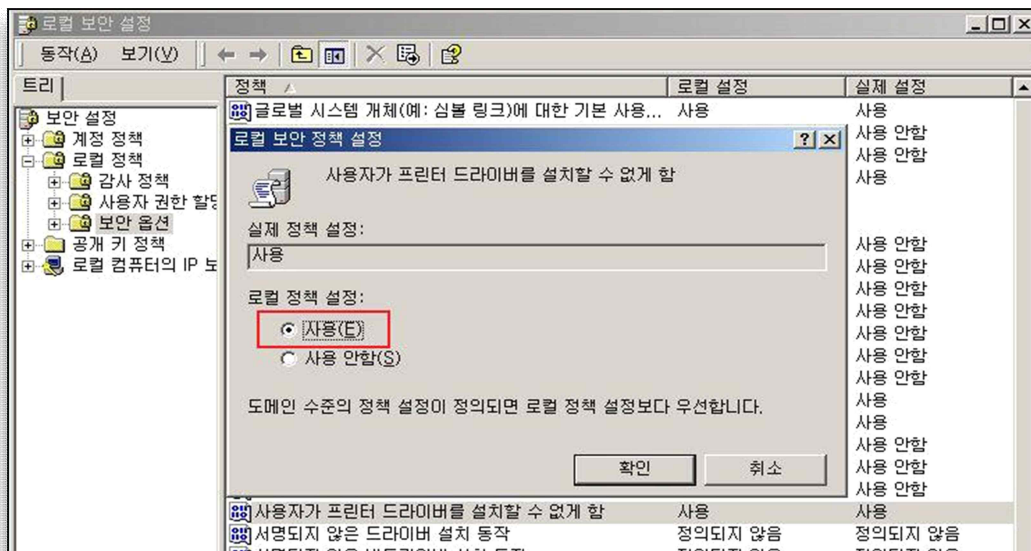
조치 시 영향 잘못된 값을 설정할 경우 OS 재설치를 요구할 수 있음

윈دوز즈 서버

취약점 항목	5.12. 사용자가 프린터 드라이버를 설치할 수 없게 함				
대상 OS	NT, 2000, 2003, 2008	위험도	중	Code	W-73
취약점 개요	서버에 프린터 드라이버를 설치하는 경우 악의적인 사용자가 고의적으로 잘못된 프린터 드라이버를 설치하여 컴퓨터를 손상시킬 수 있으며, 프린터 드라이버로 위장한 악성 코드를 설치할 수 있으므로 사용자가 프린터 드라이버를 설치할 수 없게 설정하여야 함.				
보안대책					
판단기준	양호: "사용자가 프린터 드라이버를 설치할 수 없게 함" 정책이 "사용"인 경우				
	취약: "사용자가 프린터 드라이버를 설치할 수 없게 함" 정책이 "사용 안 함"인 경우				
조치방법	사용자가 프린터 드라이버를 설치할 수 없게 함 → 사용				
보안설정방법					

■ Windows NT, 2000

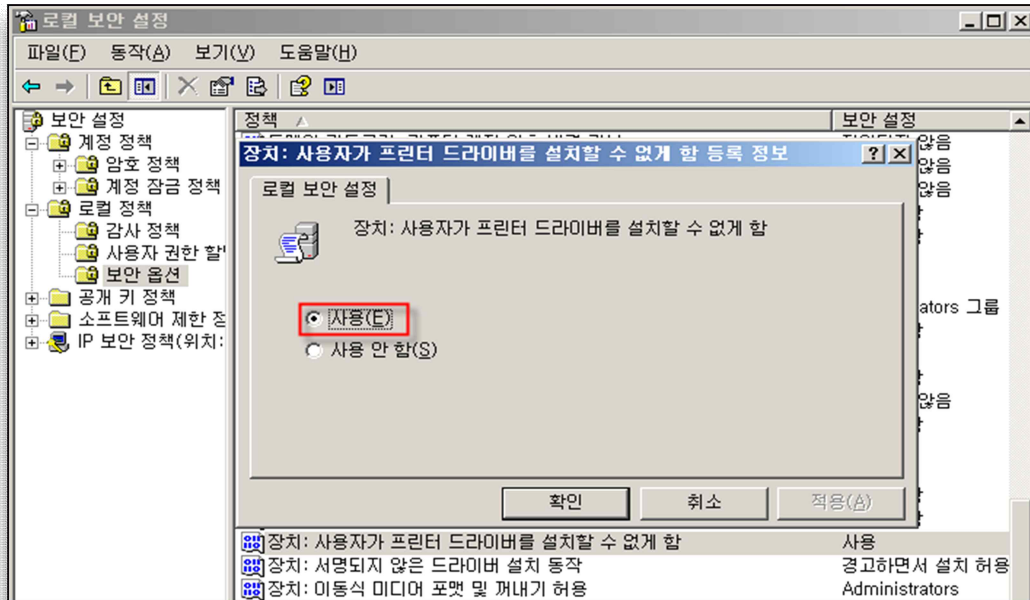
1. 시작> 실행> SECPOL.MSC> 로컬 정책> 보안 옵션
2. "사용자가 프린터 드라이버를 설치할 수 없게 함" 정책을 "사용" 으로 설정



윈도우즈 서버

■ Windows 2003, 2008

1. 시작 > 실행 > SECPOL.MSC > 로컬 정책 > 보안 옵션
2. "장치: 사용자가 프린터 드라이버를 설치할 수 없게 함" 정책을 "사용" 으로 설정



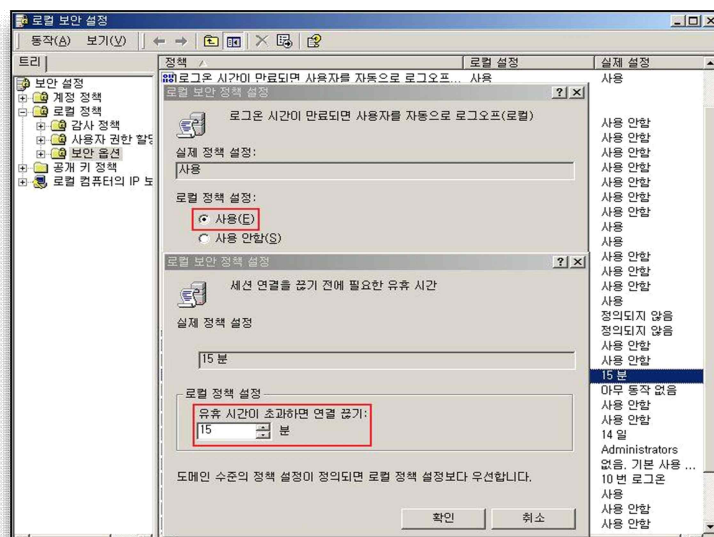
조치 시 영향 일반적으로 영향 없음

윈도우즈 서버

취약점 항목	5.13. 세션 연결을 중단하기 전에 필요한 유휴시간				
대상 OS	NT, 2000, 2003, 2008	위험도	중	Code	W-74
취약점 개요	세션이 중단되기 전에 *SMB(서버 메시지 블록) 세션에서 보내야 하는 연속 유휴 시간을 결정할 수 있음. 각 SMB 세션에서는 서버 리소스를 사용하며, null(공백) 세션 수가 많으면 서버 속도가 느려지거나 서버에 오류를 발생시킬 수 있으므로 공격자는 이를 악용하여 SMB 세션을 반복 설정하여 서버의 SMB 서비스가 느려지거나 응답하지 않게 하여 서비스 거부 공격을 실행 할 수 있음. ※ Administrator는 이 정책을 활성화하여 컴퓨터가 비활성 SMB 세션을 중단하는 시점을 제어할 수 있으며, 클라이언트를 다시 시작하면 해당 세션은 자동으로 다시 연결됨. 이 정책의 값을 0으로 설정하면 가능한 한 빨리 유휴 세션 연결은 끊어지며, 최대 값은 99999(208일)로 사실상 정책 설정 해제를 의미함. *SMB(서버 메시지 블록): LAN이나 컴퓨터 간의 통신에서 데이터 송수신을 하기 위한 프로토콜				
보안대책					
판단기준	양호: "로그온 시간이 만료되면 클라이언트 연결 끊기" 정책을 "사용"으로, "세션 연결을 중단하기 전에 필요한 유휴 시간" 정책을 "15분"으로 설정한 경우 취약: "로그온 시간이 만료되면 클라이언트 연결 끊기" 정책이 "사용 안 함"으로, "세션 연결을 중단하기 전에 필요한 유휴 시간" 정책이 "15분"으로 설정되어 있지 않은 경우				
조치방법	로그온 시간이 만료되면 클라이언트 연결 끊기 → 사용 세션 연결을 중단하기 전에 필요한 유휴 시간 → 15분				
보안설정방법					

■ Windows NT, 2000

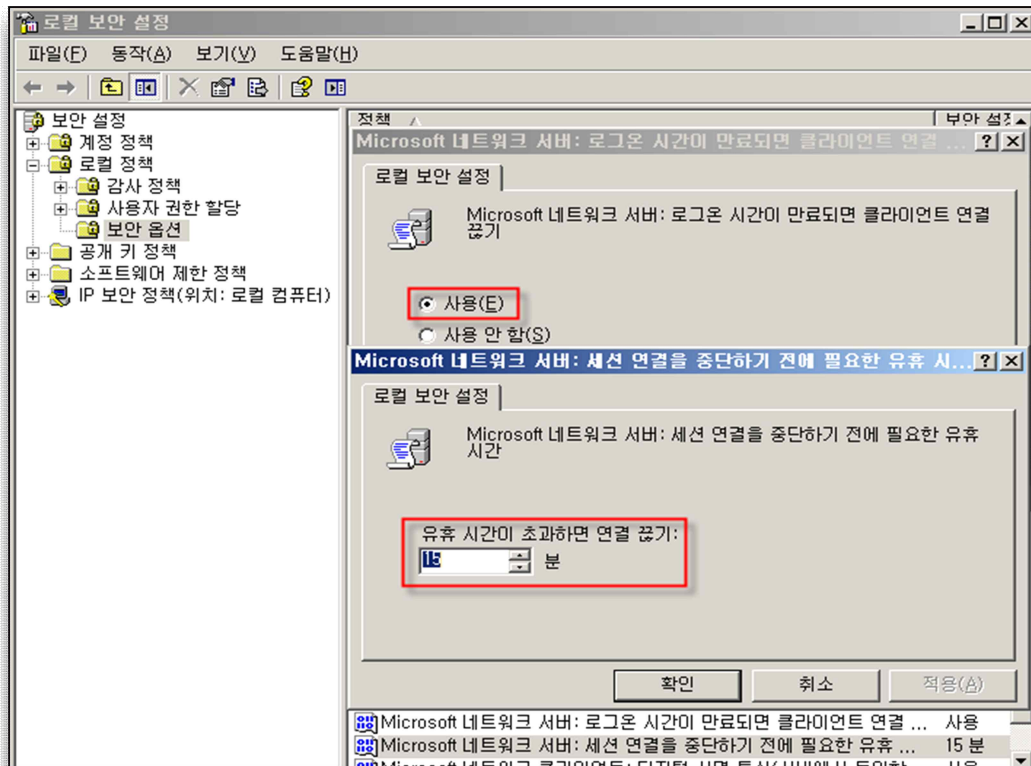
1. 시작> 실행> SECPOL.MSC> 로컬 정책> 보안 옵션
2. "로그인 시간이 만료되면 클라이언트 연결 끊기" 정책 "사용" 설정
"세션 연결을 중단하기 전에 필요한 유휴 시간" 정책 "15분" 설정



윈도우즈 서버

■ Windows 2003, 2008

1. 시작 > 실행 > SECPOL.MSC > 로컬 정책 > 보안 옵션
2. "로그온 시간이 만료되면 클라이언트 연결 끊기" 정책 "사용" 설정
"세션 연결을 중단하기 전에 필요한 유휴 시간" 정책 "15분" 설정



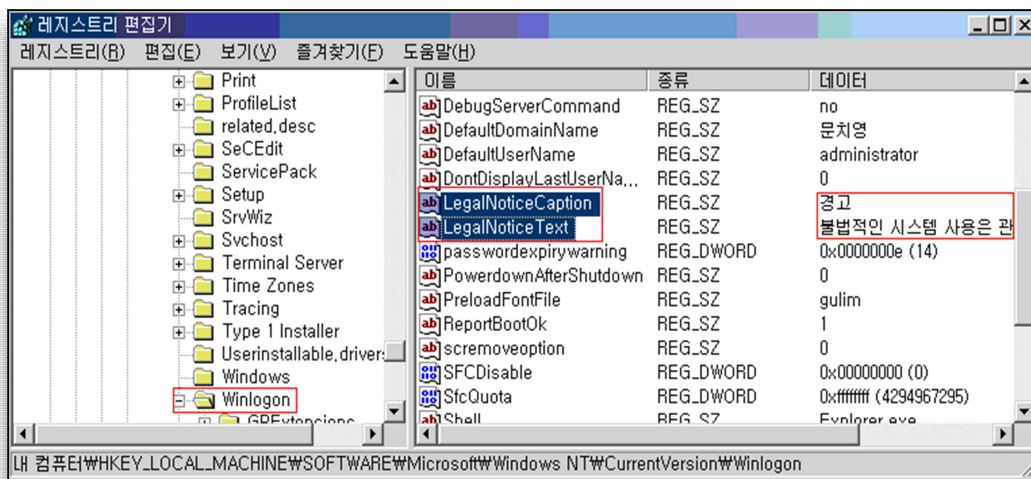
조치 시 영향	일반적으로 영향 없음
---------	-------------

윈도우즈 서버

취약점 항목	5.14. 경고 메시지 설정				
대상 OS	NT, 2000, 2003, 2008	위험도	하	Code	W-75
취약점 개요	시스템에 로그인을 시도하는 사용자에게 관리자는 시스템의 불법적인 사용에 대하여 경고 창을 띄움으로써 경각심을 줄 수 있음. 이러한 경고창의 효과는 악의적인 사용자에게 관리자가 적절한 보안수준으로 시스템을 보호하고 있으며, 공격자의 활동을 주시하고 있다는 생각을 상기시킴으로써 간접적으로 공격 피해를 감소시키는 효과를 볼 수 있음.				
보안대책					
판단기준	양호: 로그인 경고 메시지제목 및 내용이 설정되어 있는 경우				
	취약: 로그인 경고 메시지제목 및 내용이 설정되어 있지 않은 경우				
조치방법	로그인 메시지 제목 및 메시지 내용에 경고 문구 삽입				
보안설정방법					

■ Windows NT

1. HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon
2. LegalNoticeCaption: 제목
3. LegalNoticeText: 메시지 내용

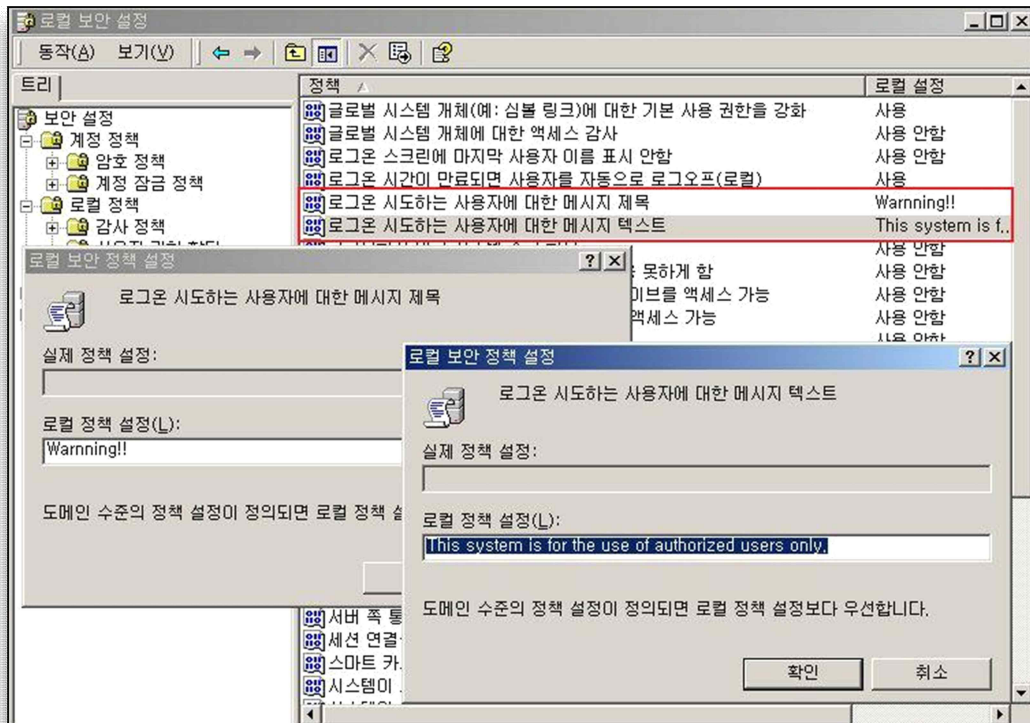


※ 이처럼 변경된 레지스트리 키의 내용은 시스템을 로그오프 한 후 반영됨

윈도우즈 서버

■ Windows 2000

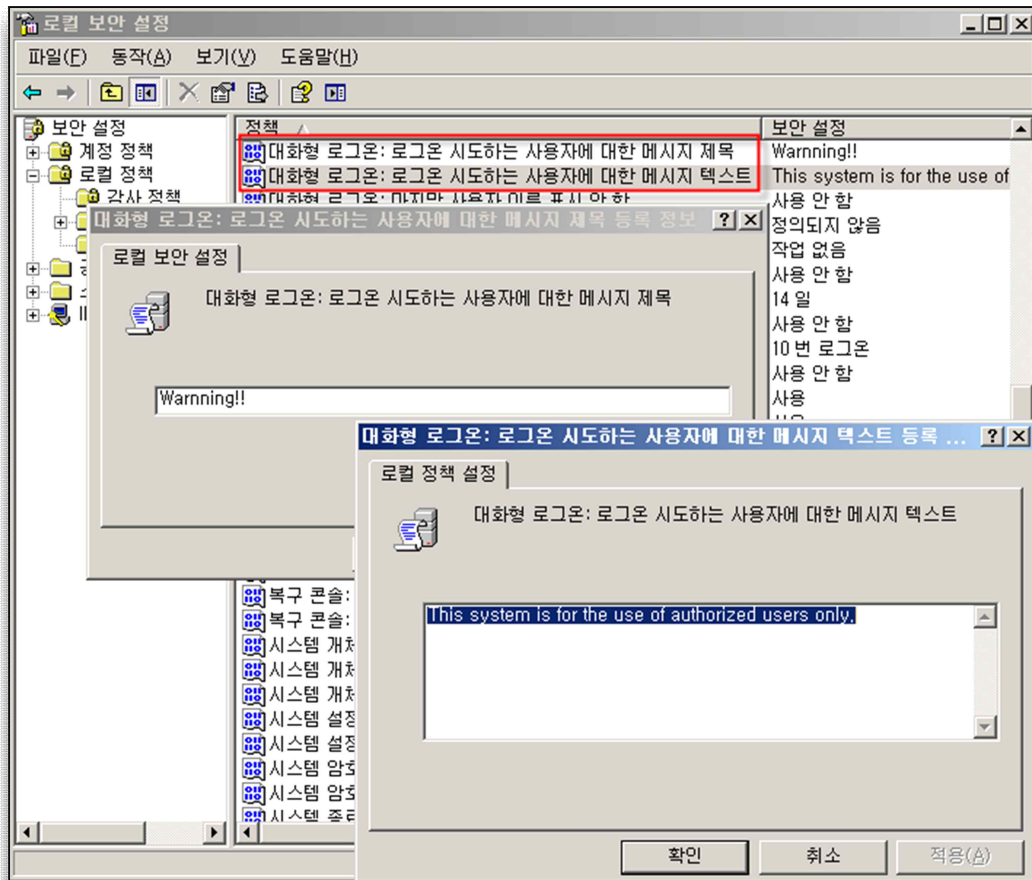
1. 시작> 실행> SECPOL.MSC> 로컬 정책> 보안 옵션
2. 로그인 시도하는 사용자에게 대한 메시지 제목: 배너 제목 입력
3. 로그인 시도하는 사용자에게 대한 메시지 텍스트: 배너 내용 입력



윈도우즈 서버

■ Windows 2003, 2008

1. 시작 > 실행 > SECPOL.MSC > 로컬 정책 > 보안 옵션
2. 대화형 로그인: 로그인 시도하는 사용자에게 대한 메시지 제목: 배너 제목 입력
3. 대화형 로그인: 로그인 시도하는 사용자에게 대한 메시지 텍스트: 배너 내용 입력



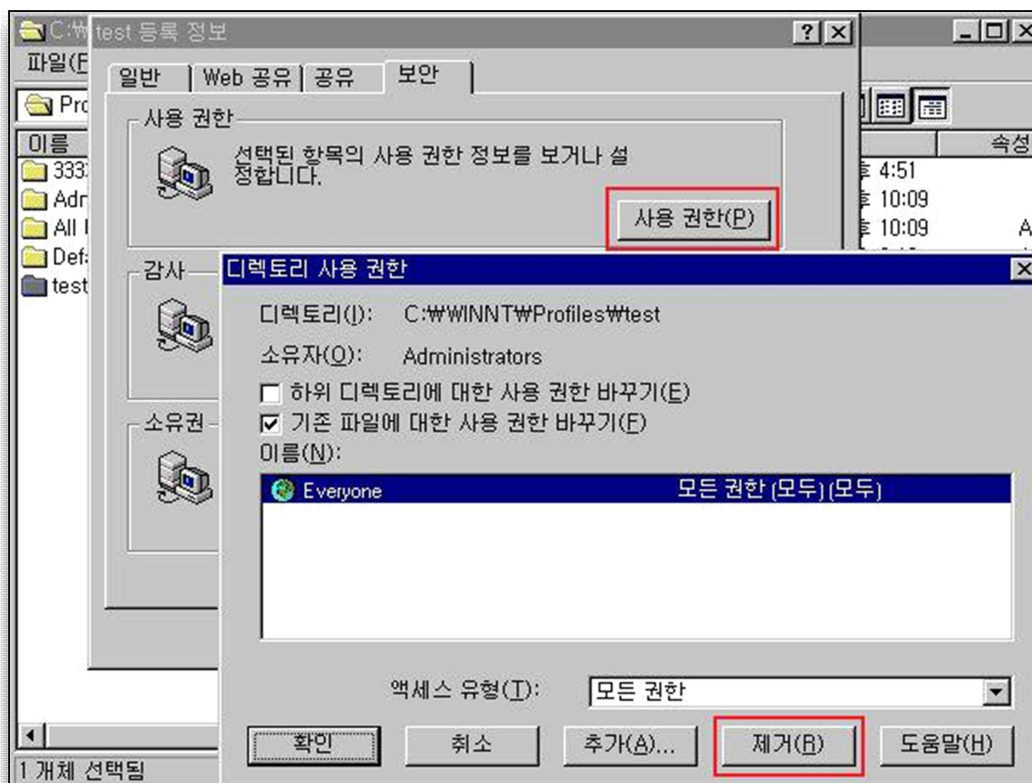
조치 시 영향 일반적인 경우 영향 없음

윈도즈 서버

취약점 항목	5.15. 사용자별 홈 디렉터리 권한 설정				
대상 OS	NT, 2000, 2003, 2008	위험도	중	Code	W-76
취약점 개요	사용자 계정별 홈 디렉터리의 권한이 제한되어 있지 않은 경우 임의의 사용자 다른 사용자의 홈 디렉터리에 악의적인 목적으로 접근할 수 있으며, 접근 후 의도 또는, 의도하지 않은 행위로 시스템에 악영향을 미칠 수 있음.				
보안대책					
판단기준	양호: 홈 디렉터리에 Everyone 권한이 없는 경우(All Users, Default User 디렉터리 제외)				
	취약: 홈 디렉터리에 Everyone 권한이 있는 경우				
조치방법	Everyone 권한 제거				
보안설정방법					

■ Windows NT

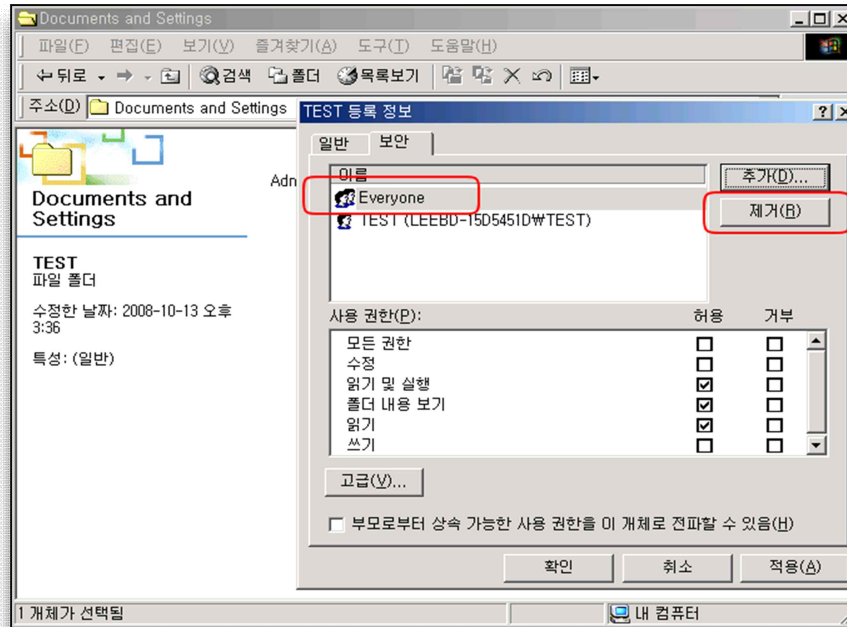
1. Windows NT: C:\WinNT\Profiles\사용자 홈 디렉터리> 등록 정보> 보안
2. Everyone 권한 제거(All Users, Default User 디렉터리는 제외)



윈도우즈 서버

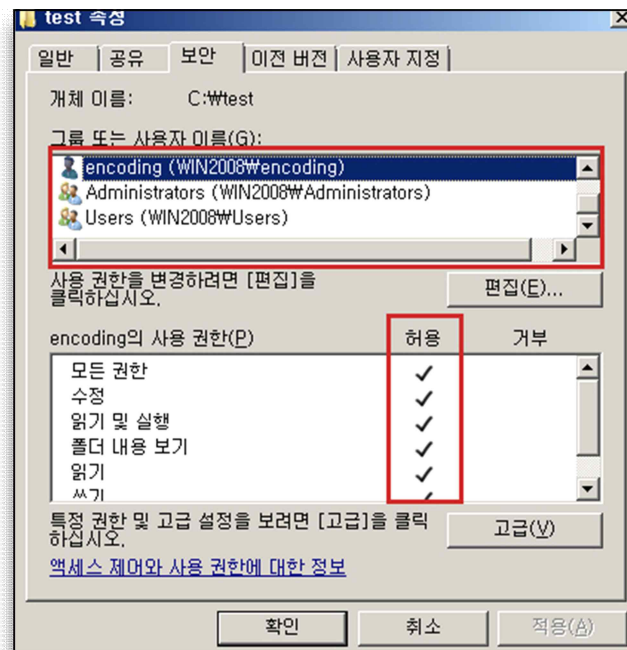
■ Windows 2000, 2003

1. C:\Documents and Settings\사용자 홈 디렉터리> 속성> 보안
2. Everyone 권한 제거(All Users, Default User 디렉터리는 제외)



■ Windows 2008

1. C:\Users\사용자\<사용자 계정>
2. 해당 사용자에게 대한 권한 외 일반 계정 삭제



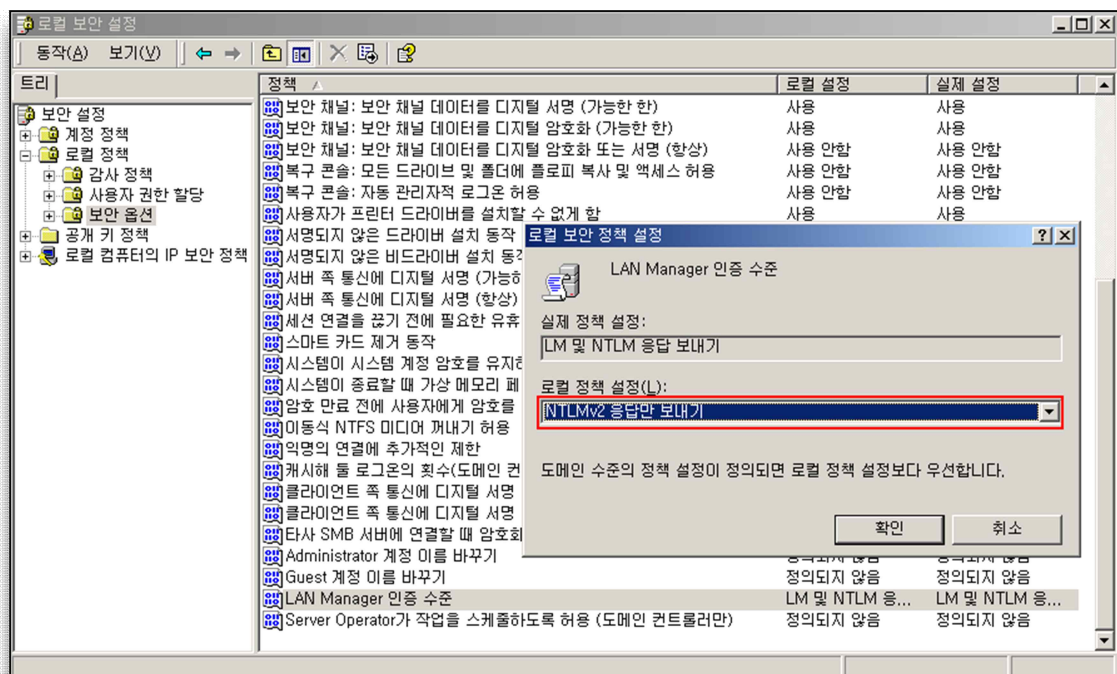
조치 시 영향 일반적으로 영향 없음

윈도우즈 서버

취약점 항목	5.16. LAN Manager 인증 수준				
대상 OS	NT, 2000, 2003, 2008	위험도	중	Code	W-77
취약점 개요	*Lan Manager 인증 수준 설정을 통해 네트워크 로그인에 사용할 Challenge/Response 인증 프로토콜을 결정하며, 이 설정은 클라이언트가 사용하는 인증 프로토콜 수준, 협상된 세션 보안 수준 및 서버가 사용하는 인증 수준에 영향을 주기 때문에 보다 안전한 인증을 위해 NTLMv2를 사용하는 것을 권장함. ※ NTLMv2는 Windows 2000, 2003, XP 이상에서 지원되며, Windows 98, NT 버전과 통신 할 경우 패치를 설치하여야 함. *LAN Manager는 네트워크를 통한 파일 및 프린터 공유 등과 같은 작업 시 인증을 담당함.				
보안대책					
판단기준	양호: "LAN Manager 인증 수준" 정책에 "NTLMv2 응답만 보냄"이 설정되어 있는 경우				
	취약: "LAN Manager 인증 수준" 정책에 "LM" 및 "NTLM"인증이 설정되어 있는 경우				
조치방법	Windows 2000: LAN Manager 인증 7수준 -> NTLMv2 응답만 보냄				
	Windows 2003: 네트워크 보안: LAN Manager 인증 수준 -> NTMLv2 응답만 보냄				
	Windows 2008: 네트워크 보안: LAN Manager 인증 수준 -> NTMLv2 응답만 보냄				
보안설정방법					

■ Windows NT, 2000

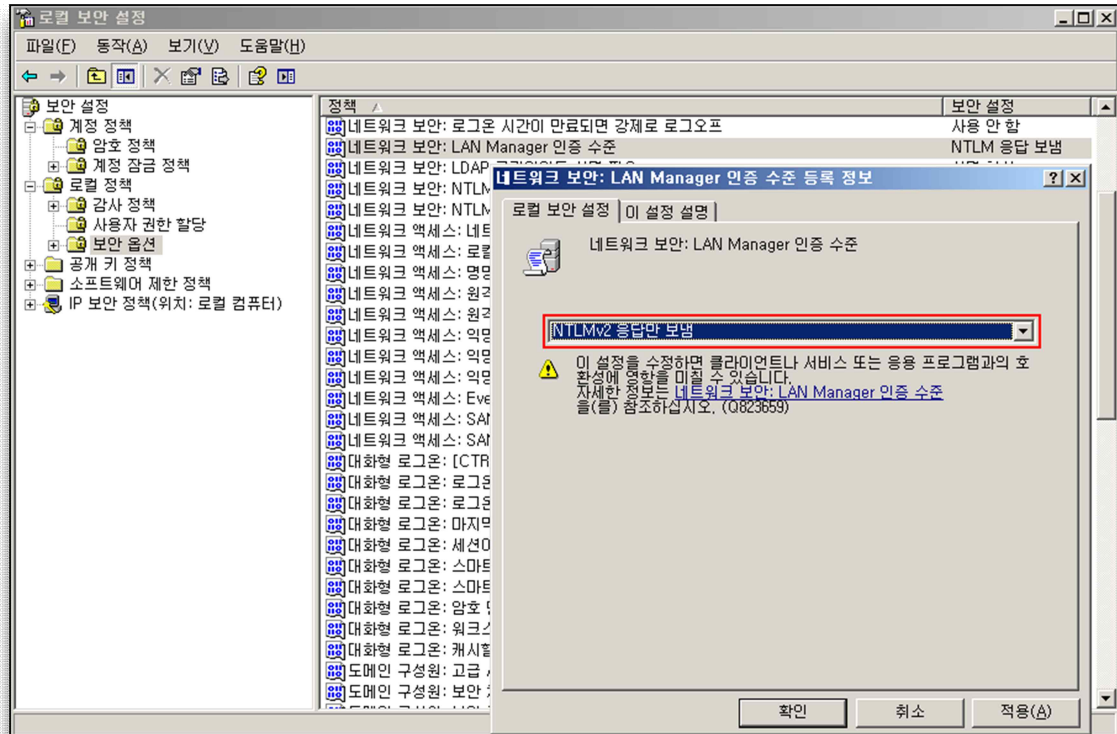
1. 시작> 실행> SECPOL.MSC> 로컬 정책> 보안 옵션
2. "LAN Manager 인증 수준" 정책에 "NTLMv2 응답만 보내기" 설정



윈도우즈 서버

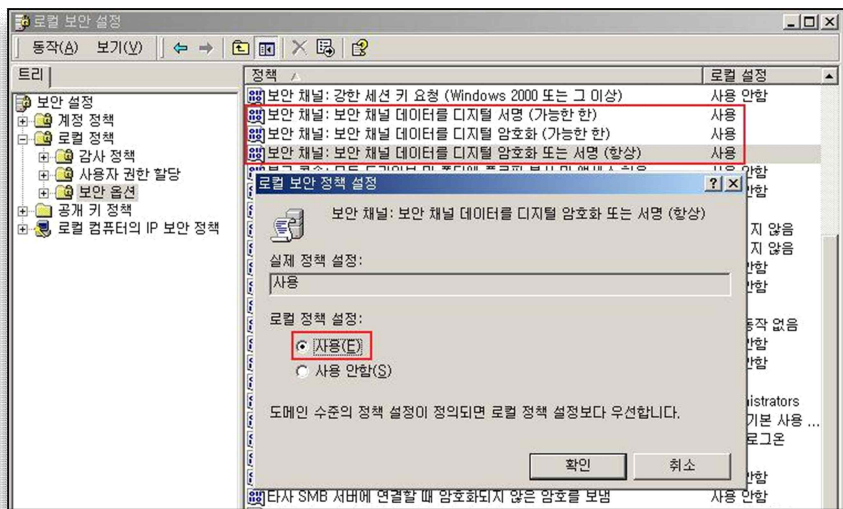
■ Windows 2003, 2008

1. 시작 > 실행 > SECPOL.MSC > 로컬 정책 > 보안 옵션
2. "네트워크 보안: LAN Manager 인증 수준" 정책에 NTLMv2 응답만 보냄" 설정



조치 시 영향	일반적으로 영향 없음
---------	-------------

윈도즈 서버

취약점 항목	5.17. 보안 채널 데이터 디지털 암호화 또는, 서명				
대상 OS	NT, 2000, 2003, 2008	위험도	중	Code	W-78
취약점 개요	보안 채널 데이터 디지털 암호화 또는, 서명 설정을 통해 도메인 구성원이 시작한 모든 보안 채널 트래픽이 최소 보안 요구 사항을 충족해야 하는지를 설정함. 특히 도메인 구성원에 의해 시작된 모든 보안 채널 트래픽의 서명과 암호화 여부를 설정함. 인증 트래픽 끼어들기 공격, 반복 공격 및 기타 유형의 네트워크 공격으로부터 보호하기 위해 Windows 기반에서는 NetLogon을 통해 보안 채널이라는 통신 채널을 만들어 컴퓨터 및 사용자 계정에 대한 인증을 함. 이 정책을 사용하면 모든 보안 채널의 서명 또는, 암호화가 협상되지 않는 한 보안 채널이 확립되지 않으며, 사용하지 않을 경우 모든 보안 채널 트래픽의 암호화 및 서명이 도메인 컨트롤러와 협상되고 서명 및 암호화 수준은 도메인 컨트롤러의 버전 및 다음 두 정책의 설정에 따라 좌우됨. (정책 사용 시 자동으로 활성화됨) • 도메인 구성원: 보안 채널 데이터를 디지털 암호화(가능하면) • 도메인 구성원: 보안 채널 데이터를 디지털 서명(가능하면)				
보안대책					
판단기준	양호: 아래 3가지 정책이 "사용"으로 되어 있는 경우 아래 3가지 정책이 "사용 안 함" 으로 되어 있는 경우 취약: • 도메인 구성원: 보안 채널 데이터를 디지털 암호화 또는, 서명(항상) • 도메인 구성원: 보안 채널 데이터를 디지털 암호화(가능한 경우) • 도메인 구성원: 보안 채널 데이터를 디지털 서명(가능한 경우)				
조치방법	보안 채널 데이터를 디지털 암호화·서명 관련 3개 정책 → 사용				
보안설정방법					
■ Windows NT, 2000					
1. 시작> 실행> SECPOL.MSC> 로컬 정책> 보안 옵션					
2. 위 3가지 정책을 모두 "사용"으로 설정					
					

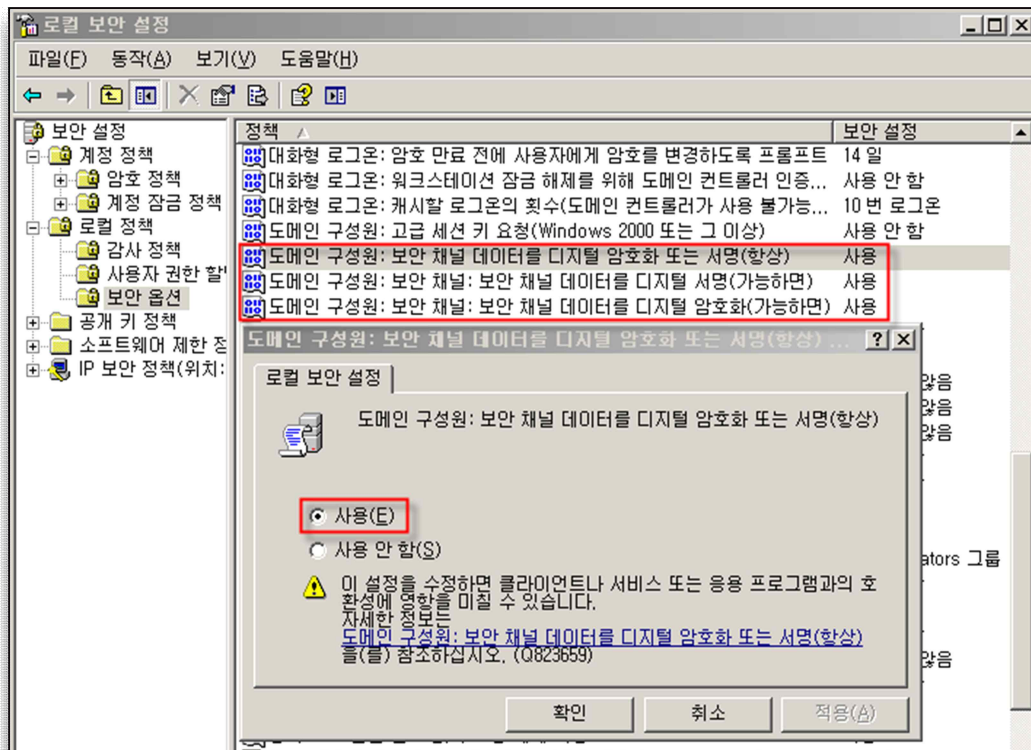
윈도우즈 서버

■ Windows 2003, 2008

1. 시작> 실행> SECPOL.MSC> 로컬 정책> 보안 옵션

2. 아래 3가지 정책을 모두 "사용" 으로 설정

- 도메인 구성원: 보안 채널 데이터를 디지털 암호화 또는 서명 (항상)
- 도메인 구성원: 보안 채널: 보안채널 데이터를 디지털 서명 (가능하면)
- 도메인 구성원: 보안 채널: 보안채널 데이터를 디지털 암호화 (가능하면)



조치 시 영향

도메인 구성원만 해당되며, Windows 98/NT와 파일 및 프린터 공유 등의 작업을 하지 않는 경우 일반적으로 영향 없음

윈도우즈 서버

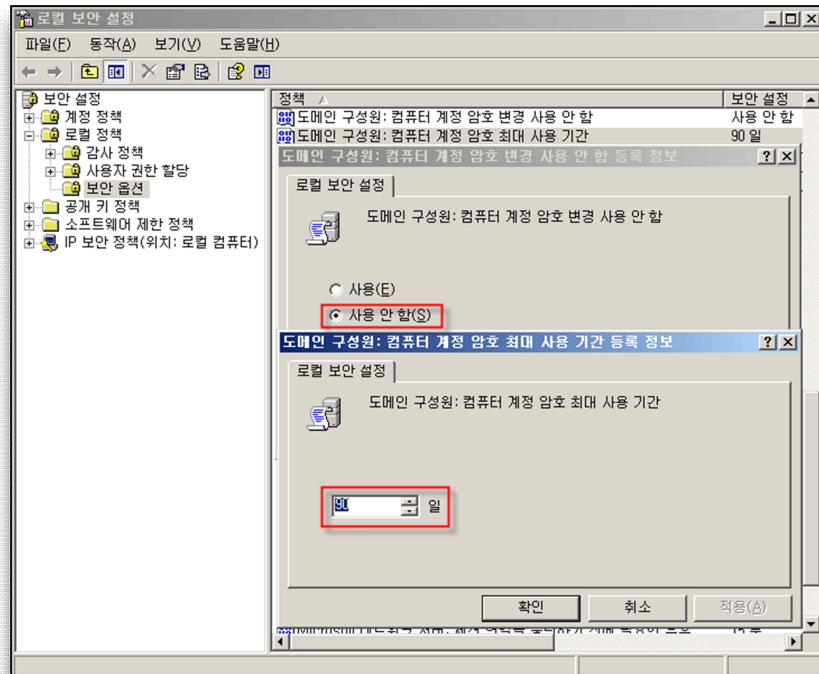
취약점 항목	5.18. 파일 및 디렉터리 보호				
대상 OS	NT, 2000, 2003, 2008	위험도	중	Code	W-79
취약점 개요	*NTFS 파일 시스템은 포맷 시 모든 파일과 디렉터리에 소유권과 사용 권한 설정이 가능하고 ACL(접근 통제 목록)을 제공함으로써 *FAT 파일 시스템에 비해 보다 강화된 보안 기능을 제공함.				
	기존에 FAT파일 시스템을 사용하다가 NTFS로 변환하기 위해서는 convert.exe 명령을 사용할 수 있지만 FAT파일 시스템으로 운영 중 변환해야 하는 경우 Default ACL이 적용되지 않으므로 가능한 초기 설치 시 NTFS 파일 시스템을 선택하는 것을 권장함.				
	*NTFS, FAT 파일 시스템 비교: FAT32에는 NTFS가 제공하는 보안 기능이 없으므로 컴퓨터에 FAT32 파티션 또는, 볼륨이 있는 경우 컴퓨터에 액세스 가능한 모든 사용자가 파일을 읽을 수 있으며 FAT32에는 크기 제한이 있음.				
보안대책					
판단기준	양호: NTFS 파일 시스템을 사용하는 경우				
	취약: FAT파일 시스템을 사용하는 경우				
조치방법	FAT파일 시스템을 사용하고 있다면, 가급적 NTFS 파일 시스템으로 변환				
보안설정방법					
■ Windows 2000, 2003, 2008					
명령어프롬프트(DOS창)에서 다음과 같이 입력.					
시작> 실행> CMD> convert 드라이브명: /fs:ntfs					
(예) convert F: /fs:ntfs라고 입력하면 F 드라이브는 NTFS 형식으로 포맷 됨					
조치 시 영향	파일시스템을 변환할 경우 기존 파일시스템에 영향을 줄 수 있음				

윈도우즈 서버

취약점 항목	5.19. 컴퓨터 계정 암호 최대 사용 기간				
대상 OS	2003, 2008	위험도	중	Code	W-80
취약점 개요	도메인 구성원이 해당 컴퓨터 계정 암호를 정기적으로 변경할지를 결정할 수 있으며, 기본적으로 도메인 구성원이 사용하는 도메인 암호 변경 기간은 '자동'으로 설정되어 있음. 이 설정을 활성화하는 경우 도메인 구성원은 해당 컴퓨터 계정 암호를 변경할 필요가 없고, 비활성화하는 경우 도메인 구성원은 컴퓨터 계정 암호 최대 사용 기간에 지정된 대로 컴퓨터 계정 암호를 변경하여야 함.				
보안대책					
판단기준	양호: "컴퓨터 계정 암호 변경 사용 안 함" 정책을 사용하지 않으며, "컴퓨터 계정 암호 최대 사용 기간" 정책이 "90일"로 설정되어 있는 경우				
	취약: "컴퓨터 계정 암호 변경 사용 안 함" 정책이 "사용"으로 설정되어 있거나 "컴퓨터 계정 암호 최대 사용 기간" 정책이 "90일"로 설정되어 있지 않은 경우				
조치방법	컴퓨터 계정 암호 변경 사용 → 사용 안 함 컴퓨터 계정 암호 최대 사용 기간 → 90일				
보안설정방법					

■ Windows 2003, 2008

1. 시작> 실행> SECPOL.MSC> 로컬 정책> 보안 옵션
2. 컴퓨터 계정 암호 변경 사용 → 사용 안 함
컴퓨터 계정 암호 최대 사용 기간 → 90일



※ Windows Server 2000 이하 버전 해당 사항 없음

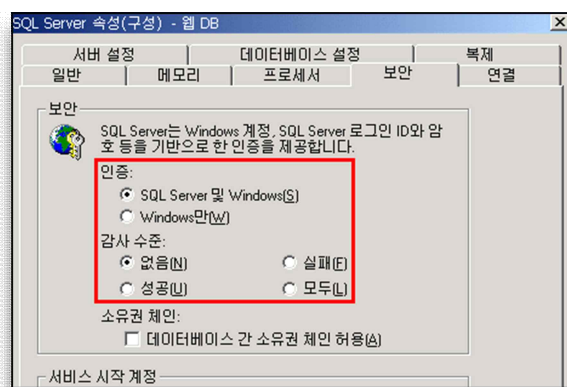
조치 시 영향	도메인 구성원만 해당되며 일반적으로 영향 없음
---------	---------------------------

윈도우즈 서버

취약점 항목	5.20. 시작프로그램 목록 분석				
대상 OS	2000, 2003, 2008	위험도	중	Code	W-81
취약점 개요	윈도우 부팅 시 너무 많은 시작프로그램이 동시에 실행되면 속도가 저하되는 문제가 발생하므로 불필요한 프로그램을 확인하고 삭제하거나 체크를 해제할 필요가 있음. 뿐만 아니라 공격자가 심어놓은 악성 프로그램이나 해킹 툴이 실행되어 시스템에 피해를 줄 수 있으므로 시작프로그램 목록을 수시로 검사하고 불필요하거나 의심스러운 프로그램은 제거하여야 함.				
보안대책					
판단기준	양호: 시작프로그램 목록을 정기적으로 검사하고 불필요한 서비스 체크해제를 한 경우.				
	취약: 시작프로그램 목록을 정기적으로 검사하지 않고, 부팅 시 불필요한 서비스도 실행되고 있는 경우				
조치방법	시작프로그램 목록의 정기적인 검사 실시 및 불필요한 서비스 비활성화				
보안설정방법					
■ Windows 2000, 2003, 2008 1. 시작> 검색> msconfig 명령어 입력 2. 시작 프로그램 탭 클릭> 시작 프로그램 목록 중 불필요하거나 의심스러운 항목 체크 표시 해제					
조치 시 영향	일반적으로 영향 없음				

윈도우즈 서버

6. DB 관리

취약점 항목		6.1. Windows 인증 모드 사용			
대상 OS	2003, 2008	위험도	중	Code	W-82
취약점 개요	데이터베이스 엔진 인증 모드에는 Windows 인증 모드와 SQL Sever가 있는 혼합 모드 두 가지 구성이 있음. Windows 인증 모드 선택 시 SQL Sever 인증을 위해서 설치 프로그램은 *sa라는 비활성화 된 계정을 생성하고, 이 계정은 혼합 모드를 사용함으로써 활성화 됨. sa 계정은 일반 사용자들에게 잘 알려진 만큼 쉽게 공격의 대상이 될 수 있으므로 꼭 필요하지 않는 경우 비활성화 하고, 만약 필요하다면 강력한 암호 체계를 사용하여야 함.				
	Windows 인증은 *kerberos 보안프로토콜을 사용하며, 강력한 암호정책을 적용하여 적합한 복잡성 수준을 유지함. 또한, 계정 잠금 및 암호만료를 지원하고 SQL 서버가 Windows에서 제공하는 자격증명을 신뢰한 트러스트 연결을 사용하기 때문에 Windows 인증 모드 사용을 권고함.				
*sa 계정: 데이터베이스 서버 설치 시 자동으로 생성되며 DB서버 관리자 계정을 뜻함. *kerberos 보안프로토콜: 개방된 컴퓨터 네트워크 내에서 서비스 요구를 인증하기 위한 보안 시스템.					
보안대책					
판단기준	양호: Windows 인증 모드를 사용하고 sa계정이 비활성화되어 있는 경우 sa계정 사용 시 강력한 암호정책을 설정한 경우				
	취약: 혼합 인증 모드를 사용하고, 활성화 된 sa 계정에 대해 강력한 암호정책 설정을 하지 않은 경우				
조치방법	Windows 인증 모드 사용				
보안설정방법					
Windows만 인증 활성화 < SQL Server 2005 > 1. 우클릭> 서버> 등록 정보> 보안 탭> 인증> 인증 모드> Windows만[W]를 클릭하여 활성화시킴					
					
조치 시 영향	일반적으로 영향 없음				

보안장비 보안가이드라인

2014. 01



안전행정부 *희망의 새시대*

보안장비 취약점 분석·평가 항목

분류	점검항목	항목 중요도	항목코드
1. 계정관리	보안장비 Default 계정 변경	상	S-1
	보안장비 Default 패스워드 변경	상	S-2
	보안장비 계정별 권한 설정	상	S-3
	보안장비 계정 관리	상	S-4
	로그인 실패횟수 제한	중	S-5
2. 접근관리	보안장비 원격 관리 접근 통제	상	S-6
	보안장비 보안 접속	상	S-7
	Session timeout 설정	상	S-8
3. 패치관리	벤더에서 제공하는 최신 업데이트 적용	상	S-9
	보안장비 로그 설정	중	S-10
4. 로그관리	보안장비 로그 정기적 검토	중	S-11
	보안장비 로그 보관	중	S-12
	보안장비 정책 백업 설정	중	S-13
	원격 로그 서버 사용	중	S-14
	로그 서버 설정 관리	하	S-15
	NTP 서버 연동	중	S-16
5. 기능관리	정책 관리	상	S-17
	NAT 설정	상	S-18
	DMZ 설정	상	S-19
	최소한의 서비스만 제공	상	S-20
	이상징후 탐지 경고 기능 설정	상	S-21
	장비 사용량 검토	상	S-22
	SNMP 서비스 확인	상	S-23
	SNMP community string 복잡성 설정	상	S-24
	부가 기능 설정	중	S-25
	유해 트래픽 차단 정책 설정	중	S-26

보안장비

1. 계정 관리

취약점 항목	1.1. 보안장비 Default 계정 변경												
대상	방화벽, IPS, VPN	위험도	상	Code	S-01								
취약점 개요	디폴트 로그인 계정은 장비 제조업체에서 출고 시 설정되어 나오는 기본 계정정보를 의미함. 각 제조사의 장비별 디폴트 계정 리스트는 인터넷 등을 통해 쉽게 구할 수 있으며 악의적인 사용자가 이러한 디폴트 계정을 이용하여 불법적으로 방화벽 장비에 접근할 수 있고 시스템 침입 경로를 제공하는 등 일반적인 정보시스템 침해사고보다 심각한 피해를 초래할 수 있음.												
보안대책													
판단기준	양호: 장비에서 제공하고 있는 디폴트 계정명을 변경하여 사용하는 경우 (ID 변경이 불가능 할 경우 패스워드로 보완 필요)												
	취약: 장비에서 제공하고 있는 디폴트 계정명을 변경하지 않고 사용하는 경우												
조치방법	디폴트 계정명 변경												
보안설정방법													
점검방법													
1. Web을 통한 접속 2. 디폴트 계정, 비밀번호 입력 3. 접속확인													
이름: 암호: 로그인													
위에 제시한 설정이 적용되지 않은 경우 아래의 보안설정방법에 따라 설정을 변경함													
■ 조치방법													
1. 보안장비에서 제공하고 있는 계정 메뉴에서 ID 변경 2. ID 변경이 불가능 할 경우 패스워드로 보완 필요													
관리자 접근 프로파일 새로생성 <table><tr><td>이름</td><td>내부(망) 호스트 IP</td><td>허가</td><td></td></tr><tr><td>admin</td><td>0.0.0.0/0, 0.0.0.0/0, 127.0.0.1/32</td><td>prof_admin</td><td> </td></tr></table>						이름	내부(망) 호스트 IP	허가		admin	0.0.0.0/0, 0.0.0.0/0, 127.0.0.1/32	prof_admin	 
이름	내부(망) 호스트 IP	허가											
admin	0.0.0.0/0, 0.0.0.0/0, 127.0.0.1/32	prof_admin	 										
조치 시 영향	일반적인 경우 영향 없음												

보안장비

취약점 항목	1.2. 보안장비 Default 패스워드 변경				
대상	방화벽, IPS, VPN	위험도	상	Code	S-02
취약점 개요	디폴트 로그인 패스워드는 장비 제조업체에서 출고 시 설정되어 나오는 기본 로그인 패스워드 정보를 의미함. 각 제조사의 장비별 디폴트 로그인 패스워드 리스트는 인터넷 등을 통해 쉽게 구할 수 있으므로 악의적인 사용자가 이러한 디폴트 로그인 패스워드를 이용하여 불법적으로 방화벽 장비에 접근할 수 있고 시스템 침입 경로를 제공하는 등 일반적인 정보시스템 침해사고보다 심각한 피해를 초래할 수 있음.				
보안대책					
판단기준	양호: 장비 디폴트 패스워드 또는 유추 가능한 패스워드를 사용하지 않은 경우 (특수문자, 숫자, 영문 대소문자 포함 8자리이상)				
	취약: 장비 디폴트 패스워드 또는 유추 가능한 패스워드를 사용하는 경우				
조치방법	디폴트 패스워드를 특수문자, 숫자, 영문 대소문자 포함하여 8자리 이상으로 변경				
보안설정방법					
점검방법					
1. Web을 통한 접속 2. 디폴트 계정, 비밀번호 입력 3. 접속확인					
이름: 암호: 로그인					
위에 제시한 설정이 적용되지 않은 경우 아래의 보안설정방법에 따라 설정을 변경함					
■ 조치방법					
1. 패스워드 메뉴에서 패스워드 변경 2. 보안장비가 제공하는 범위에서 패스워드 설정 (특수문자, 숫자, 영소문자 포함 8자리이상)					
암호 수정: admin 새 암호 암호 확인 확인 취소					
조치 시 영향	일반적인 경우 영향 없음				

보안장비

취약점 항목		1.3. 보안장비 계정별 권한 설정															
대상	방화벽, IPS, VPN	위험도	상	Code	S-03												
취약점 개요	여러 사용자가 접속하여 사용하는 경우, 계정의 부적절한 권한 설정으로 인해 시스템의 침입 경로가 유출될 수 있음. 예를 들어 보안정책과 관련 없는 사용자에게 보안정책을 수정할 수 있는 권한이 부여된다면, 의도하지 않게 보안정책이 수정될 수 있으므로, 계정별 권한의 타당성을 확인해야 함.																
보안대책																	
판단기준	양호: 사용자별 계정의 용도 파악 및 적절한 권한을 부여하는 경우																
	취약: 사용자별 계정의 용도 파악 및 적절한 권한을 부여하지 않는 경우																
조치방법	사용자별 계정의 용도 파악 및 적절한 권한 부여																
보안설정방법																	
점검방법																	
보안장비에서 제공하고 있는 계정 메뉴에서 계정별 권한 확인																	
새로생성 <table><tr><td>이름</td><td>내부(망) 호스트 IP</td><td>허가</td><td></td></tr><tr><td>admin</td><td>0.0.0.0/0, 0.0.0.0/0, 127.0.0.1/32</td><td>prof_admin</td><td></td></tr><tr><td>test</td><td>0.0.0.0/0, 0.0.0.0/0, 127.0.0.1/32</td><td>prof_admin</td><td></td></tr></table>						이름	내부(망) 호스트 IP	허가		admin	0.0.0.0/0, 0.0.0.0/0, 127.0.0.1/32	prof_admin	  	test	0.0.0.0/0, 0.0.0.0/0, 127.0.0.1/32	prof_admin	  
이름	내부(망) 호스트 IP	허가															
admin	0.0.0.0/0, 0.0.0.0/0, 127.0.0.1/32	prof_admin	  														
test	0.0.0.0/0, 0.0.0.0/0, 127.0.0.1/32	prof_admin	  														
위에 제시한 설정이 적용되지 않은 경우 아래의 보안설정방법에 따라 설정을 변경함																	
■ 조치방법																	
1. 보안장비에서 제공하고 있는 계정 메뉴에서 새로운 계정 생성																	
2. 새로운 계정 담당자에 대한 역할 확인 후 권한 부여																	
방화벽 원격관리 관리자 추가 지정된 원격관리자 비밀번호 비밀번호 확인 내부(망) 호스트 IP #1 내부(망) 호스트 IP #2 내부(망) 호스트 IP #3 접근 프로파일 0.0.0.0/0.0.0.0 0.0.0.0/0.0.0.0 127.0.0.1/255.255.255.255 prof_admin 확인 취소																	
조치 시 영향	일반적인 경우 영향 없음																

보안장비

취약점 항목		1.4. 보안장비 계정 관리															
대상	방화벽, IPS, VPN	위험도	상	Code	S-04												
취약점 개요	계정 관리가 미흡한 경우 자신의 업무와 관련이 없는 애플리케이션 및 자원에 접속할 수 있기 때문에 보안사고의 위험이 증가함. 공용계정 및 휴면계정이 존재하는 시스템은 침해사고 및 장애 발생 시 사후 추적이 어려움. 공용 계정의 사용을 금지하고, 사용하지 않는 계정은 즉시 삭제하도록 계정 관리를 해야 함.																
보안대책																	
판단기준	양호: 불필요한 공용계정 및 휴면계정을 제거하거나 관리하는 경우																
	취약: 불필요한 공용계정 및 휴면계정을 제거하지 않고 관리하지 않는 경우																
조치방법	불필요한 공용계정 및 휴면계정 제거																
보안설정방법																	
점검방법																	
보안장비에서 제공하고 있는 계정 메뉴에서 계정 및 담당자 확인																	
새로생성 <table><tr><td>이름</td><td>내부(망) 호스트 IP</td><td>허가</td><td></td></tr><tr><td>admin</td><td>0.0.0.0/0, 0.0.0.0/0, 127.0.0.1/32</td><td>prof_admin</td><td></td></tr><tr><td>test</td><td>0.0.0.0/0, 0.0.0.0/0, 127.0.0.1/32</td><td>prof_admin</td><td></td></tr></table>						이름	내부(망) 호스트 IP	허가		admin	0.0.0.0/0, 0.0.0.0/0, 127.0.0.1/32	prof_admin	 	test	0.0.0.0/0, 0.0.0.0/0, 127.0.0.1/32	prof_admin	  
이름	내부(망) 호스트 IP	허가															
admin	0.0.0.0/0, 0.0.0.0/0, 127.0.0.1/32	prof_admin	 														
test	0.0.0.0/0, 0.0.0.0/0, 127.0.0.1/32	prof_admin	  														
위에 제시한 설정이 적용되지 않은 경우 아래의 보안설정방법에 따라 설정을 변경함																	
■ 조치방법																	
1. 시스템에 대해 1인 1계정 사용을 원칙으로 하고 공용으로 사용하는 계정 사용금지																	
2. 사용하지 않는 계정은 삭제하고 시스템 접근 이력을 관리하여 명시적인 계정 관리 설정																	
새로생성 <table><tr><td>이름</td><td>내부(망) 호스트 IP</td><td>허가</td><td></td></tr><tr><td>admin</td><td>0.0.0.0/0, 0.0.0.0/0, 127.0.0.1/32</td><td>prof_admin</td><td></td></tr><tr><td>test</td><td>0.0.0.0/0, 0.0.0.0/0, 127.0.0.1/32</td><td>prof_admin</td><td></td></tr></table>						이름	내부(망) 호스트 IP	허가		admin	0.0.0.0/0, 0.0.0.0/0, 127.0.0.1/32	prof_admin	 	test	0.0.0.0/0, 0.0.0.0/0, 127.0.0.1/32	prof_admin	  
이름	내부(망) 호스트 IP	허가															
admin	0.0.0.0/0, 0.0.0.0/0, 127.0.0.1/32	prof_admin	 														
test	0.0.0.0/0, 0.0.0.0/0, 127.0.0.1/32	prof_admin	  														
※ 시스템이 아닌 사람을 중심으로 하는 통합된 계정관리가 중요함																	
조치 시 영향	일반적인 경우 영향 없음																

보안장비

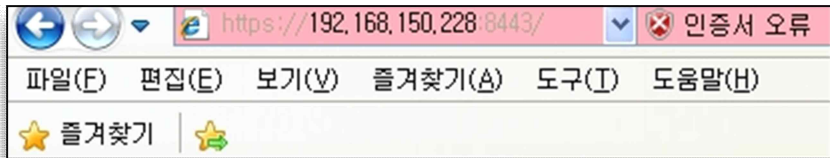
취약점 항목	1.5. 로그인 실패횟수 제한				
대상	방화벽, IPS, VPN	위험도	중	Code	S-05
취약점 개요	암호 공격에서는 자동화된 방법을 통해 모든 사용자 계정에 대해 수천 또는 수백만 개의 암호 조합을 시도하기 때문에 가능한 로그인 실패 수를 제한하여야 함.				
보안대책					
판단기준	양호: 로그인 실패 수를 5회 이하로 제한한 경우				
	취약: 로그인 실패 수를 5회 이하로 제한하지 않은 경우				
조치방법	로그온 실패 수를 5회 이하로 제한				
보안설정방법					
점검방법					
보안장비에서 제공하고 있는 계정 메뉴에서 로그인 임계값 확인					
위에 제시한 설정이 적용되지 않은 경우 아래의 보안설정방법에 따라 설정을 변경함					
■ 조치방법					
보안장비에서 제공하고 있는 계정 메뉴에서 Lockout 기능 설정					
Account User ID 100 ☐ Super user ☐ ☐ Expires on 15 Sep 2010 Last bad logon Last logon Bad logons Reset bad logon count ☐ ☒ Lockout 5					
조치 시 영향	일반적인 경우 영향 없음				

보안장비

2. 접근 관리

취약점 항목	2.1. 보안장비 원격 관리 접근 통제				
대상	방화벽, IPS, VPN	위험도	상	Code	S-06
취약점 개요	대부분 보안장비는 원격에서 관리하기 위한 관리자 접근방법을 제공하고 있어 이에 대한 통제가 필요함. 일반적으로 IP 단위로 접근제한을 하여 보안장비에 대한 관리자 접근을 통제함. 보안장비에서 제공하는 관리자 접근제한 기능을 통해 관리자 단말기 또는 콘솔 장비의 IP를 등록하고 접근을 제한할 수 있음.				
보안대책					
판단기준	양호: 원격 관리 시 관리자 IP만 접근 가능하도록 설정한 경우				
	취약: 원격 관리 시 관리자 IP만 접근 가능하도록 설정하지 않은 경우				
조치방법	원격 관리 시 관리자 및 특정 IP만 접근 가능하도록 함				
보안설정방법					
점검방법					
보안장비에서 제공하고 있는 메뉴에서 접속 IP나 계정 제한 확인					
위에 제시한 설정이 적용되지 않은 경우 아래의 보안설정방법에 따라 설정을 변경함					
■ 조치방법					
특정 IP 및 계정에서만 접속할 수 있도록 설정					
 사용자 정보 추가 * 사용자 ID innerbus * 성명 innerbus * 비밀번호 * 레벨 보안 담당자 * 사용여부 YES * 비밀번호확인 * 접속 IP제한 NO 저장 목록					
조치 시 영향	일반적인 경우 영향 없음				

보안장비

취약점 항목		2.2. 보안장비 보안 접속			
대상	방화벽, IPS, VPN	위험도	상	Code	S-07
취약점 개요	암호화되지 않은 데이터 전송 시 *스니핑 등을 통한 정보유출 위험이 존재함. SSL 인증 등의 암호화 접속을 통해 장비에 접속하도록 설정해야 함.				
	스니핑(Sniffing) : 스니퍼(Sniffer)는 "컴퓨터 네트워크상에 흘러다니는 트래픽을 엿듣는 도청장치"라고 말할 수 있으며 "스니핑"이란 이러한 스니퍼를 이용하여 네트워크상의 데이터를 도청하는 행위를 말함.				
보안대책					
판단기준	양호: 보안장비 접속 시 암호화 통신을 하는 경우				
	취약: 보안장비 접속 시 암호화 통신을 하지 않는 경우				
조치방법	보안장비 접속 시, 가능하다면 SSL 등의 암호화 접속 활용				
보안설정방법					
점검방법 1. https를 통한 접속 확인  2. ssh를 통한 접속 확인					
위에 제시한 설정이 적용되지 않은 경우 아래의 보안설정방법에 따라 설정을 변경함					
■ 조치방법					
1. 보안장비 접속 시, 가능하다면 *SSL 등의 암호화 접속 활용(제품마다 상이하므로 벤더사에 문의)					
*SSL(Secure Socket Layer) : 인터넷상에서 정보를 암호화하여 송/수신하는 프로토콜. 현재 인터넷에서 널리 쓰이고 있는 WWW, FTP 등의 데이터를 암호화하여, 프라이버시에 관한 정보나 신용카드 번호, 기업 비밀 등을 안전하게 송/수신 할 수 있음.					
조치 시 영향	일반적인 경우 영향 없음				

보안장비

취약점 항목	2.3. Session timeout 설정				
대상	방화벽, IPS, VPN	위험도	상	Code	S-08
취약점 개요	외부에서의 서비스 사용자가 일정 시간 동안 통신이 없을 시 해당 세션을 종료시키는 것으로 각 TCP/UDP 등에 대하여 time out을 설정해야 함. 그로 인해 불필요한 session을 정리하고 보안을 강화할 수 있음.				
보안대책					
판단기준	양호: Session Timeout 시간을 설정한 경우				
	취약: Session Timeout 시간을 설정하지 않은 경우				
조치방법	Session Timeout 시간을 설정				
보안설정방법					
점검방법					
벤더별 설정 값 확인. 대부분의 보안장비는 디폴트로 되어 있음					
위에 제시한 설정이 적용되지 않은 경우 아래의 보안설정방법에 따라 설정을 변경함					
■ 조치방법					
보안장비가 제공하는 Timeout 기능 활성화 설정					
설정옵션 타임아웃설정 유휴시간 20 (1-480 분) 권한 부여 종료 15 (1-480 분)					
조치 시 영향	일반적인 경우 영향 없음				

보안장비

3. 패치 관리

취약점 항목		3.1. 벤더에서 제공하는 최신 업데이트 적용			
대상	방화벽, IPS, VPN	위험도	상	Code	S-09
취약점 개요	보안장비는 지속적으로 취약점이 알려지고 있으며 이에 대한 패치도 지속해서 제공되고 있으므로 보안장비의 보안수준을 높이고 성능 및 기능 향상을 위해서는 버전 업그레이드 및 보안 패치 작업을 수행하여 최신 취약점을 보완하는 작업이 필요함.				
보안대책					
판단기준	양호: 패치 적용 정책을 수립하여 주기적으로 패치를 관리하고 있을 경우				
	취약: 패치 적용 정책을 수립하여 주기적으로 패치를 관리하고 있지 않을 경우				
조치방법	장비 별 제공하는 최신 취약점 정보를 파악 후 최신 패치 및 업그레이드를 수행				
보안설정방법					
점검방법					
자동 업데이트 기능 설정 또는 벤더사에 문의하여 업데이트 수행					
위에 제시한 설정이 적용되지 않은 경우 아래의 보안설정방법에 따라 설정을 변경함					
■ 조치방법					
벤더사에 문의하여 자동 업데이트 기능 설정					
장비 정보 호스트 명 Fortigate-200 [변경] 펌웨어 버전 Fortigate-200 2.80,build489,051027 [갱신] FortiGuard - AV 패턴 6.123(10/26/2005 14:55) [갱신] FortiGuard - IPS 패턴 2.240(10/20/2005 17:01) [갱신]					
조치 시 영향	서비스의 영향을 고려하여 벤더사와 협의 후 적용				

보안장비

4. 로그 관리

취약점 항목		4.1. 보안장비 로그 설정				
대상	방화벽, IPS, VPN	위험도	중	Code	S-10	
취약점 개요	로그 정보를 사용함으로써 관리자는 보안장비의 작동과 손상 여부를 파악할 수 있으며 어떤 종류의 침입이나 공격이 진행되고 있는지 알 수 있음.					
보안대책						
판단기준	양호: 정책에 따른 로그설정이 되어 있는 경우					
	취약: 정책에 따른 로그 설정이 되어 있지 않은 경우					
조치방법	정책에 따른 로깅 설정					
보안설정방법						
점검방법						
보안장비의 로그 설정 메뉴 확인						

위에 제시한 설정이 적용되지 않은 경우 아래의 보안설정방법에 따라 설정을 변경함

■ 조치방법

1. 정책에 따른 로깅 설정
(각 벤더마다 설정방법이 상이)

	전체 선택	FortiLog 애플리케이션 설정	로깅 고정 디스크 설정	메모리 배분 설정	원격 시스템 로그 서버 설정	웹 트래픽 로그 서버 설정	경고 이메일
트래픽 로그	☐	☐	☐	☐	☐	☐	☐
정책에서 허용한 트래픽	☐	☐	☐	☐	☒	☒	☐
정책을 위반한 트래픽	☐	☐	☐	☐	☒	☒	☐
이벤트 로그	☐	☐	☐	☐	☒	☒	☐
시스템 활동 이벤트	☐	☐	☐	☐	☒	☒	☐
IPSec 터널 이벤트	☐	☐	☐	☐	☒	☒	☐
DHCP 서버 이벤트	☐	☐	☐	☐	☒	☒	☐
L2TP/PPTP/PPPoE 서버 이벤트	☐	☐	☐	☐	☒	☒	☐
Admin 이벤트	☐	☐	☐	☐	☒	☒	☐
인증화 활동 이벤트	☐	☐	☐	☐	☒	☒	☐
방화벽 인증 이벤트	☐	☐	☐	☐	☒	☒	☐
패턴 업데이트 이벤트	☐	☐	☐	☐	☒	☒	☐
바이러스 로그	☐	☐	☐	☐	☒	☒	☐
바이러스 감응	☐	☐	☐	☐	☒	☒	☐
파일명 차단	☐	☐	☐	☐	☒	☒	☐
응용소과 파일	☐	☐	☐	☐	☒	☒	☐
웹 필터 로그	☐	☐	☐	☐	☒	☒	☐
컨텐츠 차단	☐	☐	☐	☐	☒	☒	☐
URL 차단	☐	☐	☐	☐	☒	☒	☐
URL 차단 예외	☐	☐	☐	☐	☒	☒	☐
분류별 차단 빈도	☐	☐	☐	☐	☒	☒	☐
분류별 빈도 감시	☐	☐	☐	☐	☒	☒	☐
분류별 빈도 오류	☐	☐	☐	☐	☒	☒	☐

조치 시 영향	세부적인 로깅 설정은 보안장비 성능에 영향을 미칠 수 있음
---------	----------------------------------

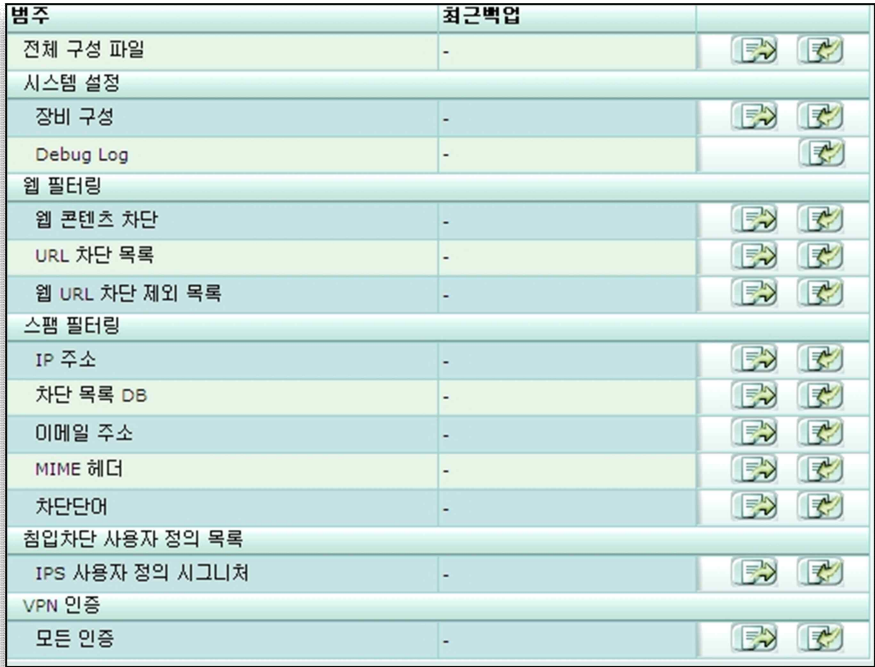
보안장비

취약점 항목	4.2. 보안장비 로그 정기적 검토				
대상	방화벽, IPS, VPN	위험도	중	Code	S-11
취약점 개요	로그를 정기적으로 조사해야 하는 것이 중요하며 로그를 정기적으로 검사함으로써, 해당 장비와 네트워크 상태의 동향을 파악할 수 있음. 정상적 운영상태 및 그 상태가 로그에 반영되어 있음을 확인함으로써 비정상적인 상태 또는 공격 상태를 식별할 수 있음.				
보안대책					
판단기준	양호: 로그 수집이 설정되어 있고, 분석이 정기적으로 되고 있는 경우				
	취약: 로그 수집이 설정되어 있지 않고, 분석이 되고 있지 않는 경우				
조치방법	보안장비 로그를 정기적으로 분석하여 보관				
보안설정방법					
점검방법					
보안장비 로그를 정기적으로 분석하여 보관하는지 확인					
위에 제시한 정책이 수립되지 않은 경우 아래의 조치방법에 따라 로그 수집 절차 실행					
■ 조치방법					
1. 로그 수집 설정					
2. 로그 분석 도구를 사용하여 결과 생성 및 리포트 제공					
(로그를 수집하여 수작업으로 분석하는 것은 시간과 인적으로 무리가 있으므로 자동 로그 분석 도구를 사용)					
조치 시 영향	일반적인 경우 영향 없음				

보안장비

취약점 항목	4.3. 보안장비 로그 보관				
대상	방화벽, IPS, VPN	위험도	중	Code	S-12
취약점 개요	보안장비 로그를 법규 기준에 따라 보관하고, 효율적이고 경제적으로 저장 관리하는 정책을 수립하지 않으면, 추후 필요한 용도에 따라 제출 할 수 없게 됨.				
보안대책					
판단기준	양호: 정책에 따라 로그 보관 설정이 되어 있는 경우				
	취약: 로그 보관 정책이 없고, 관리되고 있지 않는 경우				
조치방법	로그 기록 정책을 수립하고 정책에 따라 로깅 설정				
보안설정방법					
점검방법					
보관된 로그 날짜 확인					
로그가 법규 기준에 따라 보관 설정이 되지 않은 경우 아래의 보안설정방법에 따라 설정을 변경함					
■ 조치방법					
1. 보안장비 로그 보관 설정에서 로그 저장기간 확인 및 변경 (별도의 장비에 보관하고 있다면 로그 보관 정책에 맞춰 보관 설정)					
※ 각 벤더마다 설정방법 상이					
로그파일 백업 다이얼로그 백업 경로 /log/LCEBAKudp 예약 시간 11 매일 백업로그 유지기간 6 Months 분석데이터 유지기간 3 Months 로그 암호화 패스워드 ***** 저장 취소					
조치 시 영향	일반적인 경우 영향 없음				

보안장비

취약점 항목	4.4. 보안장비 정책 백업 설정				
대상	방화벽, IPS, VPN	위험도	중	Code	S-13
취약점 개요	보안장비의 정책은 조직의 요구에 맞게 작성되어 운영되어야 하며 이러한 정책들도 중요한 자산이 됨. 분실 시 조직의 서비스 운영에 큰 차질이 생길 수 있고 정책이 복잡하면 할수록, 새로운 정책을 수립 하는데 시간과 경제적인 손실이 늘어나게 됨.				
	보안대책				
판단기준	양호: 보안장비에 적용된 정책을 별도의 파일로 보관하고 있는 경우 취약: 보안장비에 적용된 정책을 별도의 파일로 보관하고 있지 않은 경우				
조치방법	보안장비에 적용된 정책을 별도의 파일로 보관				
	보안설정방법				
	점검방법 보안장비에 적용된 정책을 별도의 파일로 보관하는지 확인 위에 제시한 정책이 별도의 파일로 존재하지 않은 경우 아래의 조치방법에 따라 설정을 변경함				
	■ 조치방법 1. 보안장비 설정 메뉴에서 정책 백업 설정. 별도의 파일로 보관 ※ 각 벤더마다 설정방법 상이				
					
조치 시 영향	일반적인 경우 영향 없음				

보안장비

취약점 항목		4.6. 로그 서버 설정 관리			
대상	방화벽, IPS, VPN	위험도	하	Code	S-15
취약점 개요	*Syslog 서버는 모든 IP로부터 로그 메시지를 받아들이며 공격자는 syslog 서버에 저장된 로그 메시지를 변경하지는 못하지만 조작된 로그 메시지를 전송함으로써 관리자에게 혼란을 일으킬 수 있음. 또한, syslog 서버의 디스크를 모두 조작된 로그로 채움으로써 정상적으로 발생한 로그가 저장될 수 없도록 할 수 있음. 따라서 외부의 IP 주소를 가진 시스템으로부터 로그를 받아들이지 않도록 syslog 서버를 설정하여야 함. 이를 위해서는 보더 라우터의 외부로부터 syslog 패킷(UDP 포트 514)이 유입될 수 없도록 ACL을 적용함.				
	Syslog : Syslog 란 로깅 메세지 프로그램의 표준이며 Syslog는 다양한 프로그램들이 생성하는 메세지들을 저장하고, 메세지들을 이용해서 다양한 분석 등이 가능하도록 로그 메세지들을 제공함.				
보안대책					
판단기준	양호: syslog 패킷이 유입될 수 없도록 ACL을 적용한 경우				
	취약: syslog 패킷이 유입될 수 없도록 ACL을 적용하지 않은 경우				
조치방법	syslog 서버에서 로그 수집 제한 기능 설정				
보안설정방법					
점검방법					
syslog 서버에서 syslog 수집 제한 설정 가능 확인					
위에 제시한 설정이 적용되지 않은 경우 아래의 보안설정방법에 따라 설정을 변경함					
■ 조치방법					
1. 보안장비에서 로그 유입 제한 기능 설정					
2. 네트워크 장비에서 수집 제한 설정					
특정 내부 네트워크에서의 syslog 전송만 허용할 경우 ACL을 적용하여 제어할 수 있음					
조치 시 영향	일반적인 경우 영향 없음				

보안장비

취약점 항목	4.7. NTP 서버 연동				
대상	방화벽, IPS, VPN	위험도	중	Code	S-16
취약점 개요	보안장비들의 시간을 동기화시키는 것은 매우 중요하며 NTP는 RFC958을 통하여 처음 등장하여 장비의 시간 동기화 프로토콜의 표준이 되었음. 만약 보안장비에 NTP와 같은 프로토콜이 적용되어 있지 않다면 로그파일 관리를 시간별로 일관되게 하지 못할 것이며 이는 네트워크 관리, accounting, 사고 분석 등을 수행하는 데 큰 단점으로 작용할 것임. 따라서 정확한 시간 관리는 안전한 보안을 유지하는 필수적인 조건이라 할 수 있음.				
보안대책					
판단기준	양호: NTP 서버 연동이 되어 있는 경우				
	취약: NTP 서버 연동이 되어 있지 않은 경우				
조치방법	보안장비 시간 설정에서 NTP 프로토콜 연동 확인 및 벤더사에 문의				
보안설정방법					
점검방법					
보안장비 시간 설정에서 NTP 프로토콜 연동 확인 및 벤더사에 문의					
위에 제시한 설정이 적용되지 않은 경우 아래의 보안설정방법에 따라 설정을 변경함					
■ 조치방법					
1. 보안장비 설정 메뉴에서 NTP 서버 연동 설정					
시간설정 표준시간 지역 설정 Thu Sep 16 01:30:51 2010 갱신 표준시간 지역 (GMT+9:00)Osaka,Sapporo,Tokyo,Seoul ☐ 썸머타임 ○ 설정시간 시 1 분 30 초 51 월 Sep 일 16 년 2010 ● NTP 서버와 동조 서버 203.248.240.140 동조 간격 60 (mins) 적용					
조치 시 영향	일반적인 경우 영향 없음				

보안장비

5. 기능 관리

취약점 항목		5.1. 정책 관리			
대상	방화벽, IPS	위험도	상	Code	S-17
취약점 개요	관리자마다 각기 다른 관리 방법을 적용한다면 보안장비의 정책은 다양한 버전이 존재하게 되고 관리자가 퇴사하거나 팀을 옮기게 될 경우, 이는 보안장비 정책 보안성에 심각한 문제를 발생할 수 있으므로 표준 절차와 지침이 필요함. 관리자에 따라서 개별적인 정책 관리 방법이 존재하지 않도록 표준적인 정책 관리와 지침이 필요함.				
보안대책					
판단기준	양호: 정책에 대한 주기적인 검사로 미사용 및 중복된 정책을 확인하여 제거하는 경우				
	취약: 정책에 대한 주기적인 검사를 하지 않고 미사용 및 중복된 정책을 확인하여 제거하지 않은 경우				
조치방법	정책에 대한 주기적인 검사로 미사용 및 중복된 정책을 확인하여 제거				
보안설정방법					
점검방법					
정책에 대한 주기적인 검사로 미사용 & 중복된 정책 확인					
위에 제시한 정책과 지침이 적용되지 않은 경우 아래의 조치방법에 따라 정책을 수립함					
■ 조치방법					
침입차단 시스템의 정책 관리 시, 객체관리는 관리자의 편의로 발생할 수 있는 오류를 최소화하기 위하여 기존 IP 대신에 관리자가 인식하기 쉬운 "객체명"을 사용함. "객체명"을 이용해서 관리자가 숫자(IP ADDRESS)의 오타나 서버의 착각을 최대한 방지할 수 있음.					
객체를 관리할 때 가장 중요한 것은 관리자가 직관적으로 인식할 수 있도록 명명하는 것이며, 다른 관리자들의 혼동을 최소화할 수 있는 "표준 명명 규약"이 있어야 함.					
객체 관리와 더불어 정책의 입력 시, 서로 연관성이 있는 서비스들은 비슷한 카테고리로 분류하여 정책 점검 시 검색이 쉬워야 하고 관리자마다 같은 정책 내의 세부 규칙을 여러 곳에 분산시키지 않도록 해야 함. 추가로 정책내의 세부 규칙에 대한 카테고리가 존재하는지, 그리고 관리자가 다르더라도 그 카테고리 내에서 정렬 규칙이 존재하는지 등에 대해서 "정책 명명 방식"의 차이가 최소화되도록 해야 함. 즉, 어떤 관리자가 정책을 변경하더라도 같은 방법으로 정책을 변경할 수 있는 정책 변경/관리 세부 지침이 존재해야 함.					
정책 입력 시, 정책이 침입차단시스템의 성능과의 관계를 고려하였는가에 대해서 점검해야 함. 일반적으로 가장 정책의 적용을 많이 받게 되는 공개 서비스군 카테고리가 정책의 최고 상단에 존재하고 그 다음으로 접근이 많은 서비스군 카테고리가 존재하는 것이 바람직함.					
조치 시 영향	일반적인 경우 영향 없음				

보안장비

취약점 항목	5.2. NAT 설정				
대상	방화벽	위험도	상	Code	S-18
취약점 개요	NAT를 사용하는 목적에는 2가지가 있는데, 첫째는 인터넷의 공인 IP주소를 절약할 수 있으며, 둘째는 공공 망과 연결되는 사용자들의 고유한 사설망을 침입자들로부터 보호할 수 있음. NAT 설정은 공개된 인터넷과 사설망 사이에 방화벽(Firewall)을 설치하여 외부 공격으로부터 사용자의 통신망을 보호하는 기본적인 수단으로 활용할 수 있음. 외부 침입자가 내부 시스템을 공격하기 위해서는 내부 사설 IP 주소를 알아야 하므로 NAT 설정으로 내부 네트워크를 보호할 수 있음.				
보안대책					
판단기준	양호: NAT 설정으로 내부 네트워크를 보호하는 경우				
	취약: NAT 설정을 하지 않은 경우				
조치방법	NAT 설정을 적용				
보안설정방법					
점검방법					
공인 IP 확인 사이트에 접속하여 확인					
위에 제시한 설정이 적용되지 않은 경우 아래의 보안설정방법에 따라 설정을 변경함					
■ 조치방법					
대부분의 네트워크 보안 제품들은 NAT 기술을 기본으로 채택하고 있음					
조치 시 영향	일반적인 경우 영향 없음				

보안장비

취약점 항목		5.3. DMZ 설정			
대상	방화벽	위험도	상	Code	S-19
취약점 개요	컴퓨터 보안에서의 비무장지대(Demilitarized zone, DMZ)는 조직의 내부 네트워크와 외부 네트워크 사이에 위치한 부분망임. 내부 네트워크와 외부 네트워크가 DMZ로 연결할 수 있도록 허용하면서도, DMZ 내의 컴퓨터는 오직 외부 네트워크에만 연결할 수 있도록 함. 즉 DMZ 안에 있는 호스트들은 내부 네트워크로 연결할 수 없는데, 이것은 DMZ에 있는 호스트들이 외부 네트워크로 서비스를 제공하면서 DMZ 호스트의 침입으로부터 내부 네트워크를 보호하기 위함임.				
보안대책					
판단기준	양호: DMZ를 구성하여 내부 네트워크를 보호하는 경우				
	취약: DMZ를 구성하지 않은 경우				
조치방법	DMZ를 구성하여 내부 네트워크를 보호				
보안설정방법					
점검방법					
네트워크 구성도 또는 방화벽 설정 확인					
위에 제시한 설정이 적용되지 않은 경우 아래의 보안설정방법에 따라 설정을 변경함					
■ 조치방법					
1. 방화벽의 설정 옵션					
각각의 네트워크는 방화벽에 서로 다른 포트를 사용하여 연결하는데 이를 삼각 방화벽 설정(three-legged firewall set-up)이라 함					
2. 두 개의 방화벽 사용					
DMZ는 두 개의 방화벽 중간에 위치하며, 두 개의 방화벽과 연결됨. 하나의 방화벽은 내부 네트워크와 연결되고 다른 하나는 외부 네트워크와 연결됨. 우연한 설정 실수를 통해 외부 네트워크가 내부 네트워크로 연결할 수 있게 되는 상황을 방지함. 이런 구성 형식을 차단된 서브넷 방화벽(screaned-subnet firewall)이라고 함					
조치 시 영향	일반적인 경우 영향 없음				

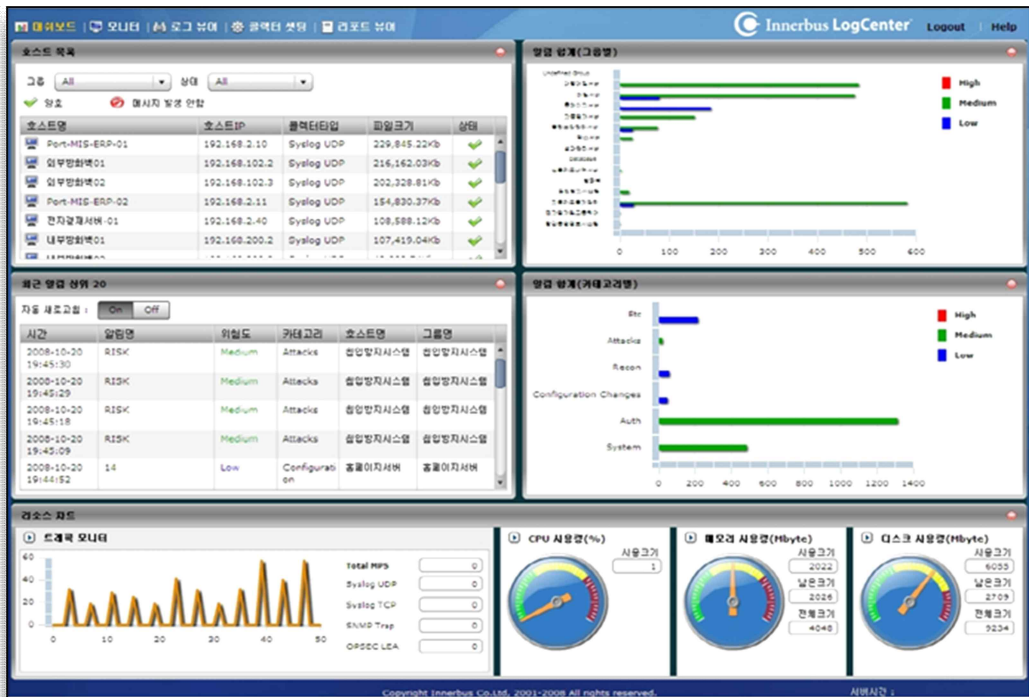
보안장비

취약점 항목	5.4. 최소한의 서비스만 제공				
대상	방화벽	위험도	상	Code	S-20
취약점 개요	방화벽은 기본적으로 all deny 설정임. 이와 더불어 허용할 포트와 IP만 추가함으로써, 관리 포인트도 적어지게 됨. 필요 없는 포트는 차단되어 침입자의 침입 가능성을 낮출 수 있음.				
	보안대책				
판단기준	양호: all deny 설정을 하고, 방화벽에 최소 서비스만 허용할 경우 취약: all deny 설정이 되어 있지 않거나, 방화벽에 불필요한 서비스를 허용할 경우				
조치방법	방화벽에 최소 서비스만 허용				
	보안설정방법				
	점검방법 방화벽에서 허용되지 않은 포트 접속 확인 위에 제시한 설정이 적용되지 않은 경우 아래의 보안설정방법에 따라 설정을 변경함 ■ 조치방법 방화벽 기본 정책인 all deny에 최소 서비스만 허용 확인 (허용된 IP와 서비스 포트만 오픈, IP 및 서비스 ANY 적용 금지) 				
조치 시 영향	허용되지 않은 접속은 모두 차단				

보안장비

취약점 항목	5.5. 이상징후 탐지 경고 기능 설정				
대상	방화벽, IPS	위험도	상	Code	S-21
취약점 개요	유해 트래픽은 정상적인 네트워크 운용 및 서비스에 지장을 주는 악의적인 공격성 패킷과 바이러스 패킷으로, 망 운영에 치명적인 장애를 유발하며 동시 다발적인 급속한 확산이 특징임. 유해 트래픽의 위험성은 지속적인 증가 추세이며 트래픽 관리는 망운용에 필수적인 요소로 부각되고 있음. 24시간 모니터링을 통한 감시가 여건상 어려울 경우 이메일이나 SMS를 통한 경고 기능 설정으로 대체함.				
보안대책					
판단기준	양호: 이상징후 탐지 시 관리자에게 이메일이나 SMS로 통보되는 경우				
	취약: 이상징후 탐지 시 관리자에게 이메일이나 SMS로 통보되지 않는 경우				
조치방법	이상징후 탐지 시 관리자에게 이메일이나 SMS로 통보				
보안설정방법					
점검방법					
보안장비의 실시간 알람, 이메일, SMS 경고 기능 설정 확인					
위에 제시한 설정이 적용되지 않은 경우 아래의 보안설정방법에 따라 설정을 변경함					
■ 조치방법					
24시간 모니터링을 통한 감시가 여건상 어려울 경우 이메일이나 SMS 을 통한 경고 기능 설정으로 대체					
경고 이메일 SMTP 서버: 192.168.100.3 이메일 발신: 수신: 인증: ☐ 활성화 SMTP 사용자 계정: 암호: 시험					
조치 시 영향	일반적인 경우 영향 없음				

보안장비

취약점 항목	5.6. 장비 사용량 검토				
대상	방화벽, IPS, VPN	위험도	상	Code	S-22
취약점 개요	장비 사용량에 대한 검토로 인해 네트워크 트래픽의 수준을 파악하게 되고, 그에 따른 가용성 향상을 고려해 볼 수 있음. 보안장비의 Web Dash Board를 모니터링함.				
보안대책					
판단기준	양호: 장비 사용량을 정기적으로 모니터링 및 검토할 경우				
	취약: 장비 사용량을 정기적으로 모니터링 및 검토하지 않을 경우				
조치방법	장비 사용량을 정기적으로 모니터링				
보안설정방법					
점검방법					
보안장비의 실시간 알람, 이메일, SMS 경고 기능 설정 확인					
위에 제시한 설정이 적용되지 않은 경우 아래의 조치방법을 수행함					
■ 조치방법					
보안장비의 Web Dash Board 모니터링					
					
조치 시 영향	일반적인 경우 영향 없음				

보안장비

취약점 항목		5.7. SNMP 서비스 확인																					
대상	방화벽, IPS, VPN	위험도	상	Code	S-23																		
취약점 개요	SNMP는 UDP 프로토콜을 사용하기 때문에 SNMP 서비스를 활성화하면 각종 공격, 예를 들어 DOS 공격에 취약해질 뿐만 아니라 보안장비의 성능저하, 크래쉬, 리로드 등의 위험이 존재함. 불필요하다면 SNMP 서비스를 중지하고, 관리를 위해 NMS 솔루션과의 연동이 필요하다면 Community String을 유추가 불가능하게 설정함.																						
보안대책																							
판단기준	양호: SNMP 서비스를 불필요하게 사용하지 않는 경우																						
	취약: SNMP 서비스를 불필요하게 사용할 경우																						
조치방법	불필요한 경우 SNMP 서비스 중지																						
보안설정방법																							
점검방법																							
보안장비의 SNMP 설정 메뉴에서 확인																							
위에 제시한 설정이 적용되지 않은 경우 아래의 보안설정방법에 따라 설정을 변경함																							
■ 조치방법																							
불필요하다면 SNMP 서비스를 중지하고, 관리를 위해 NMS 솔루션과의 연동이 필요하다면 SNMP 설정																							
SNMP Zone Default [11.4.9.107] ☒ SNMP 활성화 SNMP 커뮤니티 이름: Secu00 <table><thead><tr><th></th><th>호스트 IP 주소</th><th>커뮤니티 이름</th></tr></thead><tbody><tr><td>SNMP Trap1:</td><td>11.4.100.2</td><td>public</td></tr><tr><td>SNMP Trap2:</td><td>11.4.9.224</td><td>public</td></tr><tr><td>SNMP Trap3:</td><td></td><td></td></tr><tr><td>SNMP Trap4:</td><td></td><td></td></tr><tr><td>SNMP Trap5:</td><td></td><td></td></tr></tbody></table>							호스트 IP 주소	커뮤니티 이름	SNMP Trap1:	11.4.100.2	public	SNMP Trap2:	11.4.9.224	public	SNMP Trap3:			SNMP Trap4:			SNMP Trap5:		
	호스트 IP 주소	커뮤니티 이름																					
SNMP Trap1:	11.4.100.2	public																					
SNMP Trap2:	11.4.9.224	public																					
SNMP Trap3:																							
SNMP Trap4:																							
SNMP Trap5:																							
조치 시 영향	일반적인 경우 영향 없음																						

보안장비

취약점 항목	5.8. SNMP Community String 복잡성 설정																						
대상	방화벽, IPS, VPN	위험도	상	Code	S-24																		
취약점 개요	SNMP의 Public, Private과 같은 디폴트 Community String이 변경되지 않고 그대로 사용될 경우, 악의적인 사용자가 장비 설정을 쉽게 변경(RW)하여 중요 시스템 정보가 노출될 수 있는 위험이 존재함. 그러므로 추측하기 어려운 Community String 으로 변경하는 작업이 필요함.																						
보안대책																							
판단기준	양호: SNMP 서비스를 사용하지 않거나, 유추하기 어려운 community string을 설정한 경우																						
	취약: 디폴트 community string을 변경하지 않거나, 유추하기 쉬운 community string을 설정한 경우																						
조치방법	유추하기 어려운 community string을 설정																						
보안설정방법																							
점검방법																							
보안장비의 SNMP 설정 메뉴에서 커뮤니티 스트링 확인																							
위에 제시한 설정이 적용되지 않은 경우 아래의 보안설정방법에 따라 설정을 변경함																							
■ 조치방법																							
1. 네트워크 보안 장비는 SNMP로의 취약성이 존재하므로 누구나 추측하기 어렵고 의미가 없는 문자열, 영문자 혼합으로 변경 권고 (SNMP 버전은 v1, v2 ,v3 가 존재하는데 v1, v2 는 암호화가 되어 있지 않고 텍스트 열로 전송되지만 v3 가 암호화가 설정되어 있고 해쉬 값으로 전송한다.)																							
2. 보안장비의 SNMP 설정에서 커뮤니티 이름 변경																							
SNMP Zone Default [11.4.9.107] ☒ SNMP 활성화 SNMP 커뮤니티 이름: Secu09 <table><thead><tr><th></th><th>호스트 IP 주소</th><th>커뮤니티 이름</th></tr></thead><tbody><tr><td>SNMP Trap1 :</td><td>11.4.100.2</td><td>public</td></tr><tr><td>SNMP Trap2 :</td><td>11.4.9.224</td><td>public</td></tr><tr><td>SNMP Trap3 :</td><td></td><td></td></tr><tr><td>SNMP Trap4 :</td><td></td><td></td></tr><tr><td>SNMP Trap5 :</td><td></td><td></td></tr></tbody></table>							호스트 IP 주소	커뮤니티 이름	SNMP Trap1 :	11.4.100.2	public	SNMP Trap2 :	11.4.9.224	public	SNMP Trap3 :			SNMP Trap4 :			SNMP Trap5 :		
	호스트 IP 주소	커뮤니티 이름																					
SNMP Trap1 :	11.4.100.2	public																					
SNMP Trap2 :	11.4.9.224	public																					
SNMP Trap3 :																							
SNMP Trap4 :																							
SNMP Trap5 :																							
조치 시 영향	일반적인 경우 영향 없음																						

보안장비

취약점 항목		5.9. 부가 기능 설정													
대상	방화벽	위험도	중	Code	S-25										
취약점 개요	방화벽에서 제공하고 있는 기본 기능 이외의 부가기능 으로는 네트워크 주소변환 (Network Address Translation), 가상 사설망(VPN), 패킷 내용 검사, 감사 로그 기능 등이 있음. 부가기능을 사용하지 않는다고 운영에 큰 영향을 미치지 않지만, 사용 함으로써 도움을 줄 수 있음.														
보안대책															
판단기준	양호: 방화벽에서 제공하고 있는 부가기능을 사용하는 경우														
	취약: 방화벽에서 제공하고 있는 부가기능을 사용하지 않은 경우														
조치방법	방화벽에서 제공하고 있는 부가기능 사용														
보안설정방법															
점검방법															
보안장비에서 제공하는 부가기능 설정 확인															
위에 제시한 설정이 적용되지 않은 경우 아래의 보안설정방법에 따라 설정을 변경함															
■ 조치방법															
1. 벤더사에 문의하여 부가 기능 설정 시 발생하는 영향을 고려하여 적용															
단계 1 단계 2 수동 키 값 교환 Concentrator Ping 발생기 모 새로생성 <table><tr><td>게이트웨이 이름</td><td>게이트웨이 IP</td><td>모드</td><td>암호화 알고리즘</td><td></td></tr><tr><td>vpn_phase1</td><td>다이얼 업</td><td>Main 모드</td><td>DES-MD5</td><td></td></tr></table>						게이트웨이 이름	게이트웨이 IP	모드	암호화 알고리즘		vpn_phase1	다이얼 업	Main 모드	DES-MD5	
게이트웨이 이름	게이트웨이 IP	모드	암호화 알고리즘												
vpn_phase1	다이얼 업	Main 모드	DES-MD5												
조치 시 영향	부가기능 적용 시, 발생하는 영향 고려														

보안장비

취약점 항목		5.10. 유해 트래픽 차단 정책 설정																																	
대상	방화벽, IPS,	위험도	중	Code	S-26																														
취약점 개요	유해 트래픽은 정상적인 네트워크 운용 및 서비스에 지장을 주는 악의적인 공격성 패킷과 바이러스 패킷으로, 망 운영에 치명적인 장애를 유발하며 동시 다발적이고 급속한 확산이 특징임. 유해 트래픽의 위험성은 지속적인 증가 추세이며 트래픽 관리는 망운용에 필수적인 요소로 부각됨.																																		
보안대책																																			
판단기준	양호: 유해 트래픽 차단 정책이 설정 되어 있는 경우																																		
	취약: 유해 트래픽 차단 정책이 설정 되어 있지 않은 경우																																		
조치방법	유해 트래픽 차단 정책 설정																																		
보안설정방법																																			
점검방법																																			
침입차단시스템의 유해 트래픽 차단 기능 확인																																			
위에 제시한 설정이 적용되지 않은 경우 아래의 보안설정방법에 따라 설정을 변경함																																			
■ 조치방법																																			
침입차단시스템의 signature detection(알려진 것 탐지)와 anomaly detection(알려지지 않은 것들 탐지) 기능 설정																																			
IPS 시그네처 이상트래픽		<table><thead><tr><th>이름</th><th>활성</th></tr></thead><tbody><tr><td>▶ apache</td><td>✓</td></tr><tr><td>▶ backdoor</td><td>✓</td></tr><tr><td>▶ cgi</td><td>✓</td></tr><tr><td>▶ coldfusion</td><td>✓</td></tr><tr><td>▶ compromise</td><td>✓</td></tr><tr><td>▶ ddos</td><td>✓</td></tr><tr><td>▶ dns</td><td>✓</td></tr><tr><td>▶ dos</td><td>✓</td></tr><tr><td>▶ exploit</td><td>✓</td></tr><tr><td>▶ finger</td><td>✓</td></tr><tr><td>▶ frontpage</td><td>✓</td></tr><tr><td>▶ ftp</td><td>✓</td></tr><tr><td>▶ icmp</td><td>✓</td></tr><tr><td>▶ iis</td><td>✓</td></tr></tbody></table>				이름	활성	▶ apache	✓	▶ backdoor	✓	▶ cgi	✓	▶ coldfusion	✓	▶ compromise	✓	▶ ddos	✓	▶ dns	✓	▶ dos	✓	▶ exploit	✓	▶ finger	✓	▶ frontpage	✓	▶ ftp	✓	▶ icmp	✓	▶ iis	✓
이름	활성																																		
▶ apache	✓																																		
▶ backdoor	✓																																		
▶ cgi	✓																																		
▶ coldfusion	✓																																		
▶ compromise	✓																																		
▶ ddos	✓																																		
▶ dns	✓																																		
▶ dos	✓																																		
▶ exploit	✓																																		
▶ finger	✓																																		
▶ frontpage	✓																																		
▶ ftp	✓																																		
▶ icmp	✓																																		
▶ iis	✓																																		
조치 시 영향	오탐으로 인한 정상 트래픽 차단 가능성 있음																																		

네트워크장비 보안가이드라인

2014. 01



안전행정부 *희망의 새시대*

네트워크장비 취약점 분석·평가 항목

분류	점검항목	항목 중요도	항목코드
1. 계정관리	패스워드 설정	상	N-01
	패스워드 복잡성 설정	상	N-02
	암호화된 패스워드 사용	상	N-03
	사용자·명령어별 권한 수준 설정	중	N-04
2. 접근관리	VTY 접근(ACL) 설정	상	N-05
	Session Timeout 설정	상	N-06
	VTY 접속 시 안전한 프로토콜 사용	중	N-07
	불필요한 보조 입출력 포트 사용 금지	중	N-08
	로그온 시 경고 메시지 설정	중	N-09
3. 패치관리	최신 보안 패치 및 벤더 권고사항 적용	상	N-10
4. 기능관리	SNMP 서비스 확인	상	N-11
	SNMP community string 복잡성 설정	상	N-12
	SNMP ACL 설정	상	N-13
	SNMP 커뮤니티 권한 설정	상	N-14
	TFTP 서비스 차단	상	N-15
	Spoofing 방지 필터링 적용	상	N-16
	DDoS 공격 방어 설정	상	N-17
	사용하지 않는 인터페이스의 shutdown 설정	상	N-18
	TCP keepalive 서비스 설정	중	N-19
	Finger 서비스 차단	중	N-20
	웹 서비스 차단	중	N-21
	TCP/UDP small 서비스 차단	중	N-22
	Bootp 서비스 차단	중	N-23
	CDP 서비스 차단	중	N-24
	Directed-broadcast 차단	중	N-25
	Source 라우팅 차단	중	N-26
	Proxy ARP 차단	중	N-27
	ICMP unreachable, Redirect 차단	중	N-28
	identd 서비스 차단	중	N-29
	Domain lookup 차단	중	N-30
	pad 차단	중	N-31
	mask-rely 차단	중	N-32
	스위치 허브 보안 강화	하	N-33
5. 로그관리	원격 로그서버 사용	하	N-34
	로깅 버퍼 크기 설정	중	N-35
	정책에 따른 로깅 설정	중	N-36
	NTP 서버 연동	중	N-37
	timestamp 로그 설정	하	N-38

네트워크장비

1. 계정 관리

취약점 항목		1.1. 패스워드 설정			
대상	CISCO, Alteon, Passport, Juniper, Piolink	위험도	상	Code	N-01
취약점 개요	네트워크 장비의 초기 설정 패스워드를 변경하지 않고 사용하는 경우 비인가자의 불법적인 접근이 가능하며, 기본 패스워드는 인터넷상에서 검색을 통해 노출되어 있어 비인가자의 관리자 권한획득이 가능함. 네트워크 장비의 초기 설정 패스워드는 반드시 변경 설정하여야 함.				
보안대책					
판단기준	양호: 장비 접속 패스워드를 변경, 설정하여 사용하는 경우				
	취약: 장비 접속 패스워드가 설정되어 있지 않거나, 초기 설정 패스워드를 사용하는 경우				
조치방법	초기 설정 패스워드 변경 및 패스워드 설정				
보안설정방법					
대상 장비별 점검 방법					
CISCO	Router# show running-config Enable 패스워드 설정 확인, Line Access에서 각 라인별(VTY, CON, AUX) 패스워드 설정 확인				
Alteon, Passport	콘솔 및 Telnet으로 접근 시 각각 계정에 따라 설정 되어 있는 기본 패스워드 확인 예) Alteon Switch : admin/admin, admin/null				
Juniper	user@juniper> configure [edit] user@juniper# show root authentication 설정을 이용하여 [edit system] 레벨에서 패스워드 설정 확인				
Piolink	(configuration)# 에서 password 명령어를 통해 패스워드 설정 확인				

위에 제시한 설정이 적용되지 않은 경우 아래의 보안설정방법에 따라 설정을 변경함

■ CISCO

1. Enable 패스워드

Router# config terminal (단축 명령은 config t)

Enter configuration commands, one per line. End with CNTL/Z.

Router(config)# enable password <패스워드>

Router(config)# ^Z (Ctrl + z)

Router#

2. Virtual Terminal Password 설정

네트워크장비

```
Router# config terminal
Router(config)# line vty ?
<0-4> First Line number
Router(config)# line vty 0 4
Router(config-line)# login
Router(config-line)# password <패스워드>
```

3. 콘솔 패스워드 설정

```
Router# config terminal
Router(config)# line console ?
<0-0> First Line number
Router(config)# line console 0
Router(config-line)# login
Router(config-line)# password <패스워드>
```

4. 보조포트(AUX) 패스워드 설정

```
Router# config terminal
Router(config)# line aux ?
<0-0> First Line number
Router(config)# line aux 0
Router(config-line)# login
Router(config-line)# password <패스워드>
```

■ Alteon

1. # cfg/sys/access/user/admpw (administrator 패스워드 변경 시)
2. # apply
3. # save

■ Passport

[CLI]

1. switch 로 접속
 2. 다음 중 해당하는 계정에 따라 명령어 실행
- ```
config cli password ro <username>
config cli password l1 <username>
config cli password l2 <username>
config cli password l3 <username>
config cli password rw <username>
config cli password rwa <username>
config cli password slboper <username>
config cli password l4oper <username>
```

## 네트워크장비

```
config cli password oper <username>
config cli password slbadmin <username>
config cli password l4admin <username>
config cli password ssladmin <username>
```

### ■ Juniper

```
user@juniper> configure
[edit]
user@juniper# set system root-authentication plain-text-passwd

New password : 패스워드 <- 새로운 패스워드 입력
retype new password: : 패스워드 <- 입력했던 패스워드 확인
```

### ■ Piolink

1. Switch로 접속
2. root 계정으로 로그인
3. (configuration)# 에서 password 명령어 사용
4. new password: 입력
5. retype password: 입력

|                |               |
|----------------|---------------|
| <b>조치 시 영향</b> | 일반적인 경우 영향 없음 |
|----------------|---------------|

## 네트워크장비

| 취약점 항목       |                                                                                                                                                          | 1.2. 패스워드 복잡성 설정 |   |      |      |
|--------------|----------------------------------------------------------------------------------------------------------------------------------------------------------|------------------|---|------|------|
| 대상           | 공통                                                                                                                                                       | 위험도              | 상 | Code | N-02 |
| 취약점 개요       | 단순하거나 추측하기 쉬운 패스워드를 사용할 경우 악의적인 사용자가 쉽게 장비에 접속할 수 있으므로 암호 복잡성을 적용하여야 함. 패스워드 복잡성을 적용하지 않은 경우 공격자는 *무작위 대입 공격(Brute Force Attack)을 통하여 패스워드를 쉽게 획득할 수 있음. |                  |   |      |      |
|              | *무작위 대입 공격(Brute Force Attack): 컴퓨터로 암호를 해독하기 위해 가능한 모든 키를 하나하나 추론해 보는 시도를 말함.                                                                           |                  |   |      |      |
| 보안대책         |                                                                                                                                                          |                  |   |      |      |
| 판단기준         | 양호: 패스워드 정책이 수립되어 있으며, 보안 정책을 반영하여 설정되어 있는 경우                                                                                                            |                  |   |      |      |
|              | 취약: 초기 설정 패스워드를 사용하거나, 추측하기 쉬운 문자조합으로 이루어진 짧은 자릿수의 패스워드를 사용하는 경우                                                                                         |                  |   |      |      |
| 조치방법         | 해당 기관의 보안 정책에 적합하게 설정                                                                                                                                    |                  |   |      |      |
| 보안설정방법       |                                                                                                                                                          |                  |   |      |      |
| 대상 장비별 점검 방법 |                                                                                                                                                          |                  |   |      |      |
| 공통           | 장비별 담당자의 패스워드 복잡성 설정 적용 여부 확인                                                                                                                            |                  |   |      |      |

위에 제시한 설정이 적용되지 않은 경우 아래의 정책에 따라 패스워드 설정을 적용함

■ 공통

패스워드 설정 시 아래와 같은 패스워드 정책을 적용해야 함

1. 암호는 최소 8자 이상이어야 함 (Passport 9자 이상)

2. 사용자 계정 이름이나 이름의 문자를 3개 이상 연속하여 포함하지 않아야 함

3. 암호에는 다음 네 가지 중 세 가지 범주의 문자가 포함되어야 함

가. 대문자(26개))

나. 소문자(26개)

다. 숫자(10개)

가. 특수문자(32개)

※ 개인정보의 안전성 확보조치 기준 고시 및 해설서

• 최소 10자리 이상: 영대문자, 영소문자, 숫자 및 특수문자 중 2종류 이상으로 구성한 경우

• 최소 8자리 이상: 영대문자, 영소문자, 숫자 및 특수문자 중 3종류 이상으로 구성한 경우

|         |               |
|---------|---------------|
| 조치 시 영향 | 일반적인 경우 영향 없음 |
|---------|---------------|

## 네트워크장비

| 취약점 항목       |                                                                                                                                                | 1.3. 암호화된 패스워드 사용 |   |      |      |
|--------------|------------------------------------------------------------------------------------------------------------------------------------------------|-------------------|---|------|------|
| 대상           | CISCO, Passport, Juniper                                                                                                                       | 위험도               | 상 | Code | N-03 |
| 취약점 개요       | 네트워크 장비의 패스워드는 디폴트로 평문 텍스트 형태로 저장되기 때문에 설정파일 유출 시 패스워드도 함께 노출됨. 평문으로 저장 되어 있을시 해독될 가능성이 쉬워 정보에 대한 유출 위험이 있으므로 모든 패스워드를 암호화하여 저장하도록 설정을 변경해야 함. |                   |   |      |      |
| 보안대책         |                                                                                                                                                |                   |   |      |      |
| 판단기준         | 양호: 패스워드 암호화 설정이 적용된 경우                                                                                                                        |                   |   |      |      |
|              | 취약: 패스워드 암호화 설정이 적용되어 있지 않은 경우                                                                                                                 |                   |   |      |      |
| 조치방법         | 패스워드 암호화 설정 적용                                                                                                                                 |                   |   |      |      |
| 보안설정방법       |                                                                                                                                                |                   |   |      |      |
| 대상 장비별 점검 방법 |                                                                                                                                                |                   |   |      |      |
| CISCO        | Router# show running-config<br>1. Enable Secret 사용 확인<br>2. Password-Encryption 서비스 동작 확인                                                      |                   |   |      |      |
| Passport     | Configuration file에서 Enable Secret 패스워드를 제외한 모든 패스워드 암호화 설정 확인                                                                                 |                   |   |      |      |
| Juniper      | user@juniper>configure<br>[edit]<br>user@juniper#show<br><br>root authentication 설정을 이용하여 [edit system] 레벨에서 패스워드 암호화 설정 확인                    |                   |   |      |      |

위에 제시한 설정이 적용되지 않은 경우 아래의 보안설정방법에 따라 설정을 변경함

■ CISCO

Enable secret 패스워드는 암호화 되어 표시됨  
Enable secret 패스워드는 Enable password 보다 강력하고 우선적으로 사용함  
※ Enable 패스워드와 Enable secret 패스워드는 서로 다르게 입력

Router# config terminal  
Enter configuration commands, one per line. End with CNTL/Z.  
Router(config)# enable secret <패스워드>  
Router(config)# service password-encryption  
Router(config)# ^Z  
Router# show running

enable secret 5 \$1\$mERr\$9WCswBwUv6WeC6M8kNSs8

## 네트워크장비

```
enable password 7 0822455D0A1648121C0A0E082F
```

### ■ Passport

설정파일(Configuration file)에서 패스워드를 암호화함으로써 인증되지 않은 사용자가 설정파일의 패스워드를 획득할 수 있는 가능성을 방지함

### ■ Juniper

```
user@juniper> configure
```

```
[edit]
```

```
user@juniper# set system root-authentication encrypted-password "#1$14c5.%4Bopasddfs0"
```

```
user@juniper# ^Z
```

|                |               |
|----------------|---------------|
| <b>조치 시 영향</b> | 일반적인 경우 영향 없음 |
|----------------|---------------|

## 네트워크장비

| 취약점 항목       | 1.4. 사용자·명령어별 권한 수준 설정                                                                                                                 |     |   |      |      |
|--------------|----------------------------------------------------------------------------------------------------------------------------------------|-----|---|------|------|
| 대상           | CISCO, Alteon, Juniper, Piolink                                                                                                        | 위험도 | 중 | Code | N-04 |
| 취약점 개요       | 사용자·명령어별 권한 수준이 설정되어 있지 않은 경우 허가되지 않은 사용자가 중요한 프로그램을 실행하거나 모니터링 권한 설정을 변경하는 등의 위험이 발생할 수 있음. 사용자의 업무 및 권한에 따라 수행할 수 있는 권한과 기능을 제한해야 함. |     |   |      |      |
| 보안대책         |                                                                                                                                        |     |   |      |      |
| 판단기준         | 양호: 사용자·명령어별 레벨 설정이 되어있는 경우                                                                                                            |     |   |      |      |
|              | 취약: 사용자·명령어별 레벨 설정이 되어있지 않은 경우                                                                                                         |     |   |      |      |
| 조치방법         | 계정별 권한 설정과 중요 명령어에 대한 레벨 설정                                                                                                            |     |   |      |      |
|              | ※ 계정이 하나 존재하여 관리자만 접속하는 경우 (예: *NMS와 연동되지 않는 경우)는 적용하지 않음<br><br>*NMS(Network Management System): 네트워크 관리 시스템                          |     |   |      |      |
| 보안설정방법       |                                                                                                                                        |     |   |      |      |
| 대상 장비별 점검 방법 |                                                                                                                                        |     |   |      |      |
| CISCO        | Router# show privilege<br><br>사용자·명령어별 레벨 설정 확인                                                                                        |     |   |      |      |
| Alteon       | 사용자의 접근 레벨이 7단계로 나누어져 있는지 확인                                                                                                           |     |   |      |      |
| Juniper      | [edit system login]에서 superuser, read-only 클래스를 분리, 운영하는지 확인                                                                           |     |   |      |      |
| Piolink      | 슈퍼유저(root)와 일반유저로 권한을 부여하여 관리하는지 확인                                                                                                    |     |   |      |      |

위에 제시한 설정이 적용되지 않은 경우 아래의 보안설정방법에 따라 설정을 변경함

■ CISCO

시스코 IOS에서는 0에서 15까지 16개의 서로 다른 권한 수준을 규정하고 있으며, 레벨 1과 레벨 15는 기본적으로 정의되어 있음

사용자 EXEC 모드는 레벨 1에서 실행되며 privileged EXEC 모드는 레벨 15에서 실행되고, IOS 각 명령어는 레벨 1이나 레벨 15 중 어느 하나의 레벨이 사전에 기본적으로 지정되어 있음

레벨 1에서는 라우터의 설정 조회만 가능하고 레벨 15에서는 라우터의 전체 설정을 조회하고 변경할 수 있으므로 중요한 명령어의 권한 수준을 높여서 제한하는 것이 보안상 안전함

1. 사용자별 권한 수준 지정

Router# config terminal

Router(config)# username [ID] privilege [1-15] password [PASS]

2. 명령어별 권한 수준 지정

Router(config)# privilege exec level [1-15] [서비스명]

## 네트워크장비

※ 아래의 중요한 명령어에는 반드시 레벨 15를 적용해야 함  
connect, telnet, rlogin, show ip access-list, show logging

```
Router# config terminal
Router(config)# privilege exec level 15 connect
Router(config)# privilege exec level 15 telnet
Router(config)# privilege exec level 15 rlogin
Router(config)# privilege exec level 15 show ip access-list
Router(config)# privilege exec level 15 show logging
```

## ■ Alteon

사용자의 접근 및 권한 레벨은 7단계로 나누어져 있음

| 사용자 계정 / 기본 패스워드               | 설명                                                                                                                                                                               |
|--------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| User / User                    | User는 스위치 관리에 대한 직접적인 책임이 없지만 모든 스위치 상태 정보와 통계 자료를 볼 수 있음<br>그러나 스위치의 어떤 설정도 바꿀 수 없음                                                                                             |
| SLB Operator / slboper         | SLB Operator는 Web 서버들과 다른 인터넷 서비스의 로드를 관리함<br>부가적으로 모든 스위치 정보와 통계를 볼 수 있으며, Server Load Balancing 운영 메뉴를 사용하는 서버의 사용 가능/사용 불가능을 설정할 수 있음                                         |
| Layer4 Operator / l4oper       | Layer4 Operator는 공유된 인터넷 서비스들에 따른 라인의 트래픽을 관리함<br>SLB Operator와 같은 접근 레벨을 가지고 있고, 공유된 인터넷 서비스들에 따른 라인의 트래픽을 관리하는 운영자를 위한 운영적인 명령어에 접근할 수 있도록 제공하는 위해서 접근 레벨은 향후에 사용하기 위해 예약되어 있음 |
| Operator / oper                | Operator는 모든 스위치의 기능을 관리함<br>부가적으로 SLB Operator 기능과 포트나 전반적인 스위치를 재설정할 수 있음                                                                                                      |
| SLB Administrator / slbadmin   | SLB Administrator는 웹서버들과 다른 인터넷 서비스들과 그것에 대한 로드를 설정 및 관리를 할 수 있음<br>부가적으로 SLB Operator 기능들과 설정 필터들이나 대역폭 관리를 하는 것을 제외한 Server Load Balancing 메뉴에 매개변수를 설정할 수 있음                  |
| Layer4 Administrator / l4admin | Layer4 Administrator는 공유된 인터넷 서비스들에 따른 라인에 대한 트래픽을 설정 및 관리를 함                                                                                                                    |



## 네트워크장비

|                       |                                                                                                            |
|-----------------------|------------------------------------------------------------------------------------------------------------|
|                       | 부가적으로 SLB Administrator 기능들, 설정 필터들이나 대역폭 관리를 하는 것을 포함한 Server Load Balancing 메뉴에 모든 매개변수를 설정할 수 있음        |
| Administrator / admin | superuser Administrator는 user와 administrator 패스워드를 둘 다 변경할 수 있으며, Web 스위치에 모든 메뉴, 정보 그리고 설정 명령어들에 사용할 수 있음 |

1. switch로 접속
2. # cfg
3. # sys
4. 다음 중에 해당하는 경우를 선택  
# /user/명령어  
usrpw - user 암호 설정 및 변경  
sopw - SLB operator 암호 설정 및 변경  
l4opw - L4 operator 암호 설정 및 변경  
opw - operator 암호 설정 및 변경  
sapw - SLB administrator 암호 설정 및 변경  
l4apw - L4 administrator 암호 설정 및 변경  
admpw - administrator 암호 설정 및 변경
5. 암호 및 설정 변경
6. # apply
7. # save

### ■ Juniper

장비 구성 변경 시 사용하는 superuser 클래스와 monitoring 용으로 사용하는 read-only 클래스를 분리하여 사용할 것을 권장함. 장비 내 기본적으로 다음과 같은 클래스별 사용 권한 설정 및 세부 옵션 추가로 기능 제한을 할 수 있고, 특정 명령어 사용 제한을 계정마다 따로 설정할 수 있으므로 특정한 사용자 계정의 생성이 필요한 경우 사용 권한을 부여하여야 함

| Class-name   | Ability                            |
|--------------|------------------------------------|
| Operator     | clear, network, reset, trace, view |
| read-only    | view                               |
| Superuser    | all                                |
| unauthorized | None                               |

1. [edit system login] hierarchy level:
2. [edit system]  
login {

## 네트워크장비

```

class class-name {
 allow-commands "regular-expression";
 deny-commands "regular-expression";
 idle-timeout minutes;
 permissions [permissions];
}

```

### ■ Piolink

디폴트 계정인 슈퍼유저(root)와 관리목적에 따라 신규로 등록할 수 있는 일반유저, 2단계로 나누어져 있음. 슈퍼유저는 모든 권한이 부여되어 있으나 일반유저의 경우 장비의 설정을 변경할 수 있는 권한이 없음. 따라서 사용자의 업무 및 권한에 따라 계정을 부여하여 관리하는 것이 보안상 중요함.

#### 조치 시 영향

해당 명령어 실행 시 권한 부족으로 실행되지 않을 수 있음

## 네트워크장비

## 2. 접근 관리

| 취약점 항목           | 2.1. VTY 접근(ACL) 설정                                                                                                                                                                                                                                               |     |   |      |      |
|------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----|---|------|------|
| 대상               | CISCO, Alteon, Passport, Juniper                                                                                                                                                                                                                                  | 위험도 | 상 | Code | N-05 |
| 취약점 개요           | <p>VTY(Virtual Teletype) 사용 시 Telnet이나 SSH로 원격 접속이 가능함. 원격 접속 시 평문으로 정보가 전송되는 Telnet은 패스워드 추측 공격(Password Guessing) 및 *스니핑 공격에 취약하므로 보안상 SSH 사용을 권고함. 인가된 사용자만의 안전한 접근 관리를 위해 접속할 수 있는 IP를 제한하여 비인가자의 접근을 차단하여야 함.</p> <p>*스니핑(sniffing): 네트워크상의 데이터를 도청하는 행위</p> |     |   |      |      |
|                  | 보안대책                                                                                                                                                                                                                                                              |     |   |      |      |
| 판단기준             | <p><b>양호:</b> VTY 접근 시 접근 통제(ACL) 설정이 되어있는 경우</p> <p><b>취약:</b> VTY 접근 시 접근 통제(ACL) 설정이 되어있지 않는 경우</p>                                                                                                                                                            |     |   |      |      |
| 조치방법             | VTY(SSH 또는, Telnet) 사용 시 접근 통제(ACL) 설정                                                                                                                                                                                                                            |     |   |      |      |
|                  | 보안설정방법                                                                                                                                                                                                                                                            |     |   |      |      |
|                  | 대상 장비별 점검 방법                                                                                                                                                                                                                                                      |     |   |      |      |
| CISCO            | <p>Router# show running-config</p> <p>1. Access-List 설정 확인</p> <p>2. 각 Line Vty에 access-class 설정 확인</p>                                                                                                                                                           |     |   |      |      |
| Alteon, Passport | 장비로 접속하여 Telnet 또는 SSH 사용자의 접속 IP 설정 확인(Access Policies)                                                                                                                                                                                                          |     |   |      |      |
| Juniper          | <p>user@juniper# configure</p> <p>[edit]</p> <p>user@juniper# show</p> <p>root authentication 설정을 이용하여 [edit system] 레벨에서 ACL 설정 확인</p>                                                                                                                           |     |   |      |      |

위에 제시한 설정이 적용되지 않은 경우 아래의 보안설정방법에 따라 설정을 변경함

■ CISCO

1. VTY 접근 허용 IP 설정
 

```
Router# config terminal
Router(config)# access-list [1-99] {permit|deny} [Source Network] [WildcardMask]
Router(config)# access-list [1-99] permit any -> 기본 deny 방지
Router(config)# line vty 0 4
Router(config)# access-class [1-99] in
ex) 192.168.2.1 에서만 vty 접근 가능
Router(config)# access-list 1 permit 192.168.2.1
```
2. SSH 사용할 경우
 

```
Global configuration mode 로 접속
(config)# access-list <access_list_num> permit <source_ip mask>
```

## 네트워크장비

```
(config)#ssh access-group <num>
(config)#write memory
또는,
Global configuration mode 로 접속
(config)# ip ssh client <IP_address>
또는,
Global configuration mode 로 접속
(config)# ip ssh client <IP_address> <mac_address>
```

## ■ Alteon

1. switch 로 접속
2. # cfg
3. # sys
4. # access
5. # mgmt
6. # add <mgmt network address> <mgmt network mask> <management access protocol>
7. # apply
8. # save

## ■ Passport

1. switch 로 접속
2. # config sys access-policy
3. config/sys/access-policy# enable true
4. config/sys/access-policy# policy <pid> create
5. config/sys/access-policy# policy <pid>
6. config/sys/access-policy/policy/<pid># enable true
7. config/sys/access-policy/policy/<pid># accesslevel rwa
8. config/sys/access-policy/policy/<pid># host <ip-addr>
9. config/sys/access-policy/policy/<pid># service snmp enable
10. config/sys/access-policy/policy/<pid># service telnet enable

## ■ Juniper

ACL 로깅 설정

Access-list를 생성하면 기본 Deny가 되므로 네트워크 담당자를 통해 설정

```
user@juniper>configure
```

```
[edit]
```

```
user@juniper# source-address 127.0.0.0/24;
```

```
user@juniper# source-address 224.0.0.0/4;
```

```
user@juniper# source-address 0.0.0.0/0;
```

## 조치 시 영향

Access-list를 생성하면 기본 Deny가 되므로 네트워크 담당자를 통해 설정함

## 네트워크장비

| 취약점 항목       | 2.2. Session Timeout 설정                                                                                                                      |     |   |      |      |
|--------------|----------------------------------------------------------------------------------------------------------------------------------------------|-----|---|------|------|
| 대상           | CISCO, Alteon, Juniper, Piolink                                                                                                              | 위험도 | 상 | Code | N-06 |
| 취약점 개요       | 관리자가 네트워크 장비에 로그인 후 세션을 종료하지 않고 자리를 비우는 동안 악의적인 사용자가 접속된 터미널을 이용하여 불법적인 행위를 시도할 수 있음. 원격 접속 시 일정 시간 동안 키 입력이 없는 경우 연결된 접속을 자동 종료시키는 설정이 필요함. |     |   |      |      |
| 보안대책         |                                                                                                                                              |     |   |      |      |
| 판단기준         | 양호: Session Timeout 시간을 설정한 경우                                                                                                               |     |   |      |      |
|              | 취약: Session Timeout 시간을 설정하지 않은 경우                                                                                                           |     |   |      |      |
| 조치방법         | Session Timeout 설정 (5분 이하 권고)                                                                                                                |     |   |      |      |
| 보안설정방법       |                                                                                                                                              |     |   |      |      |
| 대상 장비별 점검 방법 |                                                                                                                                              |     |   |      |      |
| CISCO        | Router# show running-config<br><br>각 Line Access의 exec-timeout 설정 확인                                                                         |     |   |      |      |
| Alteon       | idle timeout in minutes 설정 확인                                                                                                                |     |   |      |      |
| Juniper      | user@juniper>configure<br>[edit]<br>user@juniper#show<br><br>root authentication 설정을 이용하여 [edit system] 레벨에서 Session Timeout 설정 확인           |     |   |      |      |
| Piolink      | terminal timeout 설정 확인                                                                                                                       |     |   |      |      |

위에 제시한 설정이 적용되지 않은 경우 아래의 보안설정방법에 따라 설정을 변경함

■ CISCO

1. Console  
Router# config terminal  
Router(config)# line con 0  
Router(config-line)# exec-timeout 5 0

2. VTY  
Router# config terminal  
Router(config)# line vty 0 4  
Router(config-line)# exec-timeout 5 0

3. AUX  
Router# config terminal

## 네트워크장비

```
Router(config)# line aux 0
Router(config-line)# exec-timeout 5 0
```

## ■ Alteon

1. # cfg
  2. # sys
  3. # idle <idle timeout in minutes, affects both console and telnet>
  4. # apply
  5. # save
- ※ 디폴트 : 5 분 설정

## ■ Juniper

```
user@juniper> configure
[edit]
user@juniper# set admin auth timeout 360
-----unknown keyword timeout
```

## ■ Piolink

1. 관리자 모드로 접속
  2. configure
  3. terminal timeout <interval>
- ※ 1분에서 60분 사이의 시간을 설정이 가능함

|                |               |
|----------------|---------------|
| <b>조치 시 영향</b> | 일반적인 경우 영향 없음 |
|----------------|---------------|

## 네트워크장비

| 취약점 항목 | 2.3. VTY 접속 시 안전한 프로토콜 사용                                                                                                                     |     |   |      |      |
|--------|-----------------------------------------------------------------------------------------------------------------------------------------------|-----|---|------|------|
| 대상     | CISCO, Alteon, Juniper                                                                                                                        | 위험도 | 중 | Code | N-07 |
| 취약점 개요 | VTY 접속 시 Telnet 프로토콜을 많이 사용하지만, Telnet은 패킷을 암호화하지 않은 텍스트 형태로 전송하므로 스니핑 공격에 의해 패스워드가 쉽게 노출되는 취약점이 존재함. 따라서 패킷 자체를 암호화하여 전송하는 SSH 프로토콜 사용을 권장함. |     |   |      |      |
| 보안대책   |                                                                                                                                               |     |   |      |      |
| 판단기준   | 양호: VTY 접속 시 SSH를 사용하는 경우                                                                                                                     |     |   |      |      |
|        | 취약: VTY 접속 시 Telnet을 사용하는 경우                                                                                                                  |     |   |      |      |
| 조치방법   | Telnet사용 제한, SSH사용 설정 변경                                                                                                                      |     |   |      |      |
| 보안설정방법 |                                                                                                                                               |     |   |      |      |

| 대상 장비별 점검 방법 |                                                                                                                                                                              |
|--------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| CISCO        | Router# show ip ssh<br>SSH Enabled – version 1.5<br>Authentication timeout: 120 secs; Authentication retries: 3 (활성화)<br>%SSH has not been enabled (비 활성화)<br><br>SSH 활성화 확인 |
| Alteon       | /sys/sshd에서 SSH 활성화 확인                                                                                                                                                       |
| Juniper      | user@juniper# set ssh<br><br>SSH 버전 확인                                                                                                                                       |

위에 제시한 설정이 적용되지 않은 경우 아래의 보안설정방법에 따라 설정을 변경함

## ■ CISCO

SSH 설정 방법

사전 작업 : 라우터명, 도메인명 설정

Router# config terminal

Router(config)# hostname <호스트명>

Router(config)# ip domain-name <도메인명>

Router(config)# username <ID> password <PASS>

Router(config)# crypto key generate rsa

!

How many bits in the modulus [512]: 1024 <- 입력

!

Router(config)# ip ssh time-out [초] <- timeout 시간(단위: second)

Router(config)# ip ssh authentication-retries [횟수] <- 재시도 횟수

Router(config)# line vty 0 4

Router(config-line)# login local

## 네트워크장비

```
Router(config-line)# transport input ssh
```

## SSH 접속

1. ssh 접속 프로그램 사용
2. # ssh -c rsa -l <ID> <라우터 IP>

## ■ Alteon

## SSH 설정 방법

1. switch 로 접속
2. # cfg
3. # /sys/sshd ena
4. # /sys/sshd on
5. # apply
6. # save

## ■ Juniper

1. SSH 버전 확인

```
user@juniper# set ssh
```

2. services로 검색하여 ssh를 사용하지 않을 경우 접속 가능 IP를 제한하여야 함

```
user@juniper> configure
```

```
[edit]
```

```
user@juniper# set ssh enable
```

## 조치 시 영향

일반적인 경우 영향 없음



## 네트워크장비

| 취약점 항목       | 2.4. 불필요한 보조 입·출력 포트 사용 금지                                                                                               |     |   |      |      |
|--------------|--------------------------------------------------------------------------------------------------------------------------|-----|---|------|------|
| 대상           | CISCO, Juniper                                                                                                           | 위험도 | 중 | Code | N-08 |
| 취약점 개요       | 불필요한 보조 입·출력 포트가 활성화되어 있으면 비인가자가 불법적인 접속을 시도할 수 있으므로 라우터나 스위치의 불필요한 포트를 차단하여 외부 접속으로 인한 내부 네트워크의 장애 발생과 데이터 손실을 예방하여야 함. |     |   |      |      |
| 보안대책         |                                                                                                                          |     |   |      |      |
| 판단기준         | 양호: 불필요한 보조 입·출력 포트 사용을 제한한 경우                                                                                           |     |   |      |      |
|              | 취약: 불필요한 보조 입·출력 포트 사용을 제한하지 않은 경우                                                                                       |     |   |      |      |
| 조치방법         | 포트 차단 및 허용 설정 확인                                                                                                         |     |   |      |      |
| 보안설정방법       |                                                                                                                          |     |   |      |      |
| 대상 장비별 점검 방법 |                                                                                                                          |     |   |      |      |
| CISCO        | Router# show running                                                                                                     |     |   |      |      |
|              | 불필요한 보조 입출력 포트의 오른쪽 끝부분에 Up (활성화)<br>불필요한 보조 입출력 포트의 오른쪽 끝부분에 Down (비활성화)                                                |     |   |      |      |
| Juniper      | user@juniper>configure<br>[edit]<br>user@juniper#show                                                                    |     |   |      |      |
|              | root authentication 설정을 이용하여 [edit system] 레벨에서 interface 차단 설정 확인                                                       |     |   |      |      |

위에 제시한 설정이 적용되지 않은 경우 아래의 보안설정방법에 따라 설정을 변경함

■ CISCO

1. AUX 포트 접속 차단

Router# config terminal

Router(config)# line aux 0

Router(config-line)# no password (어떤 사용자도 접속 금지)

Router(config-line)# transport input none (어떤 입력도 받지 않음)

Router(config-line)# no exec (어떤 명령도 실행 안 됨)

Router(config-line)# exec-timeout 0 1 (1 초 지나면 자동 타임아웃)

2. 해당 인터페이스 차단

Router# config terminal

Router(config)# int f0/1 (해당 포트 선택)

Router(config-line)# shutdown

■ Juniper

user@juniper> configure

[edit]

## 네트워크장비

```

user@juniper# editinterfacesso-1/0/3
[edit interfaces so-1/0/3]
user@juniper# setunit0familyinetaddress10.0.20.1/24
user@juniper# commit

```

|                |                                 |
|----------------|---------------------------------|
| <b>조치 시 영향</b> | 차단된 포트를 사용해야 할 경우 별도의 활성화 설정 필요 |
|----------------|---------------------------------|

## 네트워크장비

| 취약점 항목 | 2.5. 로그인 시 경고 메시지 설정                                                                                                                                      |     |   |      |      |
|--------|-----------------------------------------------------------------------------------------------------------------------------------------------------------|-----|---|------|------|
| 대상     | CISCO, Alteon, Juniper                                                                                                                                    | 위험도 | 중 | Code | N-09 |
| 취약점 개요 | 네트워크 장비에 로그인을 시도하는 사용자들에게 관리자는 시스템의 불법적인 사용에 대하여 경고 창을 띄움으로써 경각심을 줄 수 있음. 불필요한 정보를 제공하지 않으면서 모든 활동이 모니터링 되고 있음을 표시하고, 불법 또는, 악의적인 행동에 경고를 주는 메시지 설정이 필요함. |     |   |      |      |
| 보안대책   |                                                                                                                                                           |     |   |      |      |
| 판단기준   | 양호: 로그인 시 접근에 대한 경고 메시지를 설정한 경우                                                                                                                           |     |   |      |      |
|        | 취약: 로그인 시 접근에 대한 경고 메시지를 설정하지 않은 경우                                                                                                                       |     |   |      |      |
| 조치방법   | 네트워크 장비 접속 시 경고 메시지 설정                                                                                                                                    |     |   |      |      |

## 보안설정방법

| 대상 장비별 점검 방법 |                                                |
|--------------|------------------------------------------------|
| CISCO        | Router# show running-config<br>Banner 설정 내용 확인 |
| Alteon       | banner <string> 설정 내용 확인                       |
| Juniper      | edit system login 설정 내용 확인                     |

위에 제시한 설정이 적용되지 않은 경우 아래의 보안설정방법에 따라 설정을 변경함

### ■ CISCO

Router# config terminal

Enter configuration commands, one per line. End with CNTL/Z.

Router(config)# banner motd #

Enter TEXT message. End with the character '#'.  
<배너 문구 입력> #

Router(config)# banner login #

Enter TEXT message. End with the character '#'.  
<배너 문구 입력> #

Router(config)# banner exec #

Enter TEXT message. End with the character '#'.  
<배너 문구 입력> #

Router(config)#

※ 바람직한 배너 예시

This system have to access authorized user and only use for officially.

During using equipment, privacy of individuals is not guaranteed.

All access and usage is monitored and recorded and can be provided evidence as court or

## 네트워크장비

related organization.

Use of this system constitutes consent to monitoring for these purposes.

#### ■ Alteon

1. switch로 접속
2. # cfg
3. # sys
4. # banner <string>
5. # apply
6. # save

#### ■ Juniper

1. [edit system login]  
message text;

#### 조치 시 영향

일반적인 경우 영향 없음

## 네트워크장비

## 3. 패치 관리

| 취약점 항목       | 3.1. 최신 보안 패치 및 벤더 권고사항 적용                                                                                                      |     |   |      |      |
|--------------|---------------------------------------------------------------------------------------------------------------------------------|-----|---|------|------|
| 대상           | 공통                                                                                                                              | 위험도 | 상 | Code | N-10 |
| 취약점 개요       | 네트워크 장비의 보안 수준을 높이고 성능 및 기능 향상을 위해서는 버전 업그레이드 및 보안 패치 작업을 수행하여 취약점을 보완하는 작업이 필요함.                                               |     |   |      |      |
| 보안대책         |                                                                                                                                 |     |   |      |      |
| 판단기준         | 양호: 패치 적용 정책을 수립하여 주기적으로 패치를 관리하고 있을 경우                                                                                         |     |   |      |      |
|              | 취약: 패치 적용 정책을 수립하여 주기적으로 패치를 관리하고 있지 않을 경우                                                                                      |     |   |      |      |
| 조치방법         | 장비 별 제공하는 최신 취약점 정보를 파악 후 최신 패치 및 업그레이드를 수행                                                                                     |     |   |      |      |
| 보안설정방법       |                                                                                                                                 |     |   |      |      |
| 대상 장비별 점검 방법 |                                                                                                                                 |     |   |      |      |
| CISCO        | Router# show version<br><br>버전정보 확인                                                                                             |     |   |      |      |
| Juniper      | user@juniper> configure<br>[edit]<br>user@juniper# show version<br><br>root authentication 설정을 이용하여 [edit system] 레벨에서 패치 정보 확인 |     |   |      |      |

위에 제시한 버전 정보 확인 방법을 통해 최신 패치가 적용되지 않은 경우 아래의 방법에 따라 최신 패치 적용을 수행함

■ 공통

- 네트워크 장비는 지속해서 취약점이 발견되고 있으며, 이에 대한 패치도 계속 제공되고 있음
- 테스트와 수정을 통하여 검증 받은 패치를 사용하여야 하며, 이외 버전은 꼭 필요한 기능이 있는 경우만 사용함
- 최신 패치를 적용 하지 않을 경우 IP Option, TCP, IPv6, Header 패킷을 발송할 경우 서비스 거부 등의 피해가 발생할 수 있음

1. CISCO 버전별 정보

<http://www.cisco.com/web/about/security/intelligence/ios-ref.html>

2. Juniper 버전별 정보

<http://www.juniper.net/us/en/products-services/routing/>

※ Alteon 은 Redware 로 벤더가 변경됨

|         |                           |
|---------|---------------------------|
| 조치 시 영향 | 서비스 영향을 고려하여 벤더사와 협의 후 적용 |
|---------|---------------------------|

## 네트워크장비

## 4. 로그 관리

| 취약점 항목       | 4.1. 원격 로그서버 사용                                                                                                                                                                                  |     |   |      |      |
|--------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----|---|------|------|
| 대상           | CISCO, Alteon, Juniper, Piolink                                                                                                                                                                  | 위험도 | 하 | Code | N-11 |
| 취약점 개요       | 네트워크 장비의 관리, 보안 알람뿐만 아니라 일반적인 정보, 분석, *디버깅 메시지 등을 지정된 로그 서버로 보내어 실시간으로 로깅 및 관리하는 것이 운영상 필요함. 일반적으로 장비 내부 버퍼에 로그를 저장할 수 있으나 저장 공간이 한정되어 있고 악의적인 사용자에게 의해 변조될 위험이 존재하므로 별도의 외부 로그 서버로의 로그 저장이 필요함. |     |   |      |      |
|              | *디버깅(Debugging): 장치가 설비되어 사용하는 초기에 일어나기 쉬운 고장은 설계 실수, 공정의 결함 등에 의해서 발생함. 이 결함을 찾아내서 가급적 일어나지 않도록 감소시키려는 과정을 말함.                                                                                  |     |   |      |      |
| 보안대책         |                                                                                                                                                                                                  |     |   |      |      |
| 판단기준         | 양호: 별도의 로그 서버를 통해 로그를 관리하는 경우                                                                                                                                                                    |     |   |      |      |
|              | 취약: 별도의 로그 서버가 없는 경우                                                                                                                                                                             |     |   |      |      |
| 조치방법         | Syslog 등을 이용하여 로그 저장 설정                                                                                                                                                                          |     |   |      |      |
| 보안설정방법       |                                                                                                                                                                                                  |     |   |      |      |
| 대상 장비별 점검 방법 |                                                                                                                                                                                                  |     |   |      |      |
| CISCO        | Router# show running-config<br>Router# show logging<br><br>1. Logging 설정 확인<br>2. Log 정보 확인                                                                                                      |     |   |      |      |
| Alteon       | /syslog/host에서 syslog host 설정 확인                                                                                                                                                                 |     |   |      |      |
| Juniper      | user@juniper> configure<br>[edit]<br>user@juniper# show version<br><br>root authentication 설정을 이용하여 [edit system] 레벨에서 syslog 설정 확인                                                              |     |   |      |      |
| Piolink      | configure에서 logging 서버 설정 확인                                                                                                                                                                     |     |   |      |      |

위에 제시한 설정이 적용되지 않은 경우 아래의 보안설정방법에 따라 설정을 변경함

■ CISCO

라우터 로깅 설정

Router# config terminal

Router(config)# logging on (log 를 console 이외도 전달)

Router(config)# logging trap informational (severity level 설정)

Router(config)# logging 192.168.3.1 (syslog 서버)

Router(config)# logging facility local6 (syslog facility 설정)

## 네트워크장비

Router(config)# logging source-interface serial 0 (syslog interface)

### ■ Alteon

1. switch로 접속
2. # cfg
3. # sys
4. 다음과 같이 설정할 수 있음
- # /syslog/host: first syslog host의 IP 주소 설정
- # /syslog/host2: second syslog host의 IP 주소 설정
5. # apply
6. # save

### ■ Juniper

```
user@juniper> configure
edit
user@juniper# edit system syslog
[edit system syslog]
user@juniper# set archive files 5 sizes 5m world-readable
(files 5는 파일 수를 5개까지 표시하여 데이터를 사용하며, 5m은 최대 사이즈를 5m까지 허용하는 것을 뜻함)
```

### ■ Piolink

1. #logging server enable
2. #logging server <ip address> <event> <level>

#### 조치 시 영향

상세한 로깅 설정은 라우터 성능에 영향을 미칠 수 있음

## 네트워크장비

| 취약점 항목                                                                                                                                                               |                                                                                                                                                                                              | 4.2. 로깅 버퍼 크기 설정 |   |      |      |
|----------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------|---|------|------|
| 대상                                                                                                                                                                   | CISCO                                                                                                                                                                                        | 위험도              | 중 | Code | N-12 |
| 취약점 개요                                                                                                                                                               | 기본적으로 로그는 파일이 아닌 *버퍼 메모리에 저장되는데 메모리의 양을 초과하여 로그가 저장될 경우 로그 정보를 잃게 되어 침해사고 발생 시 침입 흔적을 알 수 없는 상황이 발생함. 저장되는 로그 데이터 용량을 고려하여 버퍼 크기를 설정하여야 함.                                                   |                  |   |      |      |
|                                                                                                                                                                      | *버퍼 메모리: 일반적으로 주기억 장치와 중앙 처리 장치 사이에 명령이나 데이터를 일시 유지하는데 사용되는 고속의 기억 장치. 버퍼 메모리는 주기억 장치보다 메모리 용량은 적지만 고속의 기억 소자를 사용함으로써 주기억 장치와 중앙 처리 사이의 정보의 흐름을 원활하게 함. 버퍼 메모리를 달리 로컬 메모리 혹은 캐시(cache)라고도 함. |                  |   |      |      |
| 보안대책                                                                                                                                                                 |                                                                                                                                                                                              |                  |   |      |      |
| 판단기준                                                                                                                                                                 | 양호: 저장되는 로그 데이터보다 버퍼 용량이 큰 경우                                                                                                                                                                |                  |   |      |      |
|                                                                                                                                                                      | 취약: 저장되는 로그 데이터보다 버퍼 용량이 작은 경우                                                                                                                                                               |                  |   |      |      |
| 조치방법                                                                                                                                                                 | 로그에 대한 정보를 확인하여 적절한 버퍼 크기 설정                                                                                                                                                                 |                  |   |      |      |
| 보안설정방법                                                                                                                                                               |                                                                                                                                                                                              |                  |   |      |      |
| 대상 장비별 점검 방법                                                                                                                                                         |                                                                                                                                                                                              |                  |   |      |      |
| CISCO                                                                                                                                                                | Router> enable<br>Router# show logging 로그에 대한 정보를 확인<br><br>메모리(RAM)에 저장된 로그는 'show logging'으로 확인할 수 있고, 'clear logging'을 실행하거나 RAM에 저장된 로그는 재부팅하면 사라지게 됨.                                   |                  |   |      |      |
| 위에 제시한 설정이 적용되지 않은 경우 아래의 보안설정방법에 따라 설정을 변경함                                                                                                                         |                                                                                                                                                                                              |                  |   |      |      |
| 최대 버퍼 크기는 65,500Kbyte 이며 버퍼 용량을 높게 설정하면 패킷 전달이 안 되는 경우가 발생함<br>일반적으로 16Kbyte 에서 32Kbyte 의 크기가 적당하며, 최대 용량이 16Kbyte 에 못 미치는 장비의 경우 장비 성능을 고려하여 최대 용량에 가깝게 설정하는 것을 권고함 |                                                                                                                                                                                              |                  |   |      |      |
| ■ Cisco                                                                                                                                                              |                                                                                                                                                                                              |                  |   |      |      |
| Router# config terminal                                                                                                                                              |                                                                                                                                                                                              |                  |   |      |      |
| Router(config)# logging on (로그를 메모리에 백업)                                                                                                                             |                                                                                                                                                                                              |                  |   |      |      |
| Router(config)# logging buffered 16000 (16KByte 할당)                                                                                                                  |                                                                                                                                                                                              |                  |   |      |      |
| Router(config)# logging buffered information (severity 레벨 설정)                                                                                                        |                                                                                                                                                                                              |                  |   |      |      |
| Router(config)# ^Z                                                                                                                                                   |                                                                                                                                                                                              |                  |   |      |      |
| 조치 시 영향                                                                                                                                                              | 버퍼 크기가 큰 경우 라이터 성능에 영향을 줌                                                                                                                                                                    |                  |   |      |      |



## 네트워크장비

| 취약점 항목       | 4.3. 정책에 따른 로깅 설정                                                                                                                                             |     |   |      |      |
|--------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------|-----|---|------|------|
| 대상           | CISCO, Juniper                                                                                                                                                | 위험도 | 중 | Code | N-13 |
| 취약점 개요       | 관리자는 로그 정보를 통해 장비의 상태와 서비스 정상 여부를 파악할 수 있으며 네트워크에 어떤 종류의 공격이나 침입이 진행되고 있는지 알 수 있음. 정책에 따른 로깅 설정을 통해 로그를 정기적으로 검사하고 정상적인 운영 상태 및 공격 유형을 식별하여 네트워크 동향을 파악하여야 함. |     |   |      |      |
| 보안대책         |                                                                                                                                                               |     |   |      |      |
| 판단기준         | 양호: 로그 기록 정책에 따라 로깅 설정이 되어있는 경우                                                                                                                               |     |   |      |      |
|              | 취약: 로그 기록 정책 미 수립 또는, 로깅 설정이 미흡한 경우                                                                                                                           |     |   |      |      |
| 조치방법         | 로그 기록 정책을 수립하고 정책에 따른 로깅 설정                                                                                                                                   |     |   |      |      |
| 보안설정방법       |                                                                                                                                                               |     |   |      |      |
| 대상 장비별 점검 방법 |                                                                                                                                                               |     |   |      |      |
| CISCO        | Router> enable<br>Router# show logging<br><br>로그에 대한 정보 확인                                                                                                    |     |   |      |      |
| Juniper      | user@juniper> configure<br>[edit]<br>user@juniper# show log messages<br><br>로그에 대한 정보 확인                                                                      |     |   |      |      |

위에 제시한 설정이 적용되지 않은 경우 아래의 보안설정방법에 따라 설정을 변경함

■ Cisco, Juniper

라우터에 기본적으로 설정된 로그 파일 설정을 변경하지 않으면 로깅을 효율적으로 사용할 수 없으므로 크게 6가지로 이루어진 아래의 방법을 활용하여야 함

1. 콘솔 로깅

콘솔 로그 메시지는 오직 콘솔 포트에서만 보이므로 이 로그를 보기 위해서는 반드시 콘솔 포트에 연결하여야 함

2. Buffered 로깅

Buffered 로깅은 로그를 라우터의 RAM에 저장하는데 이 버퍼가 가득 차게 되면 오래된 로그는 자동으로 새로운 로그에 의해 대체됨

3. Terminal 로깅

Terminal monitor 명령을 사용하여 로깅을 설정하면 라우터에서 발생하는 로그 메시지를

## 네트워크장비

VTY terminal에 보냄

#### 4. Syslog

시스코 라우터는 라우터의 로그 메시지가 외부의 syslog 서버에 저장되도록 설정할 수 있음

#### 5. SNMP traps

SNMP trap이 설정되면 SNMP는 특별한 상황을 외부의 SNMP 서버에 전송하도록 설정할 수 있음

#### 6. ACL 침입 로깅

표준 또는, 확장된 액세스 리스트를 설정할 때 특정한 룰에 매칭하였을 경우 해당 패킷 정보를 로그에 남기도록 설정할 수 있는데, 이는 액세스 리스트 룰의 끝에 로그나 로그 인풋을 추가하면 됨  
로그 인풋은 로그와는 달리 인터페이스 정보도 함께 남기게 되므로 어떤 인터페이스를 통해 로그가 남았는지를 알 수 있음

|                |               |
|----------------|---------------|
| <b>조치 시 영향</b> | 일반적인 경우 영향 없음 |
|----------------|---------------|

## 네트워크장비

| 취약점 항목       | 4.4. NTP 서버 연동                                                                                                                                                                                                            |     |   |      |      |
|--------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----|---|------|------|
| 대상           | CISCO, Alteon, Juniper                                                                                                                                                                                                    | 위험도 | 중 | Code | N-14 |
| 취약점 개요       | NTP(Network Time Protocol)는 로그의 통합 보관 시 시간의 동기화 등 정확하고 일관된 시간 관리를 위한 필수적인 조건이라 할 수 있음. 하지만 NTP가 사용하는 프로토콜은 보안 위협에 취약하므로 별도의 내부 NTP 서버나 신뢰할 수 있는 서버로 설정해서 사용하여야 함.<br>※ IOS 12.2 이전 버전을 사용하는 장비에는 접근 통제(ACL) 설정이 되어 있어야 양호 |     |   |      |      |
| 보안대책         |                                                                                                                                                                                                                           |     |   |      |      |
| 판단기준         | 양호: NTP 서비스가 서버로 설정된 경우                                                                                                                                                                                                   |     |   |      |      |
|              | 취약: NTP 서비스를 사용하지 않거나, 서버와 연동되어 있지 않은 경우                                                                                                                                                                                  |     |   |      |      |
| 조치방법         | NTP 사용 시 신뢰할 수 있는 서버로 설정                                                                                                                                                                                                  |     |   |      |      |
| 보안설정방법       |                                                                                                                                                                                                                           |     |   |      |      |
| 대상 장비별 점검 방법 |                                                                                                                                                                                                                           |     |   |      |      |
| CISCO        | Router# show running-config<br>NTP 서버 설정 확인                                                                                                                                                                               |     |   |      |      |
| Alteon       | /sys/ntp에서 NTP 서버 설정 확인                                                                                                                                                                                                   |     |   |      |      |
| Juniper      | user@juniper> configure<br>[edit]<br>user@juniper# show<br>root authentication 설정을 이용하여 [edit system] 레벨에서 NTP 서비스 설정 확인                                                                                                  |     |   |      |      |

위에 제시한 설정이 적용되지 않은 경우 아래의 보안설정방법에 따라 설정을 변경함

Cisco

NTP 서버 연동 설정  
Router# config terminal  
Router(config)# ntp server 129.237.32.2 (NTP 서버 IP)  
Router(config)# ^Z

Alteon

1. switch로 접속함.  
2. # cfg  
3. # /sys/ntp  
4. # on  
5. # prsrvr [NTP 서버 IP]  
6. # intrval [동기화 주기]  
tzzone +9:00

## 네트워크장비

7. # apply

8. # save

### ■ Juniper

Juniper 라우터에서 NTP를 설정하기 위해 Boot 서버 설정 필요

```
user@juniper> configure
```

```
[edit]
```

```
user@juniper# edit system ntp
```

```
[edit system ntp]
```

```
user@juniper# set boot-server 1.1.1.1 <- (NTP 서버주소)
```

- 클라이언트 모드

```
user@juniper# set server (NTP 서버주소)
```

- 브로드캐스트 모드

```
user@juniper# set broadcast (NTP 서버주소)
```

- Symmetric active 모드

```
user@juniper# set peer (NTP 서버주소) prefer
```

```
user@juniper# set peer (NTP 서버주소)
```

#### 조치 시 영향

일반적인 경우 영향 없음

## 네트워크장비

| 취약점 항목                                                                                               | 4.5. timestamp 로그 설정                                                                                                                 |     |   |      |      |
|------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------|-----|---|------|------|
| 대상                                                                                                   | CISCO, Juniper                                                                                                                       | 위험도 | 하 | Code | N-15 |
| 취약점 개요                                                                                               | 로그에 시간 정보가 없다면 사고 발생 시 공격 및 침입시도 시간에 관한 정보를 정확히 분석할 수 없어 로그 기록에 대한 신뢰성이 떨어지고 로그 분석에 차질이 빚어질 수 있으므로 로그의 무결성을 위해 timestamp 로그 설정을 권고함. |     |   |      |      |
| 보안대책                                                                                                 |                                                                                                                                      |     |   |      |      |
| 판단기준                                                                                                 | 양호: timestamp 로그 설정이 되어있는 경우                                                                                                         |     |   |      |      |
|                                                                                                      | 취약: timestamp 로그 설정이 되어있지 않은 경우                                                                                                      |     |   |      |      |
| 조치방법                                                                                                 | 로그에 시간 정보가 기록될 수 있도록 timestamp 로그 설정                                                                                                 |     |   |      |      |
| 보안설정방법                                                                                               |                                                                                                                                      |     |   |      |      |
| 대상 장비별 점검 방법                                                                                         |                                                                                                                                      |     |   |      |      |
| CISCO                                                                                                | Router> enable<br>Router# show logging<br><br>로그의 기록 정보 설정 확인                                                                        |     |   |      |      |
| Juniper                                                                                              | user@juniper> configure<br>[edit]<br>user@juniper# show log messages<br><br>로그의 기록 정보 설정 확인                                          |     |   |      |      |
| 위에 제시한 설정이 적용되지 않은 경우 아래의 보안설정방법에 따라 설정을 변경함                                                         |                                                                                                                                      |     |   |      |      |
| ■ Cisco                                                                                              |                                                                                                                                      |     |   |      |      |
| Router# config terminal                                                                              |                                                                                                                                      |     |   |      |      |
| Router(config)#service timestamp log date time msec local show-timezone<br>(log할 때 시간이 print 되도록 설정) |                                                                                                                                      |     |   |      |      |
| Router(config)# ^Z                                                                                   |                                                                                                                                      |     |   |      |      |
| ■ Juniper                                                                                            |                                                                                                                                      |     |   |      |      |
| user@juniper> set cli timestamp format '%m-%d-%T' <- 해당 월 일 시간을 입력.                                  |                                                                                                                                      |     |   |      |      |
| 조치 시 영향                                                                                              | 일반적인 경우 영향 없음                                                                                                                        |     |   |      |      |

## 네트워크장비

## 5. 기능 관리

| 취약점 항목       |                                                                                                                                                                                                  | 5.1. SNMP 서비스 확인 |   |      |      |
|--------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------|---|------|------|
| 대상           | CISCO, Alteon, Passport, Juniper                                                                                                                                                                 | 위험도              | 상 | Code | N-16 |
| 취약점 개요       | *SNMP는 *UDP 프로토콜을 사용하기 때문에 SNMP 서비스를 활성화하면 각종 공격, 예를 들어 *DOS 공격에 취약해질 뿐만 아니라 보안장비의 성능저하, 크래쉬, 리로드 등의 위험이 존재함. 불필요하다면 SNMP 서비스를 중지하고, 관리를 위해 NMS 솔루션과의 연동이 필요하다면 *Community String을 유추할 수 없게 설정함. |                  |   |      |      |
|              | *SNMP(Simple Network Management Protocol): TCP/IP 기반 네트워크상의 각 호스트에서 정기적으로 여러 정보를 자동으로 수집하여 네트워크 관리를 하기 위한 프로토콜을 의미함.                                                                             |                  |   |      |      |
|              | *UDP: 사용자 데이터그램 프로토콜(User Datagram Protocol)의 줄임말로 인터넷상에서 서로 정보를 주고받을 때 정보를 보낸다는 신호나 받는다는 신호 절차를 거치지 않고, 보내는 쪽에서 일방적으로 데이터를 전달하는 통신 프로토콜을 말함.                                                    |                  |   |      |      |
|              | *Community String: SNMP는 MIB라는 정보를 주고받기 위해 인증 과정에서 일종의 비밀번호인 'Community String'을 사용함.                                                                                                            |                  |   |      |      |
|              | *Dos(Denial of Service attack): 시스템을 악의적으로 공격해 해당 시스템의 자원을 부족하게 하여 원래 의도된 용도로 사용하지 못하게 하는 공격임. 특정 서버에게 수많은 접속 시도를 만들어 다른 이용자가 정상적으로 서비스 이용을 하지 못하게 하거나, 서버의 TCP 연결을 바닷내는 등의 공격이 이 범위에 포함됨.       |                  |   |      |      |
| 보안대책         |                                                                                                                                                                                                  |                  |   |      |      |
| 판단기준         | 양호: SNMP 서비스를 불필요하게 사용하지 않는 경우                                                                                                                                                                   |                  |   |      |      |
|              | 취약: SNMP 서비스를 불필요하게 사용하는 경우                                                                                                                                                                      |                  |   |      |      |
| 조치방법         | SNMP 서비스가 불필요할 경우 중지                                                                                                                                                                             |                  |   |      |      |
| 보안설정방법       |                                                                                                                                                                                                  |                  |   |      |      |
| 대상 장비별 점검 방법 |                                                                                                                                                                                                  |                  |   |      |      |
| CISCO        | Router# show running-config<br>Router# show snmp<br><br>1. SNMP 설정 확인<br>2. SNMP 서비스 동작 확인<br>※ SNMP 서비스 비활성화 시 아래 문구 출력<br>!<br>%SNMP agent not enabled<br>!                                    |                  |   |      |      |
| Juniper      | user@juniper> configure<br>[edit]<br>user@juniper# show snmp<br><br>root authentication 설정을 이용하여 [edit system] 레벨에서 snmp 서비스 설정 확인                                                               |                  |   |      |      |

위에 제시한 설정이 적용되지 않은 경우 아래의 보안설정방법에 따라 설정을 변경함

위에 제시한 설정이 적용되지 않은 경우 아래의 보안설정방법에 따라 설정을 변경함

## 네트워크장비

## ■ CISCO

```
Router# config terminal
Router(config)# no snmp-server
Router(config)# ^Z
```

## ■ Alteon / Passport

SNMP 서비스가 불필요하다면 서비스 중지

## ■ CISCO

```
user@juniper> configure
user@juniper# no set snmp community public
```

## 조치 시 영향

SNMP 서비스에 영향을 줄 수 있음

## 네트워크장비

| 취약점 항목 | 5.2. SNMP community string 복잡성 설정                                                                                                                        |     |   |      |      |
|--------|----------------------------------------------------------------------------------------------------------------------------------------------------------|-----|---|------|------|
| 대상     | CISCO, Alteon, Passport, Juniper                                                                                                                         | 위험도 | 상 | Code | N-17 |
| 취약점 개요 | SNMP의 Public, Private과 같은 디폴트 community String을 변경하지 않고 사용할 경우, 악의적인 사용자가 장비 설정을 쉽게 변경하여 중요 시스템 정보가 노출될 수 있으므로 추측하기 어려운 Community String으로 변경하는 설정이 필요함. |     |   |      |      |
| 보안대책   |                                                                                                                                                          |     |   |      |      |
| 판단기준   | 양호: SNMP 서비스를 사용하지 않거나, 유추하기 어려운 Community String을 설정한 경우                                                                                                |     |   |      |      |
|        | 취약: 디폴트 Community String을 변경하지 않거나, 유추하기 쉬운 Community String으로 설정한 경우                                                                                    |     |   |      |      |
| 조치방법   | Public, Private 외 다른 Community String을 설정                                                                                                                |     |   |      |      |
| 보안설정방법 |                                                                                                                                                          |     |   |      |      |

| 대상 장비별 점검 방법            |                                                                                                                                |
|-------------------------|--------------------------------------------------------------------------------------------------------------------------------|
| <b>CISCO</b>            | Router# show running-config<br>SNMP 설정 확인                                                                                      |
| <b>Alteon, Passport</b> | #snmp 설정에서 Community String 설정 확인                                                                                              |
| <b>Juniper</b>          | user@juniper> configure<br>[edit]<br>user@juniper# show<br>root authentication 설정을 이용하여 [edit system] 레벨에서 community string 확인 |

위에 제시한 설정이 적용되지 않은 경우 아래의 보안설정방법에 따라 설정을 변경함

#### ■ CISCO

Community String 문자열 변경

Router# config terminal

Router(config)# snmp-server Community <커뮤니티명>

#### ■ Alteon

네트워크 장비는 SNMP 로의 취약성이 존재하므로 누구나 추측하기 어렵고 의미가 없는 문자열, 영문자 혼합으로 변경 권고함

1. switch 로 접속

2. # cfg/sys/ssnmp

3. 다음 중에 해당하는 경우 선택

# rcomm - SNMP read community string 을 설정(최대 32 자, Default String – public)

# wcomm - SNMP write community string 을 설정(최대 32 자, Default String – private)

4. # apply



## 네트워크장비

5. # save

■ Passport

1. switch 로 접속

2. # config snmp-v3 community commname <Comm Idx> new-commname <value>

|         |               |
|---------|---------------|
| 조치 시 영향 | 일반적인 경우 영향 없음 |
|---------|---------------|

## 네트워크장비

| 취약점 항목       | 5.3. SNMP ACL 설정                                                                                                                                              |     |   |      |      |
|--------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------|-----|---|------|------|
| 대상           | CISCO, Passport, Juniper, Piolink                                                                                                                             | 위험도 | 상 | Code | N-18 |
| 취약점 개요       | SNMP ACL을 설정할 경우 접속 대상 호스트를 지정하여 접근이 가능한 IP를 제한할 수 있음. 이 기능을 사용하여 정보의 노출을 기본적으로 제한하는 것이 필요함. 임의의 호스트에서 SNMP 접근을 차단하여 호스트로부터의 Community String 추측공격을 차단할 수 있음. |     |   |      |      |
| 보안대책         |                                                                                                                                                               |     |   |      |      |
| 판단기준         | 양호: SNMP 서비스를 사용하지 않거나, SNMP 접근에 대한 ACL을 적용 한 경우                                                                                                              |     |   |      |      |
|              | 취약: SNMP 접근에 대한 ACL을 적용 하지 않은 경우                                                                                                                              |     |   |      |      |
| 조치방법         | SNMP 접근에 대한 Access list 설정                                                                                                                                    |     |   |      |      |
| 보안설정방법       |                                                                                                                                                               |     |   |      |      |
| 대상 장비별 점검 방법 |                                                                                                                                                               |     |   |      |      |
| CISCO        | Router# show running-config<br><br>1. SNMP 설정 확인<br>2. Access-List 설정 확인                                                                                      |     |   |      |      |
| Passport     | config snmp-v3에서 접근목록 설정 확인                                                                                                                                   |     |   |      |      |
| Juniper      | edit snmp에서 접근목록 설정 확인                                                                                                                                        |     |   |      |      |
| Piolink      | configuration 모드에서 snmp 접근목록 설정 확인                                                                                                                            |     |   |      |      |

위에 제시한 설정이 적용되지 않은 경우 아래의 보안설정방법에 따라 설정을 변경함

CISCO

1. access-list 를 이용하여 특정 호스트만 열어 주기(port:161,162)  
2. Router# config terminal  
3. Router(config)# access-list 100 permit ip host 100.100.100.100 any  
4. Router(config)# access-list 100 deny udp any any eq snmp  
5. Router(config)# access-list 100 deny udp any any eq snmptrap  
6. Router(config)# access-list 100 permit ip any any  
7. Router(config)# interface serial 0 (해당 인터페이스에 설정)  
8. Router(config-if)# ip access-group 100 in  
9. 시스코 스위치 장비인 경우 vlan 에 설정  
Router(config)# interface vlan1  
Router(config-if)# ip access-group 100 in

Passport

## 네트워크장비

1. switch 로 접속
2. # config snmp-v3 community create <Comm Idx> <name> <security> [tag <value>]
3. # config snmp-v3 group-member create <user name> <model> [<group name>]
4. # config snmp-v3 group-access create <group name> <prefix> <model> <level>
5. # config snmp-v3 group-access view <group name> <prefix> <model> <leve> [read <value>]  
[write <value>] [notify <value>]

### ■ Juniper

1. 해당 인터페이스에서만 접속가능  
[edit snmp]  
snmp {  
    interface [ so-0/0/0.0 so-0/0/0.1 at-1/0/1.0 at-1/0/1.1 ];  
}
2. 203.235.xxx.xxx에서만 해당 네트워크 장비로 접속가능  
[edit snmp community]  
    clients {  
        default restrict;  
        203.235.xxx.xxx <restrict>;

### ■ Piolink

1. 관리자 모드로 접속
2. configuration
3. snmp <agent-address> <ip-addr> <port>

|         |               |
|---------|---------------|
| 조치 시 영향 | 일반적인 경우 영향 없음 |
|---------|---------------|

## 네트워크장비

| 취약점 항목       | 5.4. SNMP 커뮤니티 권한 설정                                                                                                                                                                                                                                        |     |   |      |      |
|--------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----|---|------|------|
| 대상           | CISCO, Passport                                                                                                                                                                                                                                             | 위험도 | 상 | Code | N-19 |
| 취약점 개요       | SNMP에서는 RO(Read Only)와 RW(Read Write) 모드를 제공함. 대부분 RO 모드를 사용하지만 일부 관리자들은 SNMP를 이용한 쉬운 관리를 위해 RW Community 문자열을 사용하기도 하는데, 이때 보안 설정을 확실하게 하지 않을 경우 SNMP를 이용하여 설정을 수정할 수 있는 등 보안 문제를 유발할 수 있음. SNMP를 이용하면 전체 네트워크의 구성, MAC 주소, IP 주소, SW 정보, HW 정보 등을 알 수 있음. |     |   |      |      |
| 보안대책         |                                                                                                                                                                                                                                                             |     |   |      |      |
| 판단기준         | 양호: SNMP Community String 권한이 RO인 경우                                                                                                                                                                                                                        |     |   |      |      |
|              | 취약: SNMP Community String 권한이 불필요하게 RW로 설정된 경우                                                                                                                                                                                                              |     |   |      |      |
| 조치방법         | SNMP Community String 권한 설정 (RW 권한 삭제 권고)                                                                                                                                                                                                                   |     |   |      |      |
| 보안설정방법       |                                                                                                                                                                                                                                                             |     |   |      |      |
| 대상 장비별 점검 방법 |                                                                                                                                                                                                                                                             |     |   |      |      |
| CISCO        | Router# show running-config<br>SNMP 설정 확인                                                                                                                                                                                                                   |     |   |      |      |
| Passport     | config snmp 에서 SNMP community 권한 확인                                                                                                                                                                                                                         |     |   |      |      |
| Juniper      | user@juniper> configure<br>[edit]<br>user@juniper# show<br><br>root authentication 설정을 이용하여 [edit system] 레벨에서 SNMP community 권한 확인                                                                                                                         |     |   |      |      |

위에 제시한 설정이 적용되지 않은 경우 아래의 보안설정방법에 따라 설정을 변경함

■ CISCO

SNMP Community String 권한 설정 방법(RW 권한 삭제 권고)

Router# config terminal

Router(config)# snmp-server community <스트링명> RO

Router(config)# snmp-server community <스트링명> RW

■ Passport

SNMP Community String 권한 설정 방법(RW 권한 삭제 권고)

1. switch 로 접속

2. # config snmp-v3 community create <Comm Idx> <name> <security> [tag <value>]

3. # config snmp-v3 group-member create <user name> <model> [<group name>]

4. # config snmp-v3 group-access create <group name> <prefix> <model> <level>

5. # config snmp-v3 group-access view <group name> <prefix> <model> <leve> [read <value>]  
[write <value>] [notify <value>]

|         |                                      |
|---------|--------------------------------------|
| 조치 시 영향 | 쓰기 권한 설정 시에 라우터 정보의 변경까지 가능하므로 주의 필요 |
|---------|--------------------------------------|

## 네트워크장비

| 취약점 항목                                                 | 5.5. TFTP 서비스 차단                                                                                                           |     |   |      |      |
|--------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------|-----|---|------|------|
| 대상                                                     | CISCO, Alteon, Juniper                                                                                                     | 위험도 | 상 | Code | N-20 |
| 취약점 개요                                                 | TFTP 서비스는 인증 절차를 요구하지 않으면서 평문으로 통신하므로 보안상 취약함. 이 서비스를 사용하지 않는다면 비활성화해야 하지만 사용이 필요하다면 접근 제한 (ACL) 설정을 통해 비인가자의 접근을 차단하여야 함. |     |   |      |      |
| 보안대책                                                   |                                                                                                                            |     |   |      |      |
| 판단기준                                                   | 양호: TFTP 서비스를 사용하지 않거나, ACL을 적용하여 사용하는 경우                                                                                  |     |   |      |      |
|                                                        | 취약: TFTP 서비스를 사용하고 ACL을 설정하지 않은 경우                                                                                         |     |   |      |      |
| 조치방법                                                   | 불필요한 TFTP 서비스 사용 시 제거                                                                                                      |     |   |      |      |
| 보안설정방법                                                 |                                                                                                                            |     |   |      |      |
| 대상 장비별 점검 방법                                           |                                                                                                                            |     |   |      |      |
| CISCO                                                  | Router# show running-config                                                                                                |     |   |      |      |
|                                                        | TFTP 설정 정보 확인                                                                                                              |     |   |      |      |
| Alteon                                                 | /cfg/slb/filt에서 tftp 서비스 설정 제거 확인                                                                                          |     |   |      |      |
| Juniper                                                | user@juniper> configure                                                                                                    |     |   |      |      |
|                                                        | [edit]                                                                                                                     |     |   |      |      |
|                                                        | user@juniper# show                                                                                                         |     |   |      |      |
|                                                        | root authentication 설정을 이용하여 [edit system] 레벨에서 TFTP 서비스 확인                                                                |     |   |      |      |
| 위에 제시한 설정이 적용되지 않은 경우 아래의 보안설정방법에 따라 설정을 변경함           |                                                                                                                            |     |   |      |      |
| ■ CISCO                                                |                                                                                                                            |     |   |      |      |
| 외부망에서 사용할 필요가 없는 TFTP 서비스 포트 차단                        |                                                                                                                            |     |   |      |      |
| Router# config terminal                                |                                                                                                                            |     |   |      |      |
| Router(config)# no service tftp                        |                                                                                                                            |     |   |      |      |
| ■ Alteon                                               |                                                                                                                            |     |   |      |      |
| # /cfg/slb/filt <filter number>/sport 69 (tftp 서비스 제거) |                                                                                                                            |     |   |      |      |
| 조치 시 영향                                                | 일반적인 경우 영향 없음                                                                                                              |     |   |      |      |

## 네트워크장비

| 취약점 항목       | 5.6. Spoofing 방지 필터링 적용                                                                                                             |     |   |      |      |
|--------------|-------------------------------------------------------------------------------------------------------------------------------------|-----|---|------|------|
| 대상           | CISCO, Alteon, Juniper                                                                                                              | 위험도 | 상 | Code | N-21 |
| 취약점 개요       | Source IP 주소가 broadcast, multicast, loopback인 것은 전혀 사용될 필요가 없으나 종종 악의적인 목적(DoS 공격 시)으로 사용될 수도 있으므로, ACL를 설정하여 변조된 불법 패킷을 차단하도록 설정함. |     |   |      |      |
| 보안대책         |                                                                                                                                     |     |   |      |      |
| 판단기준         | 양호: 악의적인 공격에 대비하여 Source IP에 ACL을 적용한 경우                                                                                            |     |   |      |      |
|              | 취약: 악의적인 공격에 대비하여 Source IP에 ACL을 적용하지 않은 경우                                                                                        |     |   |      |      |
| 조치방법         | Source IP에 ACL 적용                                                                                                                   |     |   |      |      |
| 보안설정방법       |                                                                                                                                     |     |   |      |      |
| 대상 장비별 점검 방법 |                                                                                                                                     |     |   |      |      |
| CISCO        | Router# show running                                                                                                                |     |   |      |      |
|              | IP spoofing 방지 설정 확인                                                                                                                |     |   |      |      |
| Alteon       | /slb/filt에서 IP spoofing 방지를 위한 ACL 설정 확인                                                                                            |     |   |      |      |
| Juniper      | Configure Firewall Filters와 Apply Firewall Filters 설정 확인                                                                            |     |   |      |      |

위에 제시한 설정이 적용되지 않은 경우 아래의 보안설정방법에 따라 설정을 변경함

※ IP Spoofing 은 IP를 속여서 공격하는 기법을 의미하며, 다음과 같은 TCP/IP 프로토콜 약점을 이용한 공격이 알려져 있음

1. 순서 제어 번호 추측 (Sequence number guessing)
2. 반 접속 시도 공격 (Syn flooding)
3. 접속 가로채기(Connection hijacking)
4. RST를 이용한 접속 끊기 (Connection killing by RST)
5. FIN을 이용한 접속 끊기 (Connection by FIN)
6. 네트워크 데몬 정지(Killing the INETD)
7. TCP 윈도우 위장(TCP window spoofing)

IP Spoofing 공격은 공격하고자 하는 시스템 서비스 포트나 그에 대한 취약점을 알아내는 것부터 시작되며, 공격자는 스캔용 프로그램과 점검 툴을 사용하여 해당 네트워크를 공격함

공격으로 사용되는 툴 중에는 자신의 위치를 감추기 위해 Spoofed IP를 사용함

■ CISCO

1. Global configuration mode 로 접속

2. access-list number deny ip 127.0.0.0 0.255.255.255 any

## 네트워크장비

3. access-list number deny ip 224.0.0.0 31.255.255.255 any
4. access-list number deny ip host 0.0.0.0 any
5. access-list number permit ip any any

### ■ Alteon

1. switch로 접속함.
2. # cfg
3. # /slb/filt <filter number>
4. # sip 127.0.0.0

### ■ Juniper

1. Configure Firewall Filters

```
[edit firewall]
 firewall {
 filter filter-name {
 term term-name {
 accounting-profile name;
 from {
 source-address 127.0.0.0/24;
 source-address 224.0.0.0/4;
 source-address 0.0.0.0/0;
 }
 then {
 discard;
 }
 }
 }
 }
```

2. Apply Firewall Filters

```
[edit interfaces interface-name unit logical-unit-number family inet]
 interfaces {
 interface-name {
 unit logical-unit-number {
 family inet {
 filter {
 input filter-name;
 output filter-name;
 }
 }
 }
 }
 }
```

## 네트워크장비

|                                    |                                      |
|------------------------------------|--------------------------------------|
| <pre>}<br/><br/>}<br/><br/>}</pre> |                                      |
| 조치 시 영향                            | 필터링 적용 시 사용하는 ACL은 라우터 성능에 많은 영향을 미침 |



## 네트워크장비

| 취약점 항목                                                            | 5.7. DDoS 공격 방어 설정                                                                                                                                                               |     |   |      |      |
|-------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----|---|------|------|
| 대상                                                                | CISCO, Juniper                                                                                                                                                                   | 위험도 | 상 | Code | N-22 |
| 취약점 개요                                                            | 악성 봇을 이용한 DDoS 공격을 위해 해커는 일반 사용자 PC에 봇을 감염시킨 후 봇에 감염된 PC에 공격 명령을 전달함. 다른 공격 유형으로 명령 및 제어 서버의 접속 없이 감염된 컴퓨터 실행 시 특정 사이트를 공격하도록 제작·유포되어 해당 서비스를 마비시키는 등 다양한 공격이 존재하므로 각별한 주의가 요구됨. |     |   |      |      |
| 보안대책                                                              |                                                                                                                                                                                  |     |   |      |      |
| 판단기준                                                              | 양호: DDoS 공격 방어 설정이 되어있는 경우                                                                                                                                                       |     |   |      |      |
|                                                                   | 취약: DDoS 공격 방어 설정이 되어있지 않은 경우                                                                                                                                                    |     |   |      |      |
| 조치방법                                                              | DDoS 공격 방어 설정 점검                                                                                                                                                                 |     |   |      |      |
| 보안설정방법                                                            |                                                                                                                                                                                  |     |   |      |      |
| 대상 장비별 점검 방법                                                      |                                                                                                                                                                                  |     |   |      |      |
| CISCO                                                             | Router> enable<br>Router# show running (하단 부분에서 확인 가능)                                                                                                                           |     |   |      |      |
| Juniper                                                           | user@juniper> configure<br>[edit]<br>user@juniper# show configuration<br><br>root authentication 설정을 이용하여 [edit system] 레벨에서 DDoS 방어 설정 요소 확인                                    |     |   |      |      |
| 위에 제시한 설정이 적용되지 않은 경우 아래의 보안설정방법에 따라 설정을 변경함                      |                                                                                                                                                                                  |     |   |      |      |
| ■ CISCO, Juniper                                                  |                                                                                                                                                                                  |     |   |      |      |
| <DDoS 공격 방어 설정 요소>                                                |                                                                                                                                                                                  |     |   |      |      |
| 1. Fragment 공격 차단 설정                                              |                                                                                                                                                                                  |     |   |      |      |
| 2. 적절한 ACL 을 통한 사전방어 설정 필요                                        |                                                                                                                                                                                  |     |   |      |      |
| 3. 보안담당자와 네트워크담당자가 연계하여 차단 설정                                     |                                                                                                                                                                                  |     |   |      |      |
| <DDoS 공격 방어 설정(차단되어야 하는 IP 대역)>                                   |                                                                                                                                                                                  |     |   |      |      |
| 1. 0.0.0.0/8 : Default/Broadcast & Other unique IP                |                                                                                                                                                                                  |     |   |      |      |
| 2. 127.0.0.0/8 : Host Loopback IP address                         |                                                                                                                                                                                  |     |   |      |      |
| 3. 169.254.0.0/16 : DHCP 를 통한 IP 미 할당시 자동 생성되는 IP                 |                                                                                                                                                                                  |     |   |      |      |
| 4. 192.0.2.0/24 : TEST-NET IP                                     |                                                                                                                                                                                  |     |   |      |      |
| 5. 10.0.0.0/8, 172.16.0.0/12, 192.168.0.0/16:RFC 1918 에 정의된 사설 IP |                                                                                                                                                                                  |     |   |      |      |
| 6. access-list 번호는 100~199 구간을 사용하여 Extended access-list를 사용      |                                                                                                                                                                                  |     |   |      |      |
| 조치 시 영향                                                           | 필터링 적용 시 사용하는 ACL은 라우터 성능에 많은 영향을 미침                                                                                                                                             |     |   |      |      |

## 네트워크장비

| 취약점 항목       | 5.8. 사용하지 않는 인터페이스의 shutdown 설정                                                                                                                                                        |     |   |      |      |
|--------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----|---|------|------|
| 대상           | CISCO, Alteon, Juniper                                                                                                                                                                 | 위험도 | 상 | Code | N-23 |
| 취약점 개요       | 사용하지 않는 포트에 연결된 인터페이스를 shutdown 하지 않을 경우 물리적인 접근을 통해 비인가자의 불법적인 접근이 가능함. 네트워크 정보 유출 및 내부 네트워크 손상 위험 방지를 위해 사용하지 않는 인터페이스를 shutdown 시키는 설정이 필요함.                                        |     |   |      |      |
| 보안대책         |                                                                                                                                                                                        |     |   |      |      |
| 판단기준         | 양호: 사용하지 않는 인터페이스가 차단된 경우                                                                                                                                                              |     |   |      |      |
|              | 취약: 사용하지 않는 인터페이스가 차단되지 않은 경우                                                                                                                                                          |     |   |      |      |
| 조치방법         | 사용하지 않은 인터페이스 차단                                                                                                                                                                       |     |   |      |      |
| 보안설정방법       |                                                                                                                                                                                        |     |   |      |      |
| 대상 장비별 점검 방법 |                                                                                                                                                                                        |     |   |      |      |
| CISCO        | Router# show running-config<br>Router# show interface status<br>Router# show ip interface brief<br><br>1. 각 Interface 설정 확인<br>2. Interface 상태 확인<br>(해당포트가 down/up 이 되어 있는지 확인할 수 있음) |     |   |      |      |
| Juniper      | user@juniper> configure<br>user@juniper# show ip<br><br>불필요한 포트 차단 확인                                                                                                                  |     |   |      |      |

위에 제시한 설정이 적용되지 않은 경우 아래의 보안설정방법에 따라 설정을 변경함

■ CISCO

Router# config terminal  
Router(config)# interface fastethernet 0/1  
Router(config-line)# shutdown  
사용할 포트는 no shutdown 으로 포트 상태를 up 시켜줌

■ Alteon

사용하지 않은 인터페이스 차단  
# config terminal  
# interface fastethernet 0/1  
# shutdown  
사용할 포트는 no shutdown으로 포트 상태를 up 시켜줌

■ Juniper

기본적인 인터페이스 비활성

## 네트워크장비

[edit interface interface-name] <- 해당 인터페이스 이름 삽입  
disable;

예제 >

user@juniper# configure

user@juniper# edit interfaces

[edit interfaces]

user@juniper# set so-1/1/0 disable

user@juniper# ^z

user@juniper# edit interface

[edit interfaces]

user@juniper# show so-1/1/0

```
so-1/1/0 {
 disable;
 mtu 8000;
 clocking internal;
 encapsulation aaa;
 sonet-options {
 fcs 16;
 }
 unit 0 {
 family inet {
 address 1.1.1.1/32 {
 destination 1.1.1.2;
 }
 }
 }
}
```

**조치 시 영향**

일반적인 경우 영향 없음

## 네트워크장비

| 취약점 항목                                                  | 5.9. TCP keepalive 서비스 설정                                                                                                                                     |     |   |      |      |
|---------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------|-----|---|------|------|
| 대상                                                      | CISCO                                                                                                                                                         | 위험도 | 중 | Code | N-24 |
| 취약점 개요                                                  | TCP/IP 기반으로 연결된 상태에서 클라이언트의 갑작스러운 리부팅이나 스위치 Off가 일어날 경우 해당 세션을 서버에서 자동으로 종료시키지 못하므로 TCP/IP의 timeout 기능인 Keepalive를 사용하여 비정상적으로 종료된 세션이 정상적으로 종료될 수 있도록 하여야 함. |     |   |      |      |
| 보안대책                                                    |                                                                                                                                                               |     |   |      |      |
| 판단기준                                                    | 양호: TCP Keepalive 서비스가 설정된 경우                                                                                                                                 |     |   |      |      |
|                                                         | 취약: TCP Keepalive 서비스가 설정되어 있지 않은 경우                                                                                                                          |     |   |      |      |
| 조치방법                                                    | 사용되지 않는 터미널 삭제, 원격에서 동일한 터미널 접속 방지                                                                                                                            |     |   |      |      |
| 보안설정방법                                                  |                                                                                                                                                               |     |   |      |      |
|                                                         |                                                                                                                                                               |     |   |      |      |
| 대상 장비별 점검 방법                                            |                                                                                                                                                               |     |   |      |      |
| CISCO                                                   | Router# show runnnig-config                                                                                                                                   |     |   |      |      |
|                                                         | TCP Keepalive 서비스 설정 확인                                                                                                                                       |     |   |      |      |
| 위에 제시한 설정이 적용되지 않은 경우 아래의 보안설정방법에 따라 설정을 변경함            |                                                                                                                                                               |     |   |      |      |
|                                                         |                                                                                                                                                               |     |   |      |      |
| ■ CISCO                                                 |                                                                                                                                                               |     |   |      |      |
| 사용되지 않는 터미널 삭제, 원격에서의 동일한 터미널 접속 방지                     |                                                                                                                                                               |     |   |      |      |
| Router# config terminal                                 |                                                                                                                                                               |     |   |      |      |
| Router(config) service tcp-keepalives-in (비정상 종료 세션 종료) |                                                                                                                                                               |     |   |      |      |
|                                                         |                                                                                                                                                               |     |   |      |      |
| 조치 시 영향                                                 | 일반적인 경우 영향 없음                                                                                                                                                 |     |   |      |      |

## 네트워크장비

| 취약점 항목       | 5.10. Finger 서비스 차단                                                                                                                       |     |   |      |      |
|--------------|-------------------------------------------------------------------------------------------------------------------------------------------|-----|---|------|------|
| 대상           | CISCO, Juniper                                                                                                                            | 위험도 | 중 | Code | N-25 |
| 취약점 개요       | Finger 서비스를 사용할 경우 기본적인 장비의 접속 상태가 노출될 수 있고, 특별히 NMS 등에서 사용하지 않으면 VTY(Virtual Teletype)의 사용 현황을 원격에서 파악하는 것이 가능하므로 Finger 서비스 제한 설정이 필요함. |     |   |      |      |
| 보안대책         |                                                                                                                                           |     |   |      |      |
| 판단기준         | 양호: Finger 서비스를 차단하고 있는 경우                                                                                                                |     |   |      |      |
|              | 취약: Finger 서비스를 차단하고 있지 않는 경우                                                                                                             |     |   |      |      |
| 조치방법         | 각 장비별 Finger 서비스 제한 설정                                                                                                                    |     |   |      |      |
| 보안설정방법       |                                                                                                                                           |     |   |      |      |
| 대상 장비별 점검 방법 |                                                                                                                                           |     |   |      |      |
| CISCO        | Router# show running-config                                                                                                               |     |   |      |      |
|              | Finger 서비스 설정 확인                                                                                                                          |     |   |      |      |
| Juniper      | user@juniper> configure                                                                                                                   |     |   |      |      |
|              | [edit]                                                                                                                                    |     |   |      |      |
|              | user@juniper# show                                                                                                                        |     |   |      |      |
|              | root authentication 설정을 이용하여 [edit system] 레벨에서 Finger 서비스 설정 확인                                                                          |     |   |      |      |

위에 제시한 설정이 적용되지 않은 경우 아래의 보안설정방법에 따라 설정을 변경함

■ CISCO

최근 출시되는 IOS는 no service finger 명령 대신 no ip finger 명령을 사용하기도 함

Router# config terminal

Router(config)# no service finger (이전)

Router(config)# no ip finger

■ Juniper

user@juniper> configure

[edit]

user@juniper# edit system services

[edit system services]

no finger {

<connection-limit limit>;

<rate-limit limit>;

}

| 조치 시 영향 | 일반적인 경우 영향 없음 |
|---------|---------------|
|---------|---------------|

## 네트워크장비

| 취약점 항목                                                                                                                                                                                                                                                                                                                                                                                                                                         | 5.11. 웹 서비스 차단                                                                                                                                           |     |   |      |      |              |  |       |                                                |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------|-----|---|------|------|--------------|--|-------|------------------------------------------------|
| 대상                                                                                                                                                                                                                                                                                                                                                                                                                                             | CISCO                                                                                                                                                    | 위험도 | 중 | Code | N-26 |              |  |       |                                                |
| 취약점 개요                                                                                                                                                                                                                                                                                                                                                                                                                                         | 네트워크 장비에서 제공하는 관리용 웹(HTTP) 사이트는 기존에 알려진 웹 취약점이나 패스워드 추측 공격 등에 취약할 수 있으므로 불필요한 경우에는 HTTP 사용을 제한하여야 함. HTTP 서버를 사용해야 한다면 HTTP 서버에 접속할 수 있는 관리자 IP를 제한해야 함. |     |   |      |      |              |  |       |                                                |
| 보안대책                                                                                                                                                                                                                                                                                                                                                                                                                                           |                                                                                                                                                          |     |   |      |      |              |  |       |                                                |
| 판단기준                                                                                                                                                                                                                                                                                                                                                                                                                                           | 양호: 웹 서비스를 차단한 경우                                                                                                                                        |     |   |      |      |              |  |       |                                                |
|                                                                                                                                                                                                                                                                                                                                                                                                                                                | 취약: 웹 서비스를 차단하지 않은 경우                                                                                                                                    |     |   |      |      |              |  |       |                                                |
| 조치방법                                                                                                                                                                                                                                                                                                                                                                                                                                           | HTTP 서비스 차단 또는 HTTP 서버를 관리하는 관리자 접속 IP 설정.                                                                                                               |     |   |      |      |              |  |       |                                                |
| 보안설정방법                                                                                                                                                                                                                                                                                                                                                                                                                                         |                                                                                                                                                          |     |   |      |      |              |  |       |                                                |
| <table><tr><th colspan="2">대상 장비별 점검 방법</th></tr><tr><td>CISCO</td><td>Router# show running-config<br/><br/>웹 서비스 설정 확인</td></tr></table>                                                                                                                                                                                                                                                                                                      |                                                                                                                                                          |     |   |      |      | 대상 장비별 점검 방법 |  | CISCO | Router# show running-config<br><br>웹 서비스 설정 확인 |
| 대상 장비별 점검 방법                                                                                                                                                                                                                                                                                                                                                                                                                                   |                                                                                                                                                          |     |   |      |      |              |  |       |                                                |
| CISCO                                                                                                                                                                                                                                                                                                                                                                                                                                          | Router# show running-config<br><br>웹 서비스 설정 확인                                                                                                           |     |   |      |      |              |  |       |                                                |
| 위에 제시한 설정이 적용되지 않은 경우 아래의 보안설정방법에 따라 설정을 변경함                                                                                                                                                                                                                                                                                                                                                                                                   |                                                                                                                                                          |     |   |      |      |              |  |       |                                                |
| <div>■ CISCO</div> <div>Router# config terminal</div> <div>Router(config)# no ip http server</div> <div>Router(config)# ^Z</div> <div>※ IOS 상의 HTTP 서버를 사용해야만 한다면, HTTP WEB_EXEC 서비스를 비활성화 함으로써 위험을 우회할 수 있음</div> <div>Router# config terminal</div> <div>Router(config)# ip http active-session-modules exclude_webexec</div> <div>Router(config)# ip http secure-active-session-modules exclude_webexec</div> <div>Router(config)# ^Z</div> |                                                                                                                                                          |     |   |      |      |              |  |       |                                                |
| 조치 시 영향                                                                                                                                                                                                                                                                                                                                                                                                                                        | 일반적인 경우 영향 없음                                                                                                                                            |     |   |      |      |              |  |       |                                                |

## 네트워크장비

| 취약점 항목                                                                                                                                        | 5.12. TCP/UDP Small 서비스 차단                                                                                                                                         |     |   |      |      |
|-----------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----|---|------|------|
| 대상                                                                                                                                            | CISCO                                                                                                                                                              | 위험도 | 중 | Code | N-27 |
| 취약점 개요                                                                                                                                        | Cisco 제품의 경우 DoS 공격의 대상이 될 수 있는 서비스(echo, discard, daytime, chargen)를 기본적으로 제공하므로 보안상 위험이 존재함. 이러한 서비스는 일반적으로 거의 사용하지 않으므로 서비스가 불필요하게 열려있다면 제거하여 DoS 공격을 예방할 수 있음. |     |   |      |      |
| 보안대책                                                                                                                                          |                                                                                                                                                                    |     |   |      |      |
| 판단기준                                                                                                                                          | 양호: TCP/UDP Small 서비스가 제한되어 있는 경우                                                                                                                                  |     |   |      |      |
|                                                                                                                                               | 취약: TCP/UDP Small 서비스가 제한되어 있지 않는 경우                                                                                                                               |     |   |      |      |
| 조치방법                                                                                                                                          | TCP/UDP Small Service 제한 설정                                                                                                                                        |     |   |      |      |
| 보안설정방법                                                                                                                                        |                                                                                                                                                                    |     |   |      |      |
| 대상 장비별 점검 방법                                                                                                                                  |                                                                                                                                                                    |     |   |      |      |
| CISCO                                                                                                                                         | Router# show running-config<br><br>1. tcp-small-servers 설정 확인<br>2. udp-small-servers 설정 확인                                                                        |     |   |      |      |
| 위에 제시한 설정이 적용되지 않은 경우 아래의 보안설정방법에 따라 설정을 변경함                                                                                                  |                                                                                                                                                                    |     |   |      |      |
| ■ CISCO                                                                                                                                       |                                                                                                                                                                    |     |   |      |      |
| 서비스 거부 공격을 완전히 차단하지는 못하지만, 알려진 서비스 거부 공격 포트 설정 권고 TCP/UDP 관련 Small 서버들의 기능은 Disable 설정함                                                       |                                                                                                                                                                    |     |   |      |      |
| Router# config terminal<br>Router(config)# no service tcp-small-servers<br>Router(config)# no service udp-small-servers<br>Router(config)# ^Z |                                                                                                                                                                    |     |   |      |      |
| ※ TCP/UDP Small 서비스는 IOS 11.3 이상에서는 기본적으로 서비스가 제거된 상태이므로 Small 서버들이 Default로 Disable되어 있지만 낮은 버전의 경우는 직접 설정해 주어야 함.                           |                                                                                                                                                                    |     |   |      |      |
| 조치 시 영향                                                                                                                                       | 일반적인 경우 영향 없음                                                                                                                                                      |     |   |      |      |

## 네트워크장비

| 취약점 항목       | 5.13. Bootp 서비스 차단                                                                                                                                                        |     |   |      |      |
|--------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----|---|------|------|
| 대상           | CISCO, Alteon, Juniper                                                                                                                                                    | 위험도 | 중 | Code | N-28 |
| 취약점 개요       | Bootp는 네트워크를 이용하여 사용자가 OS를 로드할 수 있게 하고 자동으로 IP 주소를 받게 구성하는 프로토콜임. Bootp 서비스를 제공하는 또 다른 라우터 상의 OS 사본에 접속할 수 있으며, OS 소프트웨어의 복사본을 다운로드 할 수 있는 취약점이 존재하므로 사용하지 않는다면 비활성화 해야함. |     |   |      |      |
| 보안대책         |                                                                                                                                                                           |     |   |      |      |
| 판단기준         | 양호: Bootp 서비스가 제한되어 있는 경우                                                                                                                                                 |     |   |      |      |
|              | 취약: Bootp 서비스가 제한되어 있지 않는 경우                                                                                                                                              |     |   |      |      |
| 조치방법         | 각 장비별 Bootp 서비스 제한 설정                                                                                                                                                     |     |   |      |      |
| 보안설정방법       |                                                                                                                                                                           |     |   |      |      |
| 대상 장비별 점검 방법 |                                                                                                                                                                           |     |   |      |      |
| CISCO        | Router# show running-config<br>ip bootp server 설정 확인                                                                                                                      |     |   |      |      |
| Alteon       | #bootp disable 설정 확인                                                                                                                                                      |     |   |      |      |
| Juniper      | user@switch>show configuration & show interfaces detail<br>bootp 서비스 설정 확인                                                                                                |     |   |      |      |

위에 제시한 설정이 적용되지 않은 경우 아래의 보안설정방법에 따라 설정을 변경함

■ CISCO

라우터를 자동 리부팅 하는 취약점이 존재하므로 서비스를 차단하여 방어하기를 권고함

Bootp 차단 설정

```
Router# config terminal
Router(config)# no ip bootp server
```

■ Alteon

- 스위치로 접속
- #cfg
- #sys
- #bootp disable|enable
- #apply
- #save



## 네트워크장비

### ■ Juniper

DHCP 서버 IP 주소와 서버가 연결되어있는 스위치에 대한 인터페이스 지정 옵션 제거

```
user@switch> configure
```

```
[edit]
```

```
user@switchr# edit forwarding-options helpers bootp
```

```
[edit forwarding-options helpers bootp]
```

```
user@switch# no set interface (인터페이스 포트) server (주소)
```

#### 조치 시 영향

일반적인 경우 영향 없음

## 네트워크장비

| 취약점 항목                                                                                                | 5.14. CDP 서비스 차단                                                                                                                                                                                                        |     |   |      |      |
|-------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----|---|------|------|
| 대상                                                                                                    | CISCO                                                                                                                                                                                                                   | 위험도 | 중 | Code | N-29 |
| 취약점 개요                                                                                                | CDP(Cisco Discovery Protocol)는 Cisco 제품의 관리를 목적으로 만든 프로토콜로서 같은 네트워크에 있는 장비들과 정보를 공유하고, 같은 세그먼트에 있는 다른 라우터에 IOS version, Model, device 등의 정보를 제공함.<br>이 프로토콜은 관리적인 목적으로는 많은 이점이 있지만, 보안에 대한 검증이 되지 않으므로 서비스 사용을 제한하여야 함. |     |   |      |      |
| 보안대책                                                                                                  |                                                                                                                                                                                                                         |     |   |      |      |
| 판단기준                                                                                                  | 양호: CDP 서비스가 제한되어 있는 경우                                                                                                                                                                                                 |     |   |      |      |
|                                                                                                       | 취약: CDP 서비스가 제한되어 있지 않는 경우                                                                                                                                                                                              |     |   |      |      |
| 조치방법                                                                                                  | 각 장비별 CDP 서비스 제한 설정                                                                                                                                                                                                     |     |   |      |      |
| 보안설정방법                                                                                                |                                                                                                                                                                                                                         |     |   |      |      |
| 대상 장비별 점검 방법                                                                                          |                                                                                                                                                                                                                         |     |   |      |      |
| CISCO                                                                                                 | Router# show running-config<br>Router# show cdp<br><br>1. cdp run 설정 확인<br>2. global CDP 정보 확인                                                                                                                          |     |   |      |      |
| 위에 제시한 설정이 적용되지 않은 경우 아래의 보안설정방법에 따라 설정을 변경함                                                          |                                                                                                                                                                                                                         |     |   |      |      |
| CDP를 라우터 전체에서 사용하지 못하도록 하기 위해서는 no cdp run 명령어가 사용되며, 특정 인터페이스에서 사용하지 못하도록 하려면 no cdp enable 명령어를 사용함 |                                                                                                                                                                                                                         |     |   |      |      |
| ■ CISCO                                                                                               |                                                                                                                                                                                                                         |     |   |      |      |
| Router# config terminal                                                                               |                                                                                                                                                                                                                         |     |   |      |      |
| Router(config)# no cdp run                                                                            |                                                                                                                                                                                                                         |     |   |      |      |
| Router(config)# interface FastEthernet0/1                                                             |                                                                                                                                                                                                                         |     |   |      |      |
| Router(config-if)#no cdp enable                                                                       |                                                                                                                                                                                                                         |     |   |      |      |
| 조치 시 영향                                                                                               | 일반적인 경우 영향 없음                                                                                                                                                                                                           |     |   |      |      |

## 네트워크장비

| 취약점 항목       | 5.15. Directed-broadcast 차단                                                                                                                                                               |     |   |      |      |
|--------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----|---|------|------|
| 대상           | CISCO, Alteon, Juniper, Passport                                                                                                                                                          | 위험도 | 중 | Code | N-30 |
| 취약점 개요       | Directed Broadcast는 Dos(Denial Of Service)의 일종인 *Smurf 공격에 주로 쓰이는 방식으로 목표지점에 도달하기 전까지 Unicast 방식으로 전송되다가 최종 라우터를 통과할 때 비로소 Directed Broadcast를 알아볼 수 있으므로 장치별로 이러한 패킷을 제한할 수 있도록 설정하여야 함. |     |   |      |      |
|              | *Smurf 공격: 인터넷 프로토콜(IP) 브로드캐스트나 기타 인터넷 운용 측면을 이용하여 인터넷 망을 공격하는 행위.                                                                                                                        |     |   |      |      |
| 보안대책         |                                                                                                                                                                                           |     |   |      |      |
| 판단기준         | 양호: Directed Broadcasts가 제한된 경우                                                                                                                                                           |     |   |      |      |
|              | 취약: Directed Broadcasts가 제한되지 않은 경우                                                                                                                                                       |     |   |      |      |
| 조치방법         | 각 장치별로 Directed Broadcasts 제한 설정                                                                                                                                                          |     |   |      |      |
| 보안설정방법       |                                                                                                                                                                                           |     |   |      |      |
| 대상 장비별 점검 방법 |                                                                                                                                                                                           |     |   |      |      |
| CISCO        | Router# show running-config<br>Directed-Broadcast 설정 확인                                                                                                                                   |     |   |      |      |
| Alteon       | dirbr에서 diable 설정 확인                                                                                                                                                                      |     |   |      |      |
| Juniper      | user@juniper> configure<br>[edit]<br>user@juniper# show<br>root authentication 설정을 이용하여 [edit system] 레벨에서 Directed-Broadcast 설정 확인                                                       |     |   |      |      |
| Passport     | config에서 ip directed-broadcast 설정 확인                                                                                                                                                      |     |   |      |      |

위에 제시한 설정이 적용되지 않은 경우 아래의 보안설정방법에 따라 설정을 변경함

■ CISCO

1. Smurf Attack 공격 예방

다량의 ICMP 패킷(Echo Request Packe)을 특정 네트워크나 Broadcast 주소로 보낼 때 응답 받을 패킷의 Source 주소를 공격 대상 IP로 속여 대상 호스트를 공격할 수 있음

라우터가 공격의 경로에 있으면 특정 네트워크나 Broadcast로 보내지는 ICMP 패킷을 차단하여 예방

Router# config terminal

Router(config)# acces-list 108 deny icmp any host 1.1.1.255

(1.1.1.0/24의 broadcast address인 1.1.1.255 ICMP 차단)

## 네트워크장비

```
Router(config)# access-list 108 deny icmp any host 1.1.1.0
(1.1.1.0/24 의 network address 인 1.1.1.0 ICMP 차단)
```

## 2. Directed Broadcast 차단

Cisco IOS 는 내부 사용자가 외부 네트워크의 Broadcast 주소로 요청할 수 없도록 이와 관련된 설정이 이미 Default 로 Disable 되어 있으나 낮은 버전은 직접 설정 필요

```
Router# config terminal
Router(config)# interface fastethernet 0/1
Router(config-line)# no ip directed-Broadcast.
```

## ■ Alteon

1. switch로 접속
2. # cfg/l3/frwd
3. # dirbr disable
4. # apply
5. # save

## ■ Juniper

```
user@juniper> configure
[edit]
user@juniper# no ip directed-broadcast
```

## ■ Passport

1. Switch로 접속
2. # config vlan <vid> ip directed-broadcast
3. # diable

|                |               |
|----------------|---------------|
| <b>조치 시 영향</b> | 일반적인 경우 영향 없음 |
|----------------|---------------|

## 네트워크장비

| 취약점 항목                                       | 5.16. Source 라우팅 차단                                                                                                                                                                     |     |   |      |      |
|----------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----|---|------|------|
| 대상                                           | CISCO, Juniper                                                                                                                                                                          | 위험도 | 중 | Code | N-31 |
| 취약점 개요                                       | 라우터에서 패킷의 목적지에 따라 패킷을 라우팅하는 것이 기본이지만, 때에 따라 송신 측에서 라우팅 경로 정보를 송신 데이터에 포함해 라우팅시키는 방법을 사용하는 경우가 있음. 거의 사용하지 않는 방법이지만 내부의 라우팅 경로를 파악하여 라우팅이 되지 않는 중요 서버로 접근할 수 있으므로 소스 라우팅을 기본적으로 차단하여야 함. |     |   |      |      |
| 보안대책                                         |                                                                                                                                                                                         |     |   |      |      |
| 판단기준                                         | 양호: IP Source Routing이 제한되어 있는 경우                                                                                                                                                       |     |   |      |      |
|                                              | 취약: IP Source Routing이 제한되어 있지 않은 경우                                                                                                                                                    |     |   |      |      |
| 조치방법                                         | 장치별로 IP Source Routing 제한 설정                                                                                                                                                            |     |   |      |      |
| 보안설정방법                                       |                                                                                                                                                                                         |     |   |      |      |
| 대상 장비별 점검 방법                                 |                                                                                                                                                                                         |     |   |      |      |
| CISCO                                        | Router# show running-config                                                                                                                                                             |     |   |      |      |
|                                              | ip source route 설정 확인                                                                                                                                                                   |     |   |      |      |
| Juniper                                      | user@juniper# show route                                                                                                                                                                |     |   |      |      |
|                                              | ip source route 설정 확인                                                                                                                                                                   |     |   |      |      |
| 위에 제시한 설정이 적용되지 않은 경우 아래의 보안설정방법에 따라 설정을 변경함 |                                                                                                                                                                                         |     |   |      |      |
| ■ CISCO                                      |                                                                                                                                                                                         |     |   |      |      |
| IP Source Routing 차단                         |                                                                                                                                                                                         |     |   |      |      |
| Router# config terminal                      |                                                                                                                                                                                         |     |   |      |      |
| Router(config)# no ip source-route           |                                                                                                                                                                                         |     |   |      |      |
| Router(config)# ^Z                           |                                                                                                                                                                                         |     |   |      |      |
| ■ Juniper                                    |                                                                                                                                                                                         |     |   |      |      |
| user@juniper> configure                      |                                                                                                                                                                                         |     |   |      |      |
| [edit]                                       |                                                                                                                                                                                         |     |   |      |      |
| user@juniper# no-source-route                |                                                                                                                                                                                         |     |   |      |      |
| 조치 시 영향                                      | 일반적인 경우 영향 없음                                                                                                                                                                           |     |   |      |      |

## 네트워크장비

| 취약점 항목       | 5.17. Proxy ARP 차단                                                                                                                                                                                                   |     |   |      |      |
|--------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----|---|------|------|
| 대상           | CISCO, Alteon, Juniper                                                                                                                                                                                               | 위험도 | 중 | Code | N-32 |
| 취약점 개요       | 통신을 방해하거나 가로채기를 할 수 있게 하는 ARP 프록시(Proxy) 서비스 제한 여부를 점검함. ARP 프록시는 IP와 MAC 주소의 캐시 기능을 제공하는데 악의적인 사용자가 잘못된 IP와 MAC 정보를 보내올 경우 ARP 프록시는 잘못된 정보를 보관하게 됨. 이를 통해 잘못된 IP와 MAC이 관련된 호스트에 대한 정상적인 통신을 방해하므로 ARP Proxy 차단해야 함. |     |   |      |      |
| 보안대책         |                                                                                                                                                                                                                      |     |   |      |      |
| 판단기준         | 양호: ARP Proxy 서비스가 제한되어 있는 경우                                                                                                                                                                                        |     |   |      |      |
|              | 취약: ARP Proxy 서비스가 제한되어 있지 않는 경우                                                                                                                                                                                     |     |   |      |      |
| 조치방법         | 각 장비별 ARP Proxy 서비스 제한 설정                                                                                                                                                                                            |     |   |      |      |
| 보안설정방법       |                                                                                                                                                                                                                      |     |   |      |      |
| 대상 장비별 점검 방법 |                                                                                                                                                                                                                      |     |   |      |      |
| CISCO        | Router# show running-config<br><br>각 인터페이스 정보에서 Proxy ARP 설정 확인                                                                                                                                                      |     |   |      |      |
| Alteon       | proxy diable 설정 확인                                                                                                                                                                                                   |     |   |      |      |
| Juniper      | user@juniper# show<br>proxy {<br>inet-address inet-address;<br>}<br><br>proxy로 검색하여 특정 MAC과 IP로 제한하거나 off되어 있는지 확인                                                                                                   |     |   |      |      |

위에 제시한 설정이 적용되지 않은 경우 아래의 보안설정방법에 따라 설정을 변경함

CISCO

Proxy ARP를 차단하기 위해서는 no ip proxy-arp 명령 사용

이더넷 인터페이스에 대한 적용 예

```
Router# config terminal
Router(config)# interface fastethernet 0/1
Router(config-line)# no ip proxy-arp
Router(config)# ^Z
```

Alteon

- switch 접속
- # cfg

## 네트워크장비

3. # /slb/real
4. # proxy disable
5. # apply
6. # save

#### ■ Juniper

```
user@juniper> configure
[edit]
user@juniper# delete interfaces (interface-name) unit logical - unit
-member proxy-arp
```

|                |               |
|----------------|---------------|
| <b>조치 시 영향</b> | 일반적인 경우 영향 없음 |
|----------------|---------------|

## 네트워크장비

| 취약점 항목       |                                                                                                                                                                        | 5.18. ICMP unreachable, Redirect 차단 |   |      |      |
|--------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------|---|------|------|
| 대상           | CISCO, Juniper                                                                                                                                                         | 위험도                                 | 중 | Code | N-33 |
| 취약점 개요       | ICMP unreachable 메시지에는 특정 호스트 및 게이트웨이에 패킷을 보냈을 때 어떠한 이유로 전달될 수 없는지 나타내는 코드들을 포함하고 있으므로 스캔을 통해 해당 정보가 공격자에게 유출될 수 있음.                                                   |                                     |   |      |      |
|              | ICMP Redirect는 라우터가 송신 측 호스트에 적합하지 않은 경로로 설정되어 있으면 해당 호스트에 대한 최적 경로를 다시 지정해주는 용도로 사용되지만 불필요하게 설정되어 있다면 특정 목적지로 가기 위해 고의적으로 변경하여 패킷을 가로채는 방법으로 악용될 수 있으므로 서비스를 중지하여야 함. |                                     |   |      |      |
| 보안대책         |                                                                                                                                                                        |                                     |   |      |      |
| 판단기준         | 양호: ICMP unreachable, ICMP Redirect가 차단되어 있는 경우                                                                                                                        |                                     |   |      |      |
|              | 취약: ICMP unreachable, ICMP Redirect가 차단되어 있지 않는 경우                                                                                                                     |                                     |   |      |      |
| 조치방법         | 장비의 Configuration 설정에서 ICMP Unreachables, ICMP Redirects 차단                                                                                                            |                                     |   |      |      |
| 보안설정방법       |                                                                                                                                                                        |                                     |   |      |      |
| 대상 장비별 점검 방법 |                                                                                                                                                                        |                                     |   |      |      |
| CISCO        | Router> enable<br>Router# show running<br><br>각 인터페이스별 정보에 적용된 것을 확인                                                                                                   |                                     |   |      |      |
|              | user@juniper# show<br><br>ICMP Unreachables , ICMP redirects 적용 확인                                                                                                     |                                     |   |      |      |

위에 제시한 설정이 적용되지 않은 경우 아래의 보안설정방법에 따라 설정을 변경함

■ CISCO

인터페이스에 no ip unreachables 를 실행하여 차단하면 스캔 시 소요되는 시간도 길어져 스캔 공격을 지연·차단 가능함

Router# config terminal

Router(config)# interface FastEthernet0/1 (인터페이스 선택)

Router(config-if)# no ip unreachables

RIP, OSPF 등의 프로토콜을 사용함으로써 ICMP Redirect 제거 가능

Router# config terminal

Router(config)# interface FastEthernet0/1 (인터페이스 선택)

Router(config-if)# no ip redirects

■ Juniper

ICMP 트래픽을 추적하여 옵션 지정 가능



## 네트워크장비

[edit protocols router-options]를 통하여 특정 ICMP 옵션 값 변환 가능

<> 표시 한곳에는 해당 옵션 값을 넣어주어야 함

[edit protocols router-discovery]

```
traceoptions {
 file name <replace> <size size> <files number> <no-stamp>
 <(world-readable | no-world-readable)>;
 flag flag <flag-modifier> <disable>;
}
```

ICMP 프로토콜의 트래픽을 추적하기 위한 명령어

[edit]

```
routing-options {
 traceoptions {
 file routing-log;
 }
}

protocols {
 router-discovery {
 traceoptions {
 file icmp-log;
 flag state;
 }
 }
}
```

**조치 시 영향**

특정 경로를 찾아갈 때 시간이 경과 될 수 있음

## 네트워크장비

| 취약점 항목                                                                                  | 5.19. identd 서비스 차단                                                                                                                                                                                                                                    |     |   |      |      |
|-----------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----|---|------|------|
| 대상                                                                                      | CISCO                                                                                                                                                                                                                                                  | 위험도 | 중 | Code | N-34 |
| 취약점 개요                                                                                  | identd 서비스는 클라이언트에게 접속을 요청한 사용자에게 대한 신원 확인을 위해 사용하며, 인증 데몬에 대한 응답을 받았을 경우 유효성을 체크하지 않고 전적으로 클라이언트에서 처리하므로 인증이 위조될 수 있음. identd 가 정상적으로 동작하려면 서버와 클라이언트가 모두 작동하여야 하지만 서비스보다 필터링하는 게 대부분 이므로 보안과 속도 등의 문제 해결을 위해 대규모의 집단에서 사용하지 않는다면 identd 서비스를 차단해야 함. |     |   |      |      |
| 보안대책                                                                                    |                                                                                                                                                                                                                                                        |     |   |      |      |
| 판단기준                                                                                    | 양호: identd 서비스가 차단되어 있는 경우                                                                                                                                                                                                                             |     |   |      |      |
|                                                                                         | 취약: identd 서비스가 차단되어 있지 않은 경우                                                                                                                                                                                                                          |     |   |      |      |
| 조치방법                                                                                    | identd 서비스 차단 설정                                                                                                                                                                                                                                       |     |   |      |      |
| 보안설정방법                                                                                  |                                                                                                                                                                                                                                                        |     |   |      |      |
| 대상 장비별 점검 방법                                                                            |                                                                                                                                                                                                                                                        |     |   |      |      |
| CISCO                                                                                   | Router> enable<br>Router# show running<br><br>identd 설정 확인                                                                                                                                                                                             |     |   |      |      |
| 위에 제시한 설정이 적용되지 않은 경우 아래의 보안설정방법에 따라 설정을 변경함                                            |                                                                                                                                                                                                                                                        |     |   |      |      |
| ■ CISCO                                                                                 |                                                                                                                                                                                                                                                        |     |   |      |      |
| 1. identd 기능이 필요한 경우                                                                    |                                                                                                                                                                                                                                                        |     |   |      |      |
| identd는 추적 시 검문소 역할 및 TCP 서비스 사용자 이름을 원격 사이트에 알려주는 기능을 하여 다른 사용자가 사이트에 침입 했을 경우 대응이 가능함 |                                                                                                                                                                                                                                                        |     |   |      |      |
| 실행 시키지 않는다면 수많은 기록을 살펴봐야 하기 때문에 긴 시간이 소요 될 수 있어, 자신의 시스템 구성에 따라 설정 또는, 해제할 것을 권고함       |                                                                                                                                                                                                                                                        |     |   |      |      |
| 2. identd 서비스 차단                                                                        |                                                                                                                                                                                                                                                        |     |   |      |      |
| Router# config terminal                                                                 |                                                                                                                                                                                                                                                        |     |   |      |      |
| Router(config)# no ip identd                                                            |                                                                                                                                                                                                                                                        |     |   |      |      |
| Router(config)# ^Z                                                                      |                                                                                                                                                                                                                                                        |     |   |      |      |
| 조치 시 영향                                                                                 | 일반적인 경우 영향 없음                                                                                                                                                                                                                                          |     |   |      |      |

## 네트워크장비

| 취약점 항목       | 5.20. Domain lookup 차단                                                                                             |     |   |      |      |
|--------------|--------------------------------------------------------------------------------------------------------------------|-----|---|------|------|
| 대상           | CISCO, Juniper                                                                                                     | 위험도 | 중 | Code | N-35 |
| 취약점 개요       | Domain lookup은 라우터 상에서 명령어 수행 시 오타가 발생하는 경우 그 명령어를 주위 인접 서버나 라우터에 묻게 함. 이때 속도가 저하되거나 불필요한 시간을 낭비하게 되므로 차단할 것을 권고함. |     |   |      |      |
| 보안대책         |                                                                                                                    |     |   |      |      |
| 판단기준         | 양호: Domain lookup이 차단되어 있는 경우                                                                                      |     |   |      |      |
|              | 취약: Domain lookup이 차단되어 있지 않은 경우                                                                                   |     |   |      |      |
| 조치방법         | Domain lookup 차단 설정                                                                                                |     |   |      |      |
| 보안설정방법       |                                                                                                                    |     |   |      |      |
| 대상 장비별 점검 방법 |                                                                                                                    |     |   |      |      |
| CISCO        | Router> enable<br>Router# show running 모드로 접속하여 확인                                                                 |     |   |      |      |
| Juniper      | user@juniper# show ip domain-lookup [ filter ]<br><br>no ip domain-lookup 설정 확인                                    |     |   |      |      |

위에 제시한 설정이 적용되지 않은 경우 아래의 보안설정방법에 따라 설정을 변경함

■ CISCO

Domain Lookup 차단 설정

Router# config terminal

Router(config)# no ip domain-lookup

Router(config)# ^Z

■ Juniper

user@juniper# no ip domain-lookup

user@juniper# ^Z

| 조치 시 영향 | 일반적인 경우 영향 없음 |
|---------|---------------|
|---------|---------------|

## 네트워크장비

| 취약점 항목       |                                                                                                                          | 5.21. pad 차단 |   |      |      |
|--------------|--------------------------------------------------------------------------------------------------------------------------|--------------|---|------|------|
| 대상           | CISCO, Juniper                                                                                                           | 위험도          | 중 | Code | N-36 |
| 취약점 개요       | 라우터 서비스 중 하나인 Pad는 Packet assembler/disassembler라는 뜻의 서비스로서 기계적인 패킷을 서비스 할 때 (주로 X.25 프로토콜 사용 시) 사용하므로 불필요한 경우에는 중지해야 함. |              |   |      |      |
| 보안대책         |                                                                                                                          |              |   |      |      |
| 판단기준         | 양호: pad 서비스가 차단되어 있는 경우                                                                                                  |              |   |      |      |
|              | 취약: pad 서비스가 차단되어 있지 않은 경우                                                                                               |              |   |      |      |
| 조치방법         | pad 서비스 차단 설정                                                                                                            |              |   |      |      |
| 보안설정방법       |                                                                                                                          |              |   |      |      |
| 대상 장비별 점검 방법 |                                                                                                                          |              |   |      |      |
| CISCO        | Router> enable<br>Router# show running 모드로 접속하여 확인                                                                       |              |   |      |      |
| Juniper      | user@juniper> configure<br>[edit]<br>user@juniper# show<br><br>pad 설정 확인                                                 |              |   |      |      |

위에 제시한 설정이 적용되지 않은 경우 아래의 보안설정방법에 따라 설정을 변경함

pad 차단 설정

CISCO

```
Router# config terminal
Router(config)# no service pad
Router(config)# ^Z
```

Juniper

```
user@juniper> configure
[edit]
user@juniper# no hello-padding (adaptive | loose | strict);
```

|         |               |
|---------|---------------|
| 조치 시 영향 | 일반적인 경우 영향 없음 |
|---------|---------------|

## 네트워크장비

| 취약점 항목 | 5.22. mask-rely 차단                                                                                                       |     |   |      |      |
|--------|--------------------------------------------------------------------------------------------------------------------------|-----|---|------|------|
| 대상     | CISCO, Juniper                                                                                                           | 위험도 | 중 | Code | N-37 |
| 취약점 개요 | mask-reply는 인터페이스를 통해 netmask를 요청하는 ICMP 패킷 발송 시 응답하도록 하는 설정임. mask-reply 활성화한 경우 네트워크의 netmask 정보 등이 유출될 수 있으므로 차단해야 함. |     |   |      |      |
| 보안대책   |                                                                                                                          |     |   |      |      |
| 판단기준   | 양호: mask-rely가 차단되어 있는 경우                                                                                                |     |   |      |      |
|        | 취약: mask-rely가 차단되어 있지 않은 경우                                                                                             |     |   |      |      |
| 조치방법   | mask-rely 차단 설정                                                                                                          |     |   |      |      |
| 보안설정방법 |                                                                                                                          |     |   |      |      |

| 대상 장비별 점검 방법   |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|----------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>CISCO</b>   | <p>만약 serial interface 1/0 에 no ip mask-reply 설정을 하였다면</p> <pre>Router# config terminal Router(config)# show ip interface serial1/0 (아래의 config를 볼 수 있지만 브로드 캐스트 포워딩이 다르다.) ! Directed broadcast forwarding is * disabled * &lt;- 변경후 ICMP redirects are never sent ICMP unreachable are never sent ICMP mask replies are never sent ! Directed broadcast forwarding is * enable * &lt;- 변경전 ICMP redirects are never sent ICMP unreachable are never sent ICMP mask replies are never sent !</pre> |
| <b>Juniper</b> | <pre>user@juniper&gt; configure [edit] user@juniper# show interface terse</pre>                                                                                                                                                                                                                                                                                                                                                                                                                     |

위에 제시한 설정이 적용되지 않은 경우 아래의 보안설정방법에 따라 설정을 변경함

#### ■ CISCO

reply 설정 차단

```
Router# config terminal
Router(config)# interface serial 1/0
Router(config)# no ip mask-reply
```

## 네트워크장비

## ■ Juniper

```
user@juniper> configure
```

```
[edit]
```

```
user@juniper# no ip mask-reply
```

**조치 시 영향**

일반적인 경우 영향 없음

## 네트워크장비

| 취약점 항목                                                          |                                                                                                                                                                                                | 5.23. 스위치, 허브 보안 강화 |   |      |      |
|-----------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------|---|------|------|
| 대상                                                              | 스위치, 허브                                                                                                                                                                                        | 위험도                 | 하 | Code | N-38 |
| 취약점 개요                                                          | 스위치 계층의 공격은 크게 두 가지 유형으로 분류되는데, 대체로 장비를 이용하는 공격과 트래픽 흐름을 변경하여 네트워크를 공격하는 유형으로 분류됨. 장비 공격은 스위치의 허술한 보안 설정, 관리 정책 등의 취약점을 이용한 공격이며 네트워크 공격은 스위치 계층의 통신 원리를 이용해 트래픽의 흐름을 변조하여 네트워크 통신을 마비시키는 공격임. |                     |   |      |      |
|                                                                 | 허브는 보통 연결된 모든 PC와 통신하는 데 쓰이며, 충돌이 발생하여 데이터를 서로 보내고 있다면 다른 데이터는 기다려야 하므로 속도가 느려지는 문제가 발생함.<br>허브 및 스위치의 보안 설정이 중요함.                                                                             |                     |   |      |      |
| 보안대책                                                            |                                                                                                                                                                                                |                     |   |      |      |
| 판단기준                                                            | 양호: 스위치나 허브에 보안 위협에 관한 대책이 적용되어 있는 경우                                                                                                                                                          |                     |   |      |      |
|                                                                 | 취약: 스위치나 허브에 보안 위협에 관한 대책이 적용되어 있지 않은 경우                                                                                                                                                       |                     |   |      |      |
| 조치방법                                                            | 장비별 보안 위협에 관한 대책 설정 적용                                                                                                                                                                         |                     |   |      |      |
| 보안설정방법                                                          |                                                                                                                                                                                                |                     |   |      |      |
| 대상 장비별 점검 방법                                                    |                                                                                                                                                                                                |                     |   |      |      |
| 스위치/허브                                                          | 포트 보안 설정 확인<br>Switch> enable<br>Switch# show port-security address 명령을 통해 확인                                                                                                                  |                     |   |      |      |
|                                                                 | SPAN 설정 확인<br>Switch> enable<br>Switch# show monitor 명령을 통해 확인                                                                                                                                 |                     |   |      |      |
| 위에 제시한 설정이 적용되지 않은 경우 아래의 보안설정방법에 따라 설정을 변경함                    |                                                                                                                                                                                                |                     |   |      |      |
| 스위치를 이용한 종류별 공격 위협 및 대책                                         |                                                                                                                                                                                                |                     |   |      |      |
| 1. MAC 플루딩                                                      |                                                                                                                                                                                                |                     |   |      |      |
| - 이더넷 환경에서 스니퍼를 이용한 스니핑 공격을 하여 주요 정보 유출이 될 가능성이 높음              |                                                                                                                                                                                                |                     |   |      |      |
| - MAC 플루딩 공격은 특정 호스트가 대량의 변조된 MAC 주소를 생성하기 때문에 이를 차단함           |                                                                                                                                                                                                |                     |   |      |      |
| - 포트마다 MAC 주소를 스위치에 설정하거나 수용할 수 있는 최대 MAC 주소의 개수를 제한함           |                                                                                                                                                                                                |                     |   |      |      |
| 2. ARP 스푸핑                                                      |                                                                                                                                                                                                |                     |   |      |      |
| - 스위치 장비에 의한 직접적인 공격이 아니라 트래픽의 흐름을 변경하는 공격 유형                   |                                                                                                                                                                                                |                     |   |      |      |
| - 시스코의 경우 개인 가상랜(VLAN) 기능을 이용하여 ARP 스푸핑에 대한 대책을 세울 수 있음         |                                                                                                                                                                                                |                     |   |      |      |
| 개인 가상랜은 같은 가상랜 내에서 포트 단위로 분리할 수 있는 기능으로, promiscuous / isolated |                                                                                                                                                                                                |                     |   |      |      |

## 네트워크장비

/ community의 포트 속성을 정의하여 트래픽 이동에 대한 제한이 가능함

※ 스위치 기본 보안 설정

- 정적 포트 보안 설정

(port security는 access port , trunk port, tunnel port에만 구성 가능)

Switch> enable

Switch# config terminal

Switch(config)# interface fastethernet 0/1

Switch(config-line)# switchport mode access

Switch(config-line)# switchport port-security mac-add 0050.bf1c.82d3

Switch(config-line)# switchport port-security

- Port Sticky 방식을 사용한 포트 보안 설정

Switch# config terminal

Switch(config)# interface fastethernet 0/1

Switch(config-line)# switchport port-security violation ?

(밑에 있는 명령어를 선택하여 설정)

|                                           |                                 |
|-------------------------------------------|---------------------------------|
| Protect Security violation protect mode   | (침입 시 해당 장비 접속만 차단)             |
| restrict Security violation restrict mode | (추가 로깅 메시지 발생, 보안 침해 카운터 증가)    |
| shutdown Security violation shutdown mode | (기본적인 설정이면 침해 발생 시 포트 shutdown) |

- MAC Access List 생성 및 적용

Switch# config terminal

Switch(config)# mac access-list extended mac-pc1-to-pc2

Switch(config)# deny host xxxx.xxxx.xxxx host ssss.ssss.ssss

(Mac 호스트 적용)

|                |               |
|----------------|---------------|
| <b>조치 시 영향</b> | 일반적인 경우 영향 없음 |
|----------------|---------------|



# 제어시스템 보안가이드라인

2014. 01



안전행정부 *희망의 새시대*

## 제어시스템 취약점 분석·평가 항목

| 분류      | 점검항목                                                                         | 항목<br>중요도 | 항목코드 |
|---------|------------------------------------------------------------------------------|-----------|------|
| 1. 계정관리 | 운영, 관리를 위한 계정 공유 여부                                                          | 상         | C-01 |
|         | ID/PW, 접속경로, 인증서 등 하드 코딩 사용 금지                                               | 상         | C-02 |
|         | 운영, 관리를 위한 계정의 로그인, 사용 기록 저장                                                 | 상         | C-03 |
| 2. 패치관리 | 최신 업데이트, 보안패치를 안전하게 적용하기 위한 테스트 등의 절차 수립                                     | 상         | C-04 |
| 3. 접근통제 | 제어시스템 운영자의 제한된 운영 권한(제어범위 및 제어명령) 제한                                         | 상         | C-05 |
|         | 제어시스템 인터넷, 업무망과 물리적으로 분리                                                     | 상         | C-06 |
|         | 제어 네트워크 외부와 자료 연계 시 물리적 일방향 환경을 구축                                           | 상         | C-07 |
|         | 제어 네트워크에 무선인터넷, 테더링, 외부망등 연결 제한                                              | 상         | C-08 |
|         | 제어 네트워크에 비인가 된 시스템에 대한 연결 및 접속 차단                                            | 상         | C-09 |
| 4. 보안관리 | 제어시스템 구성도, 운용 매뉴얼, 비상조치 절차서 등 현행화 관리                                         | 상         | C-10 |
|         | 제어시스템에서의 이동형 저장 매체 사용 제한 및 통제                                                | 상         | C-11 |
|         | 제어명령에 대한 위변조 방지 대책 적용                                                        | 상         | C-12 |
|         | 제어명령 replay 공격에 대한 방지 대책 적용                                                  | 상         | C-13 |
|         | 제어시스템 개발자, 운영자, 관리자에 대한 접근권한 분리                                              | 상         | C-14 |
|         | 제어시스템, 제어기기에 (vendor default) 은닉서비스 및 취약한 서비스가 없도록 설정                        | 상         | C-15 |
|         | 제어프로그램의 입력창에 비정상적인 특정값을 입력할 시 사전에 정의한 에러 메시지가 출력되도록 하여 시스템 중요정보가 노출되지 않도록 설정 | 상         | C-16 |
|         | 정보시스템에 대한 정책과 별도로 제어시스템에 대한 정보보안 정책 및 지침 수립                                  | 중         | C-17 |
|         | 비인가자 또는 인증과정이 없는 제어시스템, 제어기기에 대한 환경 설정 제한                                    | 중         | C-18 |
|         | 목적에 맞지 않는 제어시스템과 운영시스템의 기능 및 서비스 제거                                          | 중         | C-19 |
|         | 운영에 있어 사용가능한 제어명령 및 안전한 제어를 위한 파라미터의 범위 제한                                   | 중         | C-20 |
|         | 제어시스템 개선, 신규 시스템 도입, 패치 및 수정 시, 안전성을 테스트하기 위한 테스트베드 또는 시험환경 구축               | 중         | C-21 |
|         | 제어 네트워크의 세분화 및 네트워크, 시스템 간 통신 제한                                             | 중         | C-22 |

## 제어시스템

## 1. 계정관리

| 취약점 항목                                                                                                                                                                                                                                                                                                        | 1.1. 운영, 관리를 위한 계정 공유 여부                                                                                                                                      |     |   |      |      |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------|-----|---|------|------|
| 대상                                                                                                                                                                                                                                                                                                            | 제어시스템                                                                                                                                                         | 위험도 | 상 | Code | C-01 |
| 취약점 개요                                                                                                                                                                                                                                                                                                        | 제어시스템 운영기관에서 하나의 운영 계정을 교대 근무인력들이 공유하여 사용하는 경우가 많음. 계정을 공유하여 사용하는 경우 제어시스템의 오작동, 침해사고에 대한 책임 규명과 사고 조사 시 확인이 불가능 하므로 제어시스템 운영자, 관리자 각각에 유일한 계정을 부여하여 관리하여야 함. |     |   |      |      |
| 보안대책                                                                                                                                                                                                                                                                                                          |                                                                                                                                                               |     |   |      |      |
| 판단기준                                                                                                                                                                                                                                                                                                          | 양호: 운영자별 계정이 발급되어 있는 경우                                                                                                                                       |     |   |      |      |
|                                                                                                                                                                                                                                                                                                               | 취약: 공용계정으로 공유하여 사용하는 경우                                                                                                                                       |     |   |      |      |
| 조치방법                                                                                                                                                                                                                                                                                                          | 운영자, 관리자별 계정 발급 및 계정 관리 대장 작성                                                                                                                                 |     |   |      |      |
| 보안설정방법                                                                                                                                                                                                                                                                                                        |                                                                                                                                                               |     |   |      |      |
| <div>■ Windows OS</div> <div>시작&gt; 제어판&gt; 사용자 계정</div> <div>운영자, 관리자별 계정 발급 확인</div> <div>시작&gt; 제어판&gt; 사용자 계정&gt; 추가</div> <div>제어시스템 운영자, 관리자별 계정 추가</div> <div>■ UNIX OS</div> <div>1. #cat /etc/passwd</div> <div>운영자, 관리자별 계정 발급 확인</div> <div>2. #useradd 계정명</div> <div>제어시스템 운영자, 관리자별 계정 추가</div> |                                                                                                                                                               |     |   |      |      |
| 조치 시 영향                                                                                                                                                                                                                                                                                                       | 일반적으로 영향 없음                                                                                                                                                   |     |   |      |      |

## 제어시스템

| 취약점 항목                                                                                                                                                                                                                                                                                                                               | 1.2. ID/PW, 접속경로, 인증서 등 하드 코딩 사용 금지                                                                                                                                           |     |   |      |      |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----|---|------|------|
| 대상                                                                                                                                                                                                                                                                                                                                   | 제어시스템                                                                                                                                                                         | 위험도 | 상 | Code | C-02 |
| 취약점 개요                                                                                                                                                                                                                                                                                                                               | 제어시스템 개발 시 보안에 대해 고려하지 않고 설계·개발되는 경우가 많아 ID/PW, 접속경로, 인증서 등의 주요 정보를 하드 코딩하여 개발하는 경우가 있음. 하드 코딩된 주요 정보는 벤더사의 디폴트 설정으로 정보 수집이 가능하며, 디폴트 설정을 이용하여 시스템에 침입하거나 비인가 된 제어를 수행할 수 있음. |     |   |      |      |
| 보안대책                                                                                                                                                                                                                                                                                                                                 |                                                                                                                                                                               |     |   |      |      |
| 판단기준                                                                                                                                                                                                                                                                                                                                 | 양호: ID/PW, 접속경로, 인증서 등의 주요 정보가 하드 코딩되어 있지 않은 경우                                                                                                                               |     |   |      |      |
|                                                                                                                                                                                                                                                                                                                                      | 취약: ID/PW, 접속경로, 인증서 등의 주요 정보가 하드 코딩되어 있는 경우                                                                                                                                  |     |   |      |      |
| 조치방법                                                                                                                                                                                                                                                                                                                                 | 하드 코딩된 주요 정보에 대해서 코드 변경(벤더사에 소스코드 변경 요청)                                                                                                                                      |     |   |      |      |
| 보안설정방법                                                                                                                                                                                                                                                                                                                               |                                                                                                                                                                               |     |   |      |      |
| <div>- 제어시스템 매뉴얼에서 ID/PW, 접속경로 등의 중요정보를 변경할 수 없게 설정되어 있는지 확인</div> <div>- strings 등의 명령어를 이용하여 실행파일 내에 하드 코딩된 정보 확인</div> <div># strings 실행파일명</div> <div>하드 코딩된 주요 정보를 제거하고, 서비스 이용 시 운영자 인증을 위해 계정을 입력되도록 변경</div> <div>※ 제어시스템의 경우 벤더사에 의한 소스코드의 변경이 필요한 경우가 있으며, 정상적인 제어시스템 운영, 관리를 위하여 설계·개발된 경우에는 하드코딩 된 중요 정보를 제거하기 어려움</div> |                                                                                                                                                                               |     |   |      |      |
| 조치 시 영향                                                                                                                                                                                                                                                                                                                              | 하드 코딩된 ID/PW, 접속 경로, 인증서 등 주요정보 사용 불가<br>하드 코딩된 정보로 연계된 서비스 사용 불가                                                                                                             |     |   |      |      |

## 제어시스템

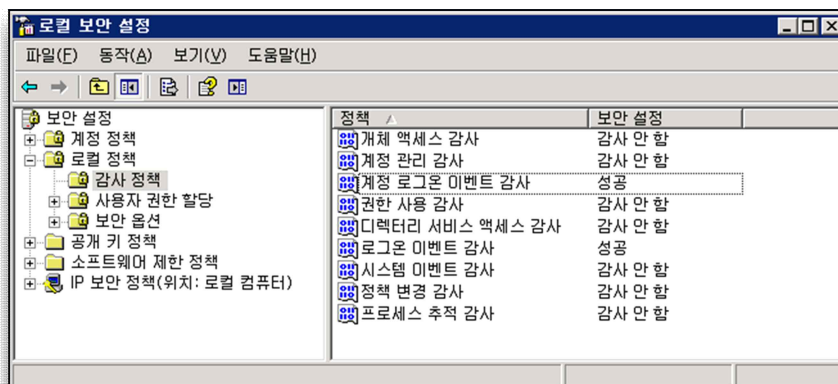
| 취약점 항목 | 1.3. 운영, 관리를 위한 계정의 로그인, 사용 기록 저장                                                                                                    |     |   |      |      |
|--------|--------------------------------------------------------------------------------------------------------------------------------------|-----|---|------|------|
| 대상     | 제어시스템                                                                                                                                | 위험도 | 상 | Code | C-03 |
| 취약점 개요 | 제어시스템의 오작동, 침해사고 발생 시 사고분석과 추적을 위해서는 제어시스템 운영 및 관리자의 계정 사용 내용을 기록하여야 함. 기록을 저장하지 않는 경우, 장애와 침해사고의 원인을 분석할 수 없어 공격자 및 공격경로를 추적하기 어려움. |     |   |      |      |
| 보안대책   |                                                                                                                                      |     |   |      |      |
| 판단기준   | 양호: 로그인 및 로그오프에 대한 감사(로그)정책이 설정되어 있는 경우                                                                                              |     |   |      |      |
|        | 취약: 로그인 및 로그오프에 대한 감사(로그)정책이 설정되어 있지 않은 경우                                                                                           |     |   |      |      |
| 조치방법   | 보안대책을 수립하여 로그를 기록하는 설정 적용                                                                                                            |     |   |      |      |
| 보안설정방법 |                                                                                                                                      |     |   |      |      |

## ■ Windows OS

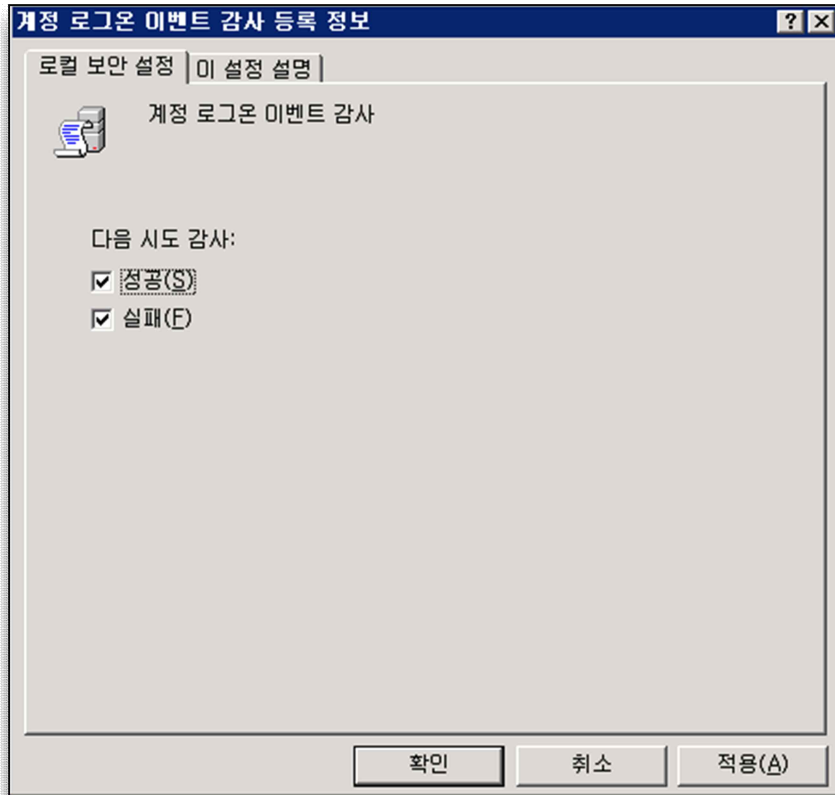
## 1. 로깅설정 및 로그파일의 로깅정보 확인

## □ Windows 2003

시작> 프로그램> 관리도구> 로컬보안정책> 보안설정> 로컬 정책> 감사 정책  
 계정 로그인 이벤트 감사> "성공", "실패" 설정



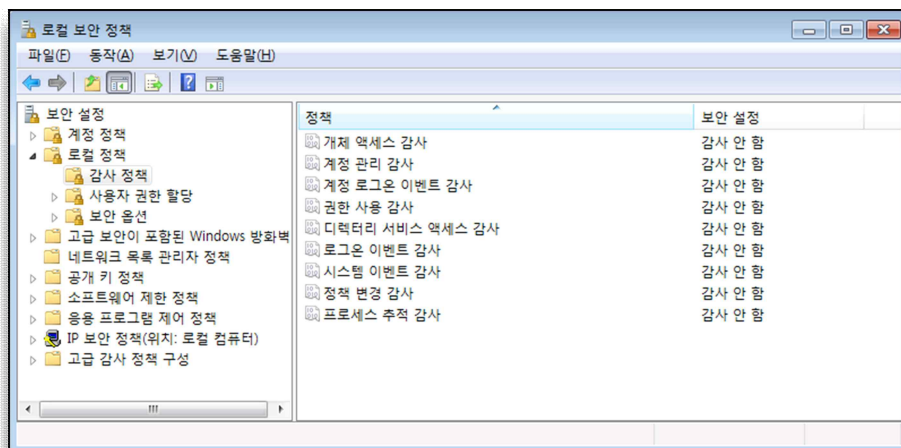
## 제어시스템



## □ Windows 7

시작 > 제어판 > 관리 도구 > 로컬 보안 정책 > 보안 설정 > 로컬 정책 > 감사 정책

- 계정 로그인 이벤트 감사 > "성공", "실패" 설정
- 권한 사용 감사 > "성공", "실패" 설정



## ■ Unix OS

1. #cat /etc/syslog.conf 파일에서 로그 설정 확인

## 제어시스템

#cat /var/adm/loginlog, authlog, sulog의 파일을 열어 로깅 정보 확인

## 2. #vi /etc/syslog.conf 파일 설정 변경

### \* 메시지 종류

auth : 로그인 등의 인증 프로그램 유형이 발생한 메시지

authpriv : 개인인증을 요구하는 프로그램 유형이 발생한 메시지

cron : cron이나 at과 같은 프로그램이 발생하는 메시지

daemon : telnetd, ftpd등과 같은 데몬이 발생한 메시지

kern : 커널이 발생한 메시지

lpr : 프린터 유형의 프로그램이 발생한 메시지

mail : 메일시스템에서 발생한 메시지

news : 유즈넷 뉴스 프로그램 유형이 발생? 메시지

syslog : syslog 프로그램 유형이 발생한 메시지

user : 사용자 프로세스

uucp : 시스템이 발생한 메시지

local0 : 여분으로 남겨둔 유형

|                |             |
|----------------|-------------|
| <b>조치 시 영향</b> | 일반적으로 영향 없음 |
|----------------|-------------|

## 제어시스템

## 2. 패치 관리

| 취약점 항목                                                                                                                                                                                                                                                                                                                                       | 2.1. 최신 업데이트, 보안패치를 안전하게 적용하기 위한 테스트 등의 절차 수립                                                                                                                                          |     |   |      |      |
|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----|---|------|------|
| 대상                                                                                                                                                                                                                                                                                                                                           | 제어시스템                                                                                                                                                                                  | 위험도 | 상 | Code | C-04 |
| 취약점 개요                                                                                                                                                                                                                                                                                                                                       | 최신 업데이트 및 보안패치는 보안 취약점을 제거하기 위해 꼭 필요하지만, 검증 없이 적용할 경우 시스템 오작동, 서비스 장애 등이 발생하여 정상적인 제어시스템 운영에 영향을 미칠 수 있음. 따라서 제어시스템 업데이트, 패치 적용 테스트, 시험운영, 유희시간 적용 테스트 등을 진행한 후 운영시스템에 적용하는 절차수립이 필요함. |     |   |      |      |
| 보안대책                                                                                                                                                                                                                                                                                                                                         |                                                                                                                                                                                        |     |   |      |      |
| 판단기준                                                                                                                                                                                                                                                                                                                                         | 양호: 제어시스템 업데이트 및 보안패치 적용 절차가 수립되어 있는 경우                                                                                                                                                |     |   |      |      |
|                                                                                                                                                                                                                                                                                                                                              | 취약: 제어시스템 업데이트 및 보안패치 적용 절차가 수립되어 있지 않은 경우                                                                                                                                             |     |   |      |      |
| 조치방법                                                                                                                                                                                                                                                                                                                                         | 제어시스템에 대한 안전한 업데이트, 보안패치 절차 수립                                                                                                                                                         |     |   |      |      |
| 보안설정방법                                                                                                                                                                                                                                                                                                                                       |                                                                                                                                                                                        |     |   |      |      |
| <div>제어시스템에 대한 안전한 업데이트, 보안패치 절차 수립</div> <div><div>- 업데이트, 보안패치에 대한 주기적 점검</div><div>- 업데이트, 보안패치에 대한 적용 전, 영향성 점검<ul style="list-style-type: none"><li>- 테스트베드를 통한 시험 적용 및 검토</li><li>- 백업 시스템에 먼저 적용하고 영향성 검토</li><li>- 제어시스템 비 운영 시간에 적용하고, 정상 동작 여부 검토</li></ul></div><div>- 업데이트, 보안패치가 문제를 일으키는 경우에 대한 복구(rollback) 대책 수립</div></div> |                                                                                                                                                                                        |     |   |      |      |
| 조치 시 영향                                                                                                                                                                                                                                                                                                                                      | 일반적으로 영향 없음                                                                                                                                                                            |     |   |      |      |



## 제어시스템

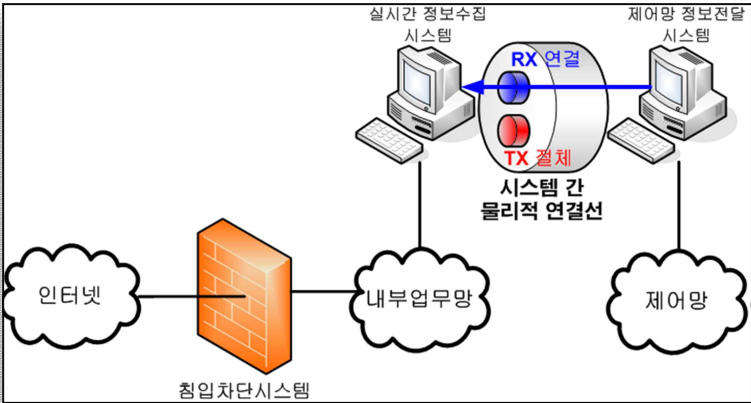
## 3. 접근 통제

| 취약점 항목                                                                                                                                                                                                                                                                | 3.1. 제어시스템 운영자의 제한된 운영 권한(제어범위 및 제어명령) 제한                                                                                                                                                                                                         |     |   |      |      |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----|---|------|------|
| 대상                                                                                                                                                                                                                                                                    | 제어시스템                                                                                                                                                                                                                                             | 위험도 | 상 | Code | C-05 |
| 취약점 개요                                                                                                                                                                                                                                                                | 제어시스템은 지리적으로 넓은 범위에 걸쳐 많은 시스템을 운영하고 있으므로 오작동 및 보안 침해 시 피해가 막대하게 발생함. 따라서 운영자가 제어 가능한 범위는 담당 기반시설로 제한하여야 하며 제어시스템의 손상, 기반시설의 피해를 일으킬 수 있는 명령들도 제한하여야 함. 이러한 제한이 적용되지 않으면 운영자는 본인의 운영 범위를 벗어난 임의의 시스템을 제어하거나 권한 이상의 제어명령을 실행할 수 있으므로 운영 권한 제한이 필요함. |     |   |      |      |
| 보안대책                                                                                                                                                                                                                                                                  |                                                                                                                                                                                                                                                   |     |   |      |      |
| 판단기준                                                                                                                                                                                                                                                                  | 양호: 계정별 운영(제어) 범위 및 명령 실행 권한이 제한되어 있는 경우                                                                                                                                                                                                          |     |   |      |      |
|                                                                                                                                                                                                                                                                       | 취약: 운영 범위 및 명령 실행 권한이 제한되어 있지 않은 경우                                                                                                                                                                                                               |     |   |      |      |
| 조치방법                                                                                                                                                                                                                                                                  | 운영자 계정에 대한 제어범위, 제어명령의 제한                                                                                                                                                                                                                         |     |   |      |      |
| 보안설정방법                                                                                                                                                                                                                                                                |                                                                                                                                                                                                                                                   |     |   |      |      |
| 1. *MMI(HMI)의 임의 운영자 계정으로 로그인하여 담당 범위 외의 시스템에 대한 제어 가능여부, 업무규정상 허용된 권한 이상의 제어명령 실행 가능 여부를 확인<br>※ 점검을 위하여 제어를 수행하거나, 권한 이상의 제어명령을 실제로 수행할 경우 심각한 결과를 초래할 수 있으므로, 제어명령 실행가능성, 접근통제 여부에 대하여 점검<br>*M(H)MI(Man(Human) Machine Interface): 작업자와 설비간의 인터페이스를 쉽고 편하게 해주는 장치 |                                                                                                                                                                                                                                                   |     |   |      |      |
| 2. 담당 범위를 벗어난 네트워크 및 시스템에 접근 여부 점검<br>- 허용된 서비스(SSH, Xwindows, Web 등)에 대하여 로그인 점검<br>- 방화벽 점검 및 운영에 필요한 타 제어시스템에 대한 접근 차단 정책을 적용                                                                                                                                      |                                                                                                                                                                                                                                                   |     |   |      |      |
| 조치 시 영향                                                                                                                                                                                                                                                               | 권한에 따라 운영자가 실행 불가능한 제어명령이 발생할 수 있음                                                                                                                                                                                                                |     |   |      |      |

## 제어시스템

| 취약점 항목                                                                                      | 3.2. 제어시스템 인터넷, 업무망과 물리적으로 분리                                                              |     |   |      |      |
|---------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------|-----|---|------|------|
| 대상                                                                                          | 제어시스템                                                                                      | 위험도 | 상 | Code | C-06 |
| 취약점 개요                                                                                      | 기반시설을 운영하고 있는 제어시스템은 침해사고 발생 시 막대한 피해가 발생하므로 외부망(인터넷) 또는 내부망(업무망)을 물리적으로 완전히 분리하여 운영하여야 함. |     |   |      |      |
| 보안대책                                                                                        |                                                                                            |     |   |      |      |
| 판단기준                                                                                        | 양호: 외부망(인터넷) 또는 내부망(업무망)과 분리하여 운영하고 있는 경우                                                  |     |   |      |      |
|                                                                                             | 취약: 외부망(인터넷) 또는 내부망(업무망)과 동일네트워크로 구성하여 운영하고 있는 경우                                          |     |   |      |      |
| 조치방법                                                                                        | 제어시스템 운영망과 업무망 분리 및 인터넷 차단                                                                 |     |   |      |      |
| 보안설정방법                                                                                      |                                                                                            |     |   |      |      |
| 1. 제어시스템 네트워크 구성도를 검토하여 물리적인 분리가 이뤄졌는지 확인하고, 네트워크 장비, 방화벽의 정책을 기술적으로 분석하여 실제로 분리되어 운영되는지 확인 |                                                                                            |     |   |      |      |
| 2. 제어시스템 운영에 인터넷, 업무망과의 연계가 필수적이지 않은 경우 제어 네트워크를 물리적으로 분리하여 구성                              |                                                                                            |     |   |      |      |
| - 국가정보원에서 배포한 “전자제어시스템 보안가이드라인” 3장 2절 “제어 네트워크의 물리적 망분리” 참조                                 |                                                                                            |     |   |      |      |
| - 제어시스템 운영에 외부망 연결이 필수적인 경우에는 3장 3절 “안전한 제어 네트워크 연동 기법” 참조                                  |                                                                                            |     |   |      |      |
| 조치 시 영향                                                                                     | 업무망에서 인터넷 사용 불가                                                                            |     |   |      |      |

## 제어시스템

| 취약점 항목                                                                                         | 3.3. 제어 네트워크 외부와 자료 연계 시 물리적 일방향 환경을 구축                                                                                                            |     |   |      |      |
|------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------|-----|---|------|------|
| 대상                                                                                             | 제어시스템                                                                                                                                              | 위험도 | 상 | Code | C-07 |
| 취약점 개요                                                                                         | 제어 네트워크는 외부망(인터넷), 내부망(업무망)과 물리적으로 분리하여야 하지만 외부망과 자료 연계 시에는 물리적 일방향 환경을 구축하여 필요한 자료를 연계하여야 함. 일방향 환경이 구축되지 않는다면 외부로부터 내부로의 접근과 침입을 근본적으로 차단할 수 없음. |     |   |      |      |
| 보안대책                                                                                           |                                                                                                                                                    |     |   |      |      |
| 판단기준                                                                                           | 양호: 독립적 네트워크로 구성되어 있거나, 제어시스템 네트워크와 외부연계 지점이 일방향 환경으로 구축되어 있는 경우                                                                                   |     |   |      |      |
|                                                                                                | 취약: 제어시스템 네트워크와 업무망 네트워크가 분리되어 있지 않거나, 제어시스템 네트워크와 외부연계 네트워크의 차단 정책이 적용되어 있지 않은 경우                                                                 |     |   |      |      |
| 조치방법                                                                                           | 외부망과 자료 연계 시 물리적 일방향 시스템 적용 설정                                                                                                                     |     |   |      |      |
| 보안설정방법                                                                                         |                                                                                                                                                    |     |   |      |      |
| 1. 제어시스템 네트워크 구성도를 검토하여 외부망 연계지점이 일원화 되어 있으며, 해당 연계구간이 물리적 일방향 시스템을 통하여 연계되어 있는지 확인            |                                                                                                                                                    |     |   |      |      |
| 2. 제어시스템 운영에 인터넷, 업무망과의 연계가 필수적인 경우 물리적 일방향 시스템 적용                                             |                                                                                                                                                    |     |   |      |      |
| - 랜, 시리얼 라인의 외부망→ 제어 네트워크로의 TX-RX 라인 절체                                                        |                                                                                                                                                    |     |   |      |      |
| <div></div> |                                                                                                                                                    |     |   |      |      |
| - 물리적 일방향 시스템 적용                                                                               |                                                                                                                                                    |     |   |      |      |
| 조치 시 영향                                                                                        | 내부망과 인터넷망 자료 연계 제한                                                                                                                                 |     |   |      |      |

제어시스템

| 취약점 항목                                                | 3.4. 제어 네트워크에 무선인터넷, 테더링, 외부망등 연결 제한                                                                                                        |     |   |      |      |
|-------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------|-----|---|------|------|
| 대상                                                    | 제어시스템                                                                                                                                       | 위험도 | 상 | Code | C-08 |
| 취약점 개요                                                | 무선인터넷, 테더링(tethering), 외부 유선망 연결 등을 통해 제어 네트워크가 외부와 연결될 수 있으므로 이를 제한하고 점검하여야 함. 외부망에 연결된 노트북, 휴대폰 등이 제어 네트워크와 연결된다면 해당 경로를 통해 직접적인 침입이 가능함. |     |   |      |      |
| 보안대책                                                  |                                                                                                                                             |     |   |      |      |
| 판단기준                                                  | 양호: 제어 시설에 비인가 장비에 대한 반입이 불가능 하며, 제어 네트워크에서 외부로 연결이 되지 않은 경우                                                                                |     |   |      |      |
|                                                       | 취약: 제어 시설에 비인가 장비에 대한 반입에 대한 통제가 이루어지지 않거나, 제어 네트워크에서 외부로 연결이 되는 경우                                                                         |     |   |      |      |
| 조치방법                                                  | 외부 연계 접점 차단(외부 연계일 경우 물리적 일방향 시스템 적용)                                                                                                       |     |   |      |      |
| 보안설정방법                                                |                                                                                                                                             |     |   |      |      |
| 제어 네트워크를 외부망과 물리적으로 분리 또는 물리적 일방향 시스템을 통하여 외부망과 연계함   |                                                                                                                                             |     |   |      |      |
| 1. 제어 네트워크 내부에서 외부 인터넷 사이트 접속 여부 점검                   |                                                                                                                                             |     |   |      |      |
| - 웹브라우저에서 인터넷 포털사이트 등 연결 점검                           |                                                                                                                                             |     |   |      |      |
| - #ping 외부 IP                                         |                                                                                                                                             |     |   |      |      |
| 2. Wifi 등의 무선네트워크 점검                                  |                                                                                                                                             |     |   |      |      |
| - 무선AP, 무선네트워크 전파 스캐너를 사용하여 점검                        |                                                                                                                                             |     |   |      |      |
| - 노트북 등을 이용하여 "무선네트워크 보기"를 실행하여 점검                    |                                                                                                                                             |     |   |      |      |
| 3. 제어 네트워크 내의 패킷을 스니핑(Sniffing)하여 외부 통신 패킷 여부 검토      |                                                                                                                                             |     |   |      |      |
| - Wireshark 등의 패킷 스니핑 도구를 이용하여 패킷 분석                  |                                                                                                                                             |     |   |      |      |
| 4. 제어 네트워크를 외부망과 물리적으로 분리 또는 물리적 일방향 시스템을 통하여 외부망과 연계 |                                                                                                                                             |     |   |      |      |
| 조치 시 영향                                               | 제어시스템 네트워크와 인터넷 연계 제한                                                                                                                       |     |   |      |      |

## 제어시스템

| 취약점 항목                                                                                                | 3.5. 제어 네트워크에 비인가 된 시스템에 대한 연결 및 접속 차단                                                                                             |     |   |      |      |
|-------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------|-----|---|------|------|
| 대상                                                                                                    | 제어시스템                                                                                                                              | 위험도 | 상 | Code | C-09 |
| 취약점 개요                                                                                                | 제어시스템은 지리적으로 널리 분포된 지역에 구축되기 때문에, 네트워크에 대한 물리적인 접근을 차단하기 어려움. 따라서 비인가자가 제어 네트워크에 연결하여 시스템에 접근하는 것을 차단할 수 있는 *NAC 등의 보안대책을 적용하여야 함. |     |   |      |      |
|                                                                                                       | *NAC(Network Access Control): 네트워크에 접근하기 전에 보안 정책을 준수했는지 여부를 검사해 네트워크 접속을 통제함.                                                     |     |   |      |      |
| 보안대책                                                                                                  |                                                                                                                                    |     |   |      |      |
| 판단기준                                                                                                  | 양호: 제어시스템 네트워크에 대한 접근 차단 정책이 설정되어 있는 경우                                                                                            |     |   |      |      |
|                                                                                                       | 취약: 제어시스템 네트워크에 대한 접근 차단 정책이 설정되어 있지 않은 경우                                                                                         |     |   |      |      |
| 조치방법                                                                                                  | 제어시스템 네트워크 접근 차단 정책(ACL) 설정 및 접근 통제                                                                                                |     |   |      |      |
| 보안설정방법                                                                                                |                                                                                                                                    |     |   |      |      |
| 1. 등록된 제어시스템에 대한 접근통제 정책 설정(제어시스템 MAC 등록 관리)<br>2. NAC 등의 보안솔루션을 적용하여 제어 네트워크 임의 접속 장비에 대한 네트워크 접근 차단 |                                                                                                                                    |     |   |      |      |
| 조치 시 영향                                                                                               | 비인가 시스템의 제어 네트워크 접근 제한                                                                                                             |     |   |      |      |

## 제어시스템

## 4. 보안 관리

| 취약점 항목                                                                                                                                                                                                                                                                                                                                            | 4.1. 제어시스템 구성도, 운용 매뉴얼, 비상조치 절차서 등 현행화 관리                                                                                                                                  |     |   |      |      |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----|---|------|------|
| 대상                                                                                                                                                                                                                                                                                                                                                | 제어시스템                                                                                                                                                                      | 위험도 | 상 | Code | C-10 |
| 취약점 개요                                                                                                                                                                                                                                                                                                                                            | 제어시스템의 장애와 사이버 침해사고에 대한 신속한 대응을 위해서는 정확한 제어 시스템 현황과 네트워크 구성도, 운용매뉴얼, 비상조치 절차서를 갖춰야 함. 해당 문서들은 제어시스템에 대한 중요정보를 포함하고 있으므로 대외비 이상으로 관리하여야 하며, 비상시 신속하게 활용할 수 있도록 절차를 마련하여야 함. |     |   |      |      |
|                                                                                                                                                                                                                                                                                                                                                   | 제어시스템에 대한 현황과 정보가 정확하지 않은 경우, 장애 및 침해사고에 대한 분석과 대응이 실제와 달라 제어시스템 운영에 악영향을 미칠 수 있으며, 해당 문서들에 대한 관리가 소홀한 경우 제어시스템 중요정보가 유출될 수 있음.                                            |     |   |      |      |
| 보안대책                                                                                                                                                                                                                                                                                                                                              |                                                                                                                                                                            |     |   |      |      |
| 판단기준                                                                                                                                                                                                                                                                                                                                              | 양호: 제어시스템 현황, 구성도, 운영 매뉴얼, 비상조치 절차서를 최신화하여 갖춰져 있는 경우                                                                                                                       |     |   |      |      |
|                                                                                                                                                                                                                                                                                                                                                   | 취약: 제어시스템 현황, 구성도, 운영 매뉴얼, 비상조치 절차서가 구비되어 있지 않은 경우                                                                                                                         |     |   |      |      |
| 조치방법                                                                                                                                                                                                                                                                                                                                              | 제어시스템을 유형별로 분류하여 비상시 신속하게 활용될 수 있도록 절차 마련                                                                                                                                  |     |   |      |      |
| 보안설정방법                                                                                                                                                                                                                                                                                                                                            |                                                                                                                                                                            |     |   |      |      |
| <div>1. 제어시스템 현황, 구성도, 운영 매뉴얼, 비상조치 절차서 확인</div> <div>- 구비된 현황, 구성도, 문서가 현재의 제어시스템과 일치하는지 검토</div> <div>- 해당 문서는 제어시스템에 대한 중요정보를 포함하고 있으므로, 문서의 비밀관리에 대한 사항 점검</div> <div>2. 유형별 제어시스템 분류 및 일련번호를 부여하여 관련 현황 파악 및 관리</div> <div>- 제어시스템 네트워크에 대한 구성도를 최신으로 파악하여 관리</div> <div>- 운영매뉴얼, 비상조치 절차서를 수립하여 활용</div> <div>- 해당문서에 대하여 대외비 이상으로 관리</div> |                                                                                                                                                                            |     |   |      |      |
| 조치 시 영향                                                                                                                                                                                                                                                                                                                                           | 일반적으로 영향 없음                                                                                                                                                                |     |   |      |      |

## 제어시스템

| 취약점 항목                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               | 4.2. 제어시스템에서의 이동형 저장 매체 사용 제한 및 통제                                                                                                                                                                                                |     |   |      |      |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----|---|------|------|
| 대상                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   | 제어시스템                                                                                                                                                                                                                             | 위험도 | 상 | Code | C-11 |
| 취약점 개요                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               | 비인가자가 제어시스템에 접근하여 USB 저장매체를 이용해 정보를 유출하거나 악의적으로 외부 파일을 실행하여 장애를 일으킬 수 있으므로 필수적인 경우가 아니라면 이동형 저장 매체 사용을 제한하여야 함. 제어시스템에 대한 네트워크 접근이 엄격하게 통제되는 가운데 USB를 통한 제어시스템 공격이 대두되고 있으므로 저장매체 포트 비활성화, 인가된 사용자만 사용, 자동실행 방지 등의 보안대책을 적용하여야 함. |     |   |      |      |
| 보안대책                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |                                                                                                                                                                                                                                   |     |   |      |      |
| 판단기준                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 | 양호: 이동형 저장 매체에 대한 통제가 이루어지고 있는 경우<br>취약: 이동형 저장 매체에 대한 통제가 이루어지고 있지 않은 경우                                                                                                                                                         |     |   |      |      |
| 조치방법                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 | 이동형 저장 매체에 대한 물리적 차단, 인가된 이동형 저장 매체에 대한 통제                                                                                                                                                                                        |     |   |      |      |
| 보안설정방법                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |                                                                                                                                                                                                                                   |     |   |      |      |
| 1. 제어시스템의 USB 포트를 물리적 차단, 또는 시건<br>시스템 관리 등의 목적으로 필요한 경우 지정된 사용자 및 인가된 장치만 사용                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |                                                                                                                                                                                                                                   |     |   |      |      |
| <div><div><p>(A) 보안스티커를 통한 USB 봉인</p></div><div><p>(B) USB 포트 잠금 장치를 이용한 봉인</p></div><div><p>(C) 잠금 장치가 구비된 USB 포트 모듈</p></div><div><p>(D) 연결된 USB 장치 잠금(예)</p></div></div> <p>&lt;USB 포트 물리적 차단 예&gt;</p> |                                                                                                                                                                                                                                   |     |   |      |      |
| 2. USB 보안통제 솔루션을 도입(도입 및 적용이 가능한 경우)<br>※ 제어시스템에 대한 보안솔루션 도입 시, 반드시 보안성 검토 필요                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |                                                                                                                                                                                                                                   |     |   |      |      |
| <div>- 제어시스템 USB 포트의 물리적 차단, USB 보안통제 솔루션 도입</div> <div>- 안전하게 포맷된 USB 메모리를 허용된 USB포트에 삽입하여 인식·사용 여부 확인</div> <div>※ USB 보안통제 솔루션이 도입된 경우에 점검(제어시스템 영향성으로 USB 보안통제 솔루션 도입을 강제할 수 없음, 단 미도입시 관리·절차적인 보안대책 수립에 대하여 점검)</div>                                                                                                                                                                                                                                                                                                                           |                                                                                                                                                                                                                                   |     |   |      |      |
| 조치 시 영향                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              | 제어시스템 USB, CD/DVD 등 사용 제한                                                                                                                                                                                                         |     |   |      |      |

## 제어시스템

| 취약점 항목                                                                                                                                                                                                                                                                                                                 | 4.3. 제어명령에 대한 위변조 방지 대책 적용                                                                                                                                                |     |   |      |      |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----|---|------|------|
| 대상                                                                                                                                                                                                                                                                                                                     | 제어시스템                                                                                                                                                                     | 위험도 | 상 | Code | C-12 |
| 취약점 개요                                                                                                                                                                                                                                                                                                                 | 일반적으로 제어시스템은 보안을 고려하지 않고 설계·개발되는 경우가 많아 제어명령을 평문으로 전송하거나, 인증 없이 명령을 수행하는 등의 취약점이 존재함. 따라서 제어명령에 대한 무결성 점검, 암호화, 인증 등의 보안대책을 적용하여 비인가자의 위·변조 공격으로 제어시스템을 장악하는 위험을 방지하여야 함. |     |   |      |      |
| 보안대책                                                                                                                                                                                                                                                                                                                   |                                                                                                                                                                           |     |   |      |      |
| 판단기준                                                                                                                                                                                                                                                                                                                   | 양호: 전송되는 제어명령에 보안 설정이 적용되어 있는 경우                                                                                                                                          |     |   |      |      |
|                                                                                                                                                                                                                                                                                                                        | 취약: 전송되는 제어명령에 보안 설정이 적용되어 있지 않은 경우                                                                                                                                       |     |   |      |      |
| 조치방법                                                                                                                                                                                                                                                                                                                   | 사용자 인증 절차 수립 및 전송되는 정보를 암호화 하는 설정 적용                                                                                                                                      |     |   |      |      |
| 보안설정방법                                                                                                                                                                                                                                                                                                                 |                                                                                                                                                                           |     |   |      |      |
| 1. 전송되는 제어명령을 스니핑(Sniffing)하여 암호화, 무결성 체크 등의 위·변조 방지대책과 제어명령의 전송과 실행과정에 인증을 수행하는지 검토<br>- 스니핑된 제어명령 위·변조하고 이를 다시 전송하여, 해당 명령이 실행되는지 확인할 수도 있음<br>- 다만 이러한 점검은 실제로 운영되는 제어시스템에서 수행될 경우 매우 위험하므로, 테스트베드 등을 통하여 분석되어야 함<br>※ 제어명령 위·변조에 대한 점검은 시스템 오작동, 장애 등의 높은 위험을 수반하므로, 암호화 여부, 무결성 체크, 인증 과정 여부를 점검하여 간접적으로 분석할 수 있음 |                                                                                                                                                                           |     |   |      |      |
| 2. 제어명령 전송 시, 인증 과정을 수행하도록 설정<br>- 제어명령의 암호화, 무결성 체크를 통하여 위·변조에 안전하도록 제어시스템을 수정하여야 함<br>※ 벤더사에 의한 제어시스템 수정, 개선이 필요하며, 정상적인 제어시스템 운영에 많은 영향을 미칠 수 있음                                                                                                                                                                    |                                                                                                                                                                           |     |   |      |      |
| 조치 시 영향                                                                                                                                                                                                                                                                                                                | 일반적으로 영향 없음                                                                                                                                                               |     |   |      |      |



## 제어시스템

| 취약점 항목                                                                                                                                                                                                                                                                                                                                                                                                    | 4.4. 제어명령 replay 공격에 대한 방지 대책 적용                                                                                                                        |     |   |      |      |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------|-----|---|------|------|
| 대상                                                                                                                                                                                                                                                                                                                                                                                                        | 제어시스템                                                                                                                                                   | 위험도 | 상 | Code | C-13 |
| 취약점 개요                                                                                                                                                                                                                                                                                                                                                                                                    | 일반적으로 제어시스템은 보안을 고려하지 않고 설계·개발되는 경우가 많아 제어명령을 재전송하는 경우 인증 없이 실행하는 취약점이 존재함. 공격자가 네트워크를 통하여 전송되는 제어명령을 스니핑(Sniffing)하여 저장한 후, 재전송하여 제어시스템을 임의로 제어할 수 있음. |     |   |      |      |
| 보안대책                                                                                                                                                                                                                                                                                                                                                                                                      |                                                                                                                                                         |     |   |      |      |
| 판단기준                                                                                                                                                                                                                                                                                                                                                                                                      | 양호: 재전송되는 제어명령에 보안설정이 적용되어 있는 경우                                                                                                                        |     |   |      |      |
|                                                                                                                                                                                                                                                                                                                                                                                                           | 취약: 재전송되는 제어명령에 보안설정이 적용되어 있지 않은 경우                                                                                                                     |     |   |      |      |
| 조치방법                                                                                                                                                                                                                                                                                                                                                                                                      | 사용자 인증 절차 수립 및 전송되는 정보를 암호화 하는 설정 적용                                                                                                                    |     |   |      |      |
| 보안설정방법                                                                                                                                                                                                                                                                                                                                                                                                    |                                                                                                                                                         |     |   |      |      |
| <p>1. 전송되는 제어명령을 스니핑(Sniffing)하여 저장하고, 이를 다시 네트워크에 전송하여 해당 제어명령이 수행되는지 점검</p> <p>※ 제어명령 재전송 취약점에 대한 점검은 시스템 오작동, 장애 등의 높은 위험을 수반하므로 테스트베드 등을 통하여 수행하여야 하며, 제어명령에 대한 인증절차, 세션키, Time Stamp 등의 보안대책을 검토하여 간접적으로 분석할 수 있음</p> <p>2. 제어명령 전송 시, 인증 과정을 수행</p> <p>- 제어명령의 인증, 세션키 확인, Time Stamp 확인 등을 통하여 재전송 공격에 안전하도록 제어시스템을 수정하여야 함</p> <p>※ 벤더사에 의한 제어시스템 수정, 개선이 필요하며, 정상적인 제어시스템 운영에 많은 영향을 미칠 수 있음</p> |                                                                                                                                                         |     |   |      |      |
| 조치 시 영향                                                                                                                                                                                                                                                                                                                                                                                                   | 일반적으로 영향 없음                                                                                                                                             |     |   |      |      |

## 제어시스템

| 취약점 항목                                                                                                                                                                                                        | 4.5. 제어시스템 개발자, 운영자, 관리자에 대한 접근권한 분리                                                                                                   |     |   |      |      |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------|-----|---|------|------|
| 대상                                                                                                                                                                                                            | 제어시스템                                                                                                                                  | 위험도 | 상 | Code | C-14 |
| 취약점 개요                                                                                                                                                                                                        | 관리자는 제어시스템의 접근권한을 개발자, 운영자, 관리자 등 각 업무에 따라 최소한으로 부여하여야 함. 개발자 운영자에 대한 접근권한을 분리·제한하지 않을 경우 개발자에 의한 비인가 제어, 운영자에 의한 제어시스템 관리 기능 접근이 가능함. |     |   |      |      |
| 보안대책                                                                                                                                                                                                          |                                                                                                                                        |     |   |      |      |
| 판단기준                                                                                                                                                                                                          | 양호: 업무 및 권한에 따라 수행할 수 있는 권한과 기능을 분리한 경우                                                                                                |     |   |      |      |
|                                                                                                                                                                                                               | 취약: 업무 및 권한에 따라 수행할 수 있는 권한과 기능을 분리하지 않은 경우                                                                                            |     |   |      |      |
| 조치방법                                                                                                                                                                                                          | 제어시스템 개발자, 운영자, 관리자 등 업무별 계정에 따라 권한을 분리하여 설정                                                                                           |     |   |      |      |
| 보안설정방법                                                                                                                                                                                                        |                                                                                                                                        |     |   |      |      |
| 1. 개발자, 운영자, 관리자별로 별도의 계정이 부여되었고 해당 계정별로 권한을 분리하여 운영하는지 확인<br>- 제어시스템 계정 확인<br>#cat /etc/passwd<br>- 확인된 계정이 개발자, 운영자, 관리자별로 구분되어 발급되었는지 확인<br>- 각 계정의 권한 및 그룹 확인(관리자 권한 및 관리자 그룹 포함 여부 등)<br>#cat /etc/group |                                                                                                                                        |     |   |      |      |
| 2. 각 계정에 대한 그룹 분리<br>#usermod -g 바꿀 GID ID                                                                                                                                                                    |                                                                                                                                        |     |   |      |      |
| 조치 시 영향                                                                                                                                                                                                       | 계정에 따라 명령어 실행 제한                                                                                                                       |     |   |      |      |

## 제어시스템

| 취약점 항목                                                                                                                                                                                                                                                                                                                                                            | 4.6. 제어시스템, 제어기기에 (vendor default) 은닉서비스 및 취약한 서비스가 없도록 설정                                                                         |     |   |      |      |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------|-----|---|------|------|
| 대상                                                                                                                                                                                                                                                                                                                                                                | 제어시스템                                                                                                                              | 위험도 | 상 | Code | C-15 |
| 취약점 개요                                                                                                                                                                                                                                                                                                                                                            | 제어시스템, 제어기기의 유지보수를 위해 인증과정이 없는 tftp와 평문 통신을 하는 telnet 등의 서비스는 벤더사에 의해 은닉되어 존재함. 이 서비스들은 공격자의 침입 경로 및 백도어로 활용될 수 있기 때문에 이를 제거하여야 함. |     |   |      |      |
| 보안대책                                                                                                                                                                                                                                                                                                                                                              |                                                                                                                                    |     |   |      |      |
| 판단기준                                                                                                                                                                                                                                                                                                                                                              | 양호: 불필요하게 은닉된 서비스가 제거된 경우                                                                                                          |     |   |      |      |
|                                                                                                                                                                                                                                                                                                                                                                   | 취약: 불필요하게 은닉된 서비스가 제거되어 있지 않은 경우                                                                                                   |     |   |      |      |
| 조치방법                                                                                                                                                                                                                                                                                                                                                              | 불필요한 서비스 제거 및 접근제한 설정                                                                                                              |     |   |      |      |
| 보안설정방법                                                                                                                                                                                                                                                                                                                                                            |                                                                                                                                    |     |   |      |      |
| <div>■ Windows OS</div> <div>시작&gt; 설정&gt; 제어판&gt; 서비스에서 불필요한 서비스를 선택하여 중지<br/>(시작옵션에서 시작유형을 "사용안함"으로 설정)</div> <div>시작&gt; 설정&gt; 제어판&gt; 방화벽설정에서 접근 가능한 IP 제한</div> <div>■ Unix OS</div> <div>#vi /etc/inetd.conf 파일에서 불필요한 서비스 주석(#) 처리하여, 해당 서비스 비활성화</div> <div>#/etc/hosts.allow에 접근 가능한 서비스, IP 지정</div> <div>#/etc/hosts.deny에서 차단하고자 하는 서비스, IP 지정</div> |                                                                                                                                    |     |   |      |      |
| 조치 시 영향                                                                                                                                                                                                                                                                                                                                                           | 일반적으로 영향 없음                                                                                                                        |     |   |      |      |

## 제어시스템

|                                                                                                          |                                                                                                                                       |     |   |      |      |
|----------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------|-----|---|------|------|
| 취약점 항목                                                                                                   | 4.7. 제어프로그램의 입력창에 비정상적인 특정값을 입력할 시 사전에 정의한 에러 메시지가 출력되도록 하여 시스템 중요정보가 노출되지 않도록 설정                                                     |     |   |      |      |
| 대상                                                                                                       | 제어시스템                                                                                                                                 | 위험도 | 상 | Code | C-16 |
| 취약점 개요                                                                                                   | 제어시스템 소프트웨어 설계 시 에러 처리 미흡으로 인하여 제어시스템의 취약점 및 정보가 노출될 수 있으며 이러한 정보가 노출된다면 제어시스템의 침투, 획득한 정보를 이용한 연계공격에 필요한 정보를 공격자가 수집하는 데 도움이 될 수 있음. |     |   |      |      |
| 보안대책                                                                                                     |                                                                                                                                       |     |   |      |      |
| 판단기준                                                                                                     | 양호: 에러 발생 시 시스템 정보가 노출되지 않으며 에러 페이지가 별도로 지정되어 있는 경우                                                                                   |     |   |      |      |
|                                                                                                          | 취약: 에러 발생 시 시스템 정보가 노출되는 경우                                                                                                           |     |   |      |      |
| 조치방법                                                                                                     | 발생 가능한 각 에러에 대해 별도의 에러 페이지를 지정                                                                                                        |     |   |      |      |
| 보안설정방법                                                                                                   |                                                                                                                                       |     |   |      |      |
| 1. 제어 프로그램은 품질 및 기술검토활동을 통하여 단위테스트, 통합테스트, 시스템테스트 및 인수테스트 등을 실시함으로써 에러를 최소화하고 성능의 검증 및 테스트가 완료된 프로그램을 사용 |                                                                                                                                       |     |   |      |      |
| 2. 제어 프로그램 에러 발생 시, 사전에 정의된 에러코드 또는 에러 메시지를 출력하여 에러를 처리하고 시스템의 주요 정보노출을 최소화                              |                                                                                                                                       |     |   |      |      |
| 조치 시 영향                                                                                                  | 일반적으로 영향 없음                                                                                                                           |     |   |      |      |

## 제어시스템

| 취약점 항목                                                                                                                                                                                                          | 4.8. 정보시스템에 대한 정책과 별도로 제어시스템에 대한 정보보안 정책 및 지침 수립                                                                                                                                                                             |     |   |      |      |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----|---|------|------|
| 대상                                                                                                                                                                                                              | 제어시스템                                                                                                                                                                                                                        | 위험도 | 중 | Code | C-17 |
| 취약점 개요                                                                                                                                                                                                          | 제어시스템은 정보시스템과 다른 보안요소 및 특성, 침해시의 높은 파급효과를 지니므로 이를 반영하여 보다 엄격하고 차별화된 정보보안 정책, 지침을 수립하여야 함. 또한 일반적인 IT시스템에 대한 보안정책이 제어시스템의 운영에 영향을 미치는 경우가 존재함. 예를 들어 신속한 업데이트, 보안패치의 적용이 제어시스템에 대한 영향 검토 없이 수행된 경우 제어시스템 오작동과 중지 발생 가능성이 존재함. |     |   |      |      |
|                                                                                                                                                                                                                 | ※ 정보시스템: C(Confidentiality) > I(Integrity) > A(Availability)<br>제어시스템: A(Availability) > I(Integrity) > C(Confidentiality)                                                                                                   |     |   |      |      |
| 보안대책                                                                                                                                                                                                            |                                                                                                                                                                                                                              |     |   |      |      |
| 판단기준                                                                                                                                                                                                            | 양호: 제어시스템에 특화된 보안정책이 별도로 수립되어 있는 경우                                                                                                                                                                                          |     |   |      |      |
|                                                                                                                                                                                                                 | 취약: 제어시스템에 특화된 보안정책이 수립되어 있지 않은 경우                                                                                                                                                                                           |     |   |      |      |
| 조치방법                                                                                                                                                                                                            | 제어시스템에 특화된 보안정책을 별도로 수립                                                                                                                                                                                                      |     |   |      |      |
| 보안설정방법                                                                                                                                                                                                          |                                                                                                                                                                                                                              |     |   |      |      |
| 1. 조직, IT시스템 전반에 대한 보안정책 외에 제어시스템에 특화된 보안정책이 별도로 수립되어 있는지 점검<br>- 기존 보안정책에 제어시스템에 대한 별도 항목, 제어시스템 특성에 따른 정책이 있는지 점검<br>2. 제어시스템의 보안요구사항 식별<br>- 제어시스템 보안요구사항을 반영한 별도의 보안정책을 수립<br>- 기존 보안정책을 제어시스템의 특성을 반영하여 개선 |                                                                                                                                                                                                                              |     |   |      |      |
| 조치 시 영향                                                                                                                                                                                                         | 일반적으로 영향 없음                                                                                                                                                                                                                  |     |   |      |      |

## 제어시스템

|                                                                                                                                                                                                                                                                                                                           |                                                                                                                                                                           |     |   |      |      |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----|---|------|------|
| 취약점 항목                                                                                                                                                                                                                                                                                                                    | 4.9. 비인가자 또는 인증과정이 없는 제어시스템, 제어기기에 대한 환경 설정 제한                                                                                                                            |     |   |      |      |
| 대상                                                                                                                                                                                                                                                                                                                        | 제어시스템                                                                                                                                                                     | 위험도 | 중 | Code | C-18 |
| 취약점 개요                                                                                                                                                                                                                                                                                                                    | 일반적으로 제어시스템은 보안을 고려하지 않고 설계·개발되는 경우가 많아 시스템 운영에 영향을 미치는 환경 설정, 중요 파라미터 설정 시 로그인, 인증 절차 없이 수행하는 경우가 존재함. 제어시스템에 대한 환경설정이 비인가자에 의해서 임의로 변경되는 경우, 제어시스템 오작동, 장애 유발 가능성이 존재함. |     |   |      |      |
| 보안대책                                                                                                                                                                                                                                                                                                                      |                                                                                                                                                                           |     |   |      |      |
| 판단기준                                                                                                                                                                                                                                                                                                                      | 양호: 제어시스템에 접근하기 위한 접근통제가 설정되어 있는 경우                                                                                                                                       |     |   |      |      |
|                                                                                                                                                                                                                                                                                                                           | 취약: 제어시스템에 접근하기 위한 접근통제가 설정되어 있지 않은 경우                                                                                                                                    |     |   |      |      |
| 조치방법                                                                                                                                                                                                                                                                                                                      | 제어시스템에 접근하기 위한 접근통제 설정                                                                                                                                                    |     |   |      |      |
| 보안설정방법                                                                                                                                                                                                                                                                                                                    |                                                                                                                                                                           |     |   |      |      |
| <div>1. 제어시스템 관리 서비스, 설정변경에 대한 인증, 접근통제 여부 확인</div> <div>- 제어시스템 관리 서비스 접근 시, ID/PW 요구 등의 인증과정 수행 여부 점검</div> <div>- 제어시스템 중요 설정명령, 설정파일에 대한 접근통제 여부 점검</div> <div>2. 제어시스템 관리 서비스 접근 시 인증과정을 수행하도록 설정</div> <div>- 제어시스템 관리 서비스에 대하여 관리자 IP만 접근하도록 TCPWrapper, 방화벽 등에서 접근통제</div> <div>- 설정명령, 설정파일의 권한을 관리자에게만 부여</div> |                                                                                                                                                                           |     |   |      |      |
| 조치 시 영향                                                                                                                                                                                                                                                                                                                   | 일반적으로 영향 없음                                                                                                                                                               |     |   |      |      |

## 제어시스템

| 취약점 항목                                                                                                                                                                                                                                                                                             | 4.10. 목적에 맞지 않는 제어시스템과 운영시스템의 기능 및 서비스 제거                                                                                             |     |   |      |      |
|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------|-----|---|------|------|
| 대상                                                                                                                                                                                                                                                                                                 | 제어시스템                                                                                                                                 | 위험도 | 중 | Code | C-19 |
| 취약점 개요                                                                                                                                                                                                                                                                                             | 제어시스템은 높은 가용성을 요구하기 때문에 이러한 위험이 없도록 제어를 위한 단일 목적으로 사용하여야 함. 제어시스템을 기반시설 제어 이외의 다른 용도로 중복하여 활용하는 경우, 타 시스템 서비스 장애가 제어시스템 장애로 전이될 수 있음. |     |   |      |      |
| 보안대책                                                                                                                                                                                                                                                                                               |                                                                                                                                       |     |   |      |      |
| 판단기준                                                                                                                                                                                                                                                                                               | 양호: 제어시스템이 제어를 위한 목적으로만 사용하고 있는 경우                                                                                                    |     |   |      |      |
|                                                                                                                                                                                                                                                                                                    | 취약: 제어시스템이 제어를 위한 목적 외로 사용되고 있는 경우                                                                                                    |     |   |      |      |
| 조치방법                                                                                                                                                                                                                                                                                               | 제어시스템을 다른 용도로 중복하여 활용하는 경우                                                                                                            |     |   |      |      |
| 보안설정방법                                                                                                                                                                                                                                                                                             |                                                                                                                                       |     |   |      |      |
| <div>■ Windows OS</div> <div>시작&gt; 설정&gt; 제어판&gt; 서비스에서 불필요한 서비스를 선택하여 중지<br/>(시작옵션에서 시작유형을 "사용 안함"으로 설정)</div> <div>■ Unix OS</div> <div>#vi /etc/inetd.conf 파일에서 불필요한 서비스 주석(#) 처리하여, 해당 서비스 비활성화</div> <div>※ 제어 시스템에서 해당 서비스 제거 시, 제거된 서비스가 제어 외의 다른 업무를 위한 목적으로 필요한 경우에는 독립된 별도의 장비 구축</div> |                                                                                                                                       |     |   |      |      |
| 조치 시 영향                                                                                                                                                                                                                                                                                            | 일반적으로 영향 없음                                                                                                                           |     |   |      |      |

제어시스템

|                                                                                                                                                                                                                                                                                                                             |                                                                                                         |     |   |      |      |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------|-----|---|------|------|
| 취약점 항목                                                                                                                                                                                                                                                                                                                      | 4.11. 운영에 있어 사용가능한 제어명령 및 안전한 제어를 위한 파라미터의 범위 제한                                                        |     |   |      |      |
| 대상                                                                                                                                                                                                                                                                                                                          | 제어시스템                                                                                                   | 위험도 | 중 | Code | C-20 |
| 취약점 개요                                                                                                                                                                                                                                                                                                                      | 제어명령, 파라미터 설정 등을 운영자 권한별로 제한하여야 함. 만약 권한별로 제한하지 않고 제어명령 및 파라미터에 의해 제어시스템 운영 시 기반시설 운영이 심각한 영향을 받을 수 있음. |     |   |      |      |
| 보안대책                                                                                                                                                                                                                                                                                                                        |                                                                                                         |     |   |      |      |
| 판단기준                                                                                                                                                                                                                                                                                                                        | 양호: 운영자의 권한별로 제어할 수 있는 기능을 제한하여 관리하고 있는 경우                                                              |     |   |      |      |
|                                                                                                                                                                                                                                                                                                                             | 취약: 운영자의 권한별로 제어할 수 있는 기능을 제한하여 관리하고 있지 않은 경우                                                           |     |   |      |      |
| 조치방법                                                                                                                                                                                                                                                                                                                        | 운영자의 권한별로 제어할 수 있는 기능을 제한하여 관리                                                                          |     |   |      |      |
| 보안설정방법                                                                                                                                                                                                                                                                                                                      |                                                                                                         |     |   |      |      |
| 1. 제어시스템 운영자 계정(HMI/MMI 등의 운영자 계정)의 제어 범위 및 명령이 제한되어 있는지 확인<br>- 제어시스템 운영자 계정, 관리자 계정이 분리되어 있는지 점검<br>- 운영자, 관리자 계정간의 제어범위, 명령의 권한이 상이한지 확인<br>※ 제어 응용프로그램에 대한 계정으로, 제어시스템 서버의 계정이 아님<br><br>2. 제어시스템 운영자, 관리자 계정을 별도로 생성하고, 제어 범위 및 중요 제어 명령에 대한 실행 권한을 제한함<br>※ 벤더사에 의한 제어시스템 수정, 개선이 필요하며, 정상적인 제어시스템 운영에 많은 영향을 미칠 수 있음 |                                                                                                         |     |   |      |      |
| 조치 시 영향                                                                                                                                                                                                                                                                                                                     | 계정에 따라 명령어 실행 제한                                                                                        |     |   |      |      |



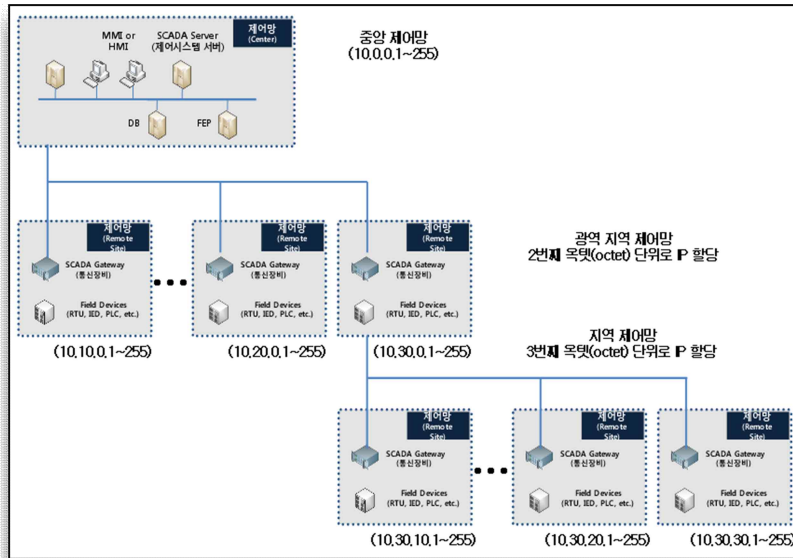
## 제어시스템

| 취약점 항목                                                                                                                                                                  | 4.12. 제어시스템 개선, 신규 시스템 도입, 패치 및 수정 시, 안전성을 테스트하기 위한 테스트베드 또는 시험환경 구축                                                                                                                                  |     |   |      |      |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----|---|------|------|
| 대상                                                                                                                                                                      | 제어시스템                                                                                                                                                                                                 | 위험도 | 중 | Code | C-21 |
| 취약점 개요                                                                                                                                                                  | 제어시스템에 새로운 기기, 장비를 도입하거나, 시스템 수정, 업데이트 및 패치를 적용하기 전에 시스템 영향을 점검할 수 있는 테스트베드의 구축이 필요함.<br>제어시스템에 대한 새로운 기기, 장비의 도입, 시스템 수정, 업데이트 및 패치의 적용은 시스템 오작동 및 장애를 유발할 수 있어, 높은 가용성을 요구한 제어시스템 운영에 문제를 야기할 수 있음. |     |   |      |      |
| 보안대책                                                                                                                                                                    |                                                                                                                                                                                                       |     |   |      |      |
| 판단기준                                                                                                                                                                    | 양호: 테스트베드를 구축하여 제어시스템의 변경사항을 적용한 경우                                                                                                                                                                   |     |   |      |      |
|                                                                                                                                                                         | 취약: 테스트베드를 구축하지 않은 채 제어시스템의 변경사항을 적용한 경우                                                                                                                                                              |     |   |      |      |
| 조치방법                                                                                                                                                                    | 제어시스템의 변경사항을 테스트할 수 있는 테스트베드를 구축                                                                                                                                                                      |     |   |      |      |
| 보안설정방법                                                                                                                                                                  |                                                                                                                                                                                                       |     |   |      |      |
| 1. 운영되는 제어시스템 외에 교육, 테스트, 시험·평가를 위한 별도의 제어시스템 테스트베드가 구축되어 있는지 확인<br><br>2. 운영 시스템 외의 별도의 제어시스템 테스트베드 구축<br>※ 제어시스템 테스트베드 구축에는 많은 예산과 시간이 소요되므로, 최초의 제어시스템 도입·구축 시 함께 고려 |                                                                                                                                                                                                       |     |   |      |      |
| 조치 시 영향                                                                                                                                                                 | 일반적으로 영향 없음                                                                                                                                                                                           |     |   |      |      |

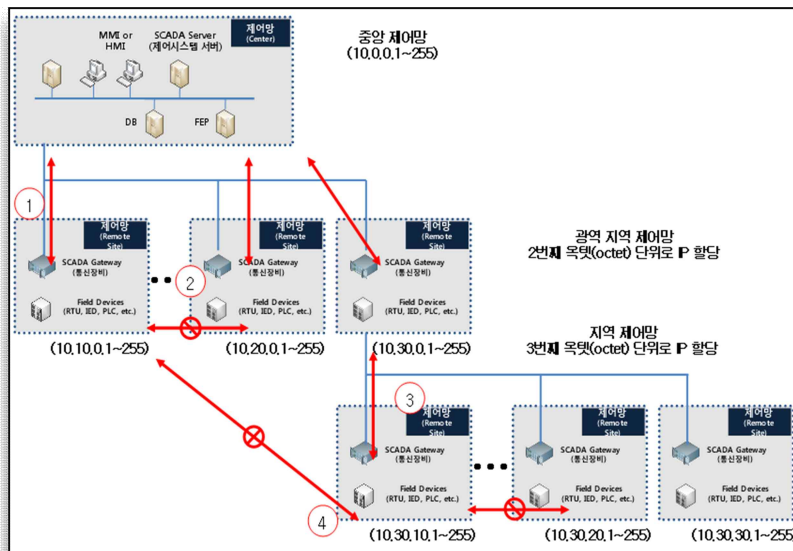
## 제어시스템

| 취약점 항목                                                     | 4.13. 제어 네트워크의 세분화 및 네트워크, 시스템 간 통신 제한                                                                                                                                                                                |     |                  |      |      |
|------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----|------------------|------|------|
| 대상                                                         | 제어시스템                                                                                                                                                                                                                 | 위험도 | 중                | Code | C-22 |
| 취약점 개요                                                     | 제어시스템은 지리적으로 넓은 범위에 걸쳐 많은 시스템을 운영하고 있으므로 구성된 제어시스템이 제어하는 범위에 맞추어 서브 네트워크로 구성하고, 각 네트워크 및 필요한 시스템 간으로 통신을 제한하여야 함. 또한 담당 구역의 제어시스템 운영자가 다른 담당 구역의 시스템을 제어하거나, 일부 시스템의 침해사고가 다른 시스템으로 전이되지 않도록 세분화된 네트워크 구성과 접근통제가 필요함. |     |                  |      |      |
| 보안대책                                                       |                                                                                                                                                                                                                       |     |                  |      |      |
| 판단기준                                                       | 양호: 세분화된 네트워크 구성과 접근통제를 통해 제어시스템을 운영하고 있는 경우                                                                                                                                                                          |     |                  |      |      |
|                                                            | 취약: 제어범위가 많은 시스템을 한 개의 네트워크에서 운영하고 있는 경우                                                                                                                                                                              |     |                  |      |      |
| 조치방법                                                       | 세분화된 네트워크 구성과 접근통제를 통해 제어시스템을 운영함                                                                                                                                                                                     |     |                  |      |      |
| 보안설정방법                                                     |                                                                                                                                                                                                                       |     |                  |      |      |
| 1. 제어 네트워크 구성도 분석 및 기술적 점검                                 |                                                                                                                                                                                                                       |     |                  |      |      |
| - 제어 네트워크가 제어 범위에 따라 별도의 서브넷으로 분리되고 적절한 접근통제가 이루어지고 있는지 점검 |                                                                                                                                                                                                                       |     |                  |      |      |
| - 네트워크 장비, 방화벽 정책 검토                                       |                                                                                                                                                                                                                       |     |                  |      |      |
| - 임의의 시스템에서 다른 서브넷의 제어시스템 서비스에 접근 점검                       |                                                                                                                                                                                                                       |     |                  |      |      |
| 2. 제어 범위에 따라 별도의 네트워크, 서브넷으로 분리                            |                                                                                                                                                                                                                       |     |                  |      |      |
| - 각 시스템, 네트워크 간에 운영에 필요한 서비스, IP에 한하여 접근 허용                |                                                                                                                                                                                                                       |     |                  |      |      |
| ※ 계층적으로 구성된 IP 체계 예시                                       |                                                                                                                                                                                                                       |     |                  |      |      |
| 네트워크 단위                                                    |                                                                                                                                                                                                                       |     | IP               |      |      |
| 중앙 제어 네트워크                                                 |                                                                                                                                                                                                                       |     | 10.0.0.1 ~ 255   |      |      |
| 광역 지역 제어 네트워크                                              | 광역 지역 제어 네트워크 1                                                                                                                                                                                                       |     | 10.10.0.1 ~ 255  |      |      |
|                                                            | 광역 지역 제어 네트워크 2                                                                                                                                                                                                       |     | 10.20.0.1 ~ 255  |      |      |
|                                                            | 광역 지역 제어 네트워크 3                                                                                                                                                                                                       |     | 10.30.0.1 ~ 255  |      |      |
| 지역 제어 네트워크                                                 | 지역 제어 네트워크 1                                                                                                                                                                                                          |     | 10.30.10.1 ~ 255 |      |      |
|                                                            | 지역 제어 네트워크 2                                                                                                                                                                                                          |     | 10.30.20.1 ~ 255 |      |      |
|                                                            | 지역 제어 네트워크 3                                                                                                                                                                                                          |     | 10.30.30.1 ~ 255 |      |      |

## 제어시스템



### ※ 제어시스템 내부 네트워크 구성 및 접근통제 예시



※ 국가정보원 “전자제어시스템 보안가이드” 3장 4절 “안전한 내부 네트워크 구성” 참조

조치 시 영향

내부망-인터넷 연계 제한

# PC 보안가이드라인

2014. 01



안전행정부 *희망의 새시대*

## PC 취약점 분석·평가 항목

| 분류       | 점검항목                                                        | 항목<br>중요도 | 항목코드  |
|----------|-------------------------------------------------------------|-----------|-------|
| 1. 계정관리  | 패스워드의 주기적 변경                                                | 상         | PC-01 |
|          | 패스워드 정책이 해당 기관의 보안 정책에 적합하게 설정                              | 상         | PC-02 |
|          | 복구 콘솔 자동 로그인 금지 설정                                          | 중         | PC-03 |
| 2. 서비스관리 | 공유 폴더 제거                                                    | 상         | PC-04 |
|          | 항목의 불필요한 서비스 제거                                             | 상         | PC-05 |
|          | Windows Messenger(MSN, .NET 메신저 등)와 같은 상용 메신저의 사용 금지        | 상         | PC-06 |
|          | 파일 시스템을 NTFS로 포맷                                            | 중         | PC-07 |
|          | 다른 OS로 멀티 부팅 금지                                             | 중         | PC-08 |
|          | 브라우저 종료 시 임시 인터넷 파일 폴더 내용 삭제                                | 하         | PC-09 |
| 3. 패치관리  | HOT FIX 등 최신 보안패치                                           | 상         | PC-10 |
|          | 항목 최신 서비스팩 적용                                               | 상         | PC-11 |
|          | MS-Office, 한글, 어도비 아크로벳 등의 응용 프로그램에 대한 최신 보안패치 및 벤더 권고사항 적용 | 상         | PC-12 |
| 4. 보안관리  | 바이러스 백신 프로그램 설치 및 주기적 업데이트                                  | 상         | PC-13 |
|          | 바이러스 백신 프로그램에서 제공하는 실시간 감시 기능 활성화                           | 상         | PC-14 |
|          | OS에서 제공하는 침입차단 기능 활성화                                       | 상         | PC-15 |
|          | 화면보호기 대기 시간 설정 및 재시작 시 암호 보호 설정                             | 상         | PC-16 |
|          | CD, DVD, USB 메모리 등과 같은 미디어의 자동실행 방지 등 이동식 미디어에 대한 보안대책 수립   | 상         | PC-17 |
|          | PC 내부의 미사용(3개월) ActiveX 제거                                  | 상         | PC-18 |
|          | 시스템 부팅 시 Windows Messenger 자동시작 금지                          | 중         | PC-19 |
|          | 항목 원격 지원 금지 정책 설정                                           | 중         | PC-20 |

## PC

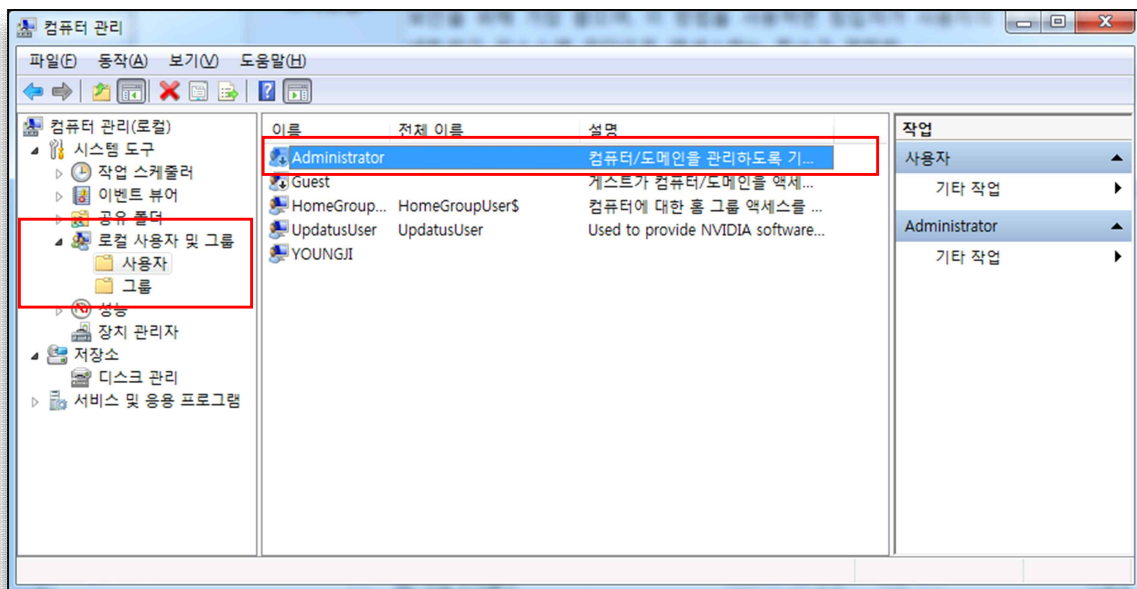
## 1. 계정 관리

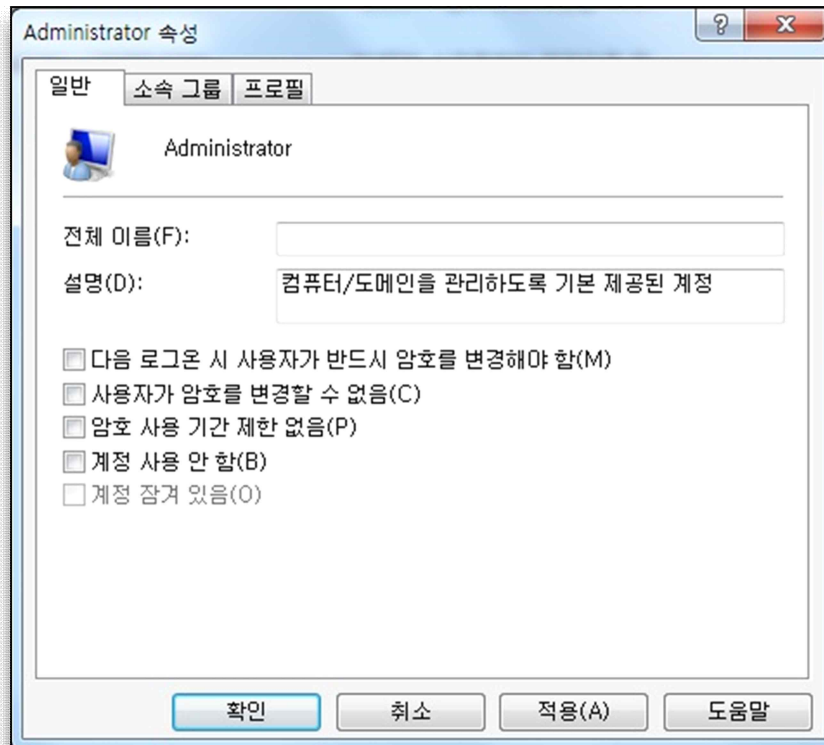
| 취약점 항목 | 1.1. 패스워드의 주기적 변경                                                                                                                                |     |   |      |       |
|--------|--------------------------------------------------------------------------------------------------------------------------------------------------|-----|---|------|-------|
| 대상 OS  | Windows XP, Windows 7                                                                                                                            | 위험도 | 상 | Code | PC-01 |
| 취약점 개요 | 계정의 패스워드를 주기적으로 변경하지 않고 오랫동안 사용할 경우 계정 패스워드가 외부에 유출될 수 있으며, 관리자 계정의 패스워드가 유출될 시 자료 유출 등 심각한 사고 발생 가능성이 존재함.                                      |     |   |      |       |
| 보안대책   |                                                                                                                                                  |     |   |      |       |
| 판단기준   | 양호: 최대 암호 사용 기간이 "90일"로 설정되어 있는 경우                                                                                                               |     |   |      |       |
|        | 취약: 암호 사용 기간이 "제한 없음"으로 설정되어 있는 경우                                                                                                               |     |   |      |       |
| 조치방법   | 최대 암호 사용 기간 "90일" 설정<br>※ 환경에 따라 30에서 90일마다(기본값: 42) 암호가 만료되도록 설정하는 것이 보안을 위해 가장 좋으며, 이 방법을 사용하면 침입자가 사용자의 암호를 도용하여 네트워크 리소스에 무단으로 액세스하는 횟수가 제한됨 |     |   |      |       |
| 보안설정방법 |                                                                                                                                                  |     |   |      |       |

## ■ Windows XP, Windows 7

## 1. 관리자 속성에서 암호 사용 기간 제한 설정 여부 확인

제어판 > 관리 도구 > 컴퓨터 관리 > 로컬 사용자 및 그룹 > 사용자 > Administrator 우클릭 > 속성 (시작 > 실행 > "lusrmgr.msc" 입력 > 사용자 > Administrator 우클릭 > 속성)

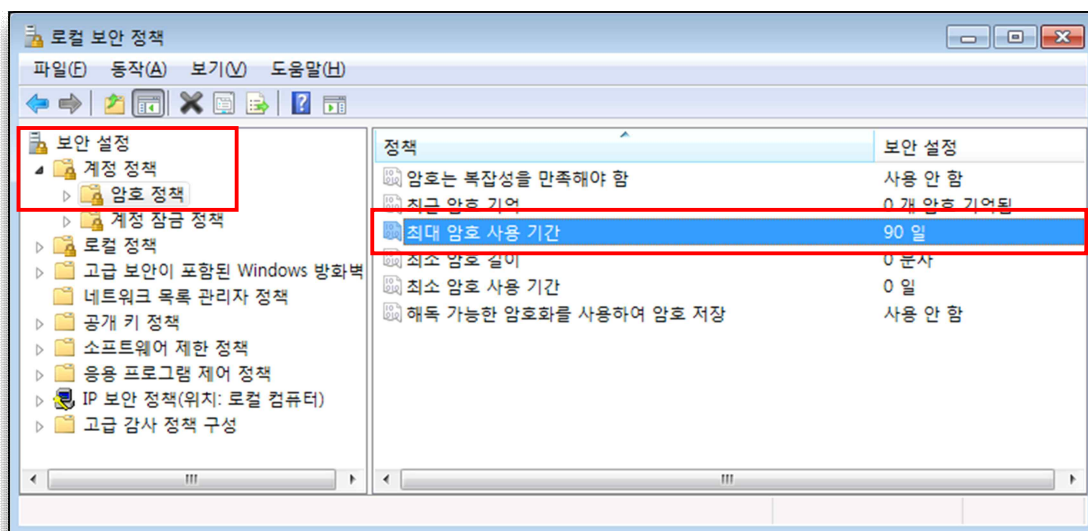


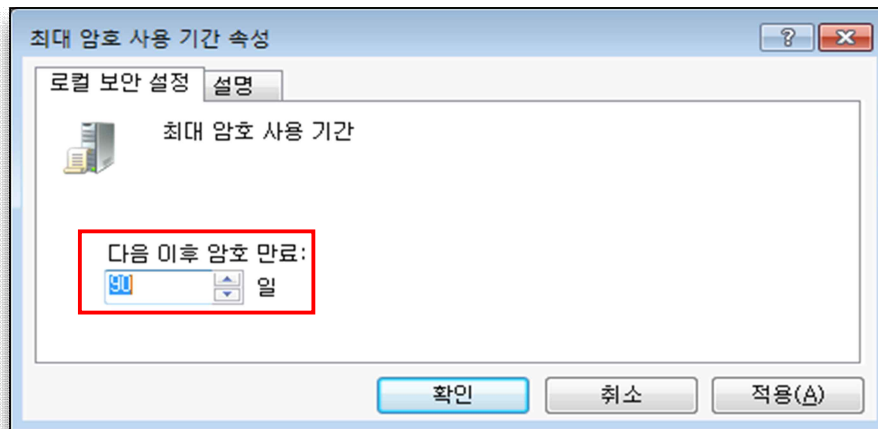


2. 제어판 > 관리 도구 > 로컬 보안 정책 > 보안 설정 > 계정 정책 > 암호 정책

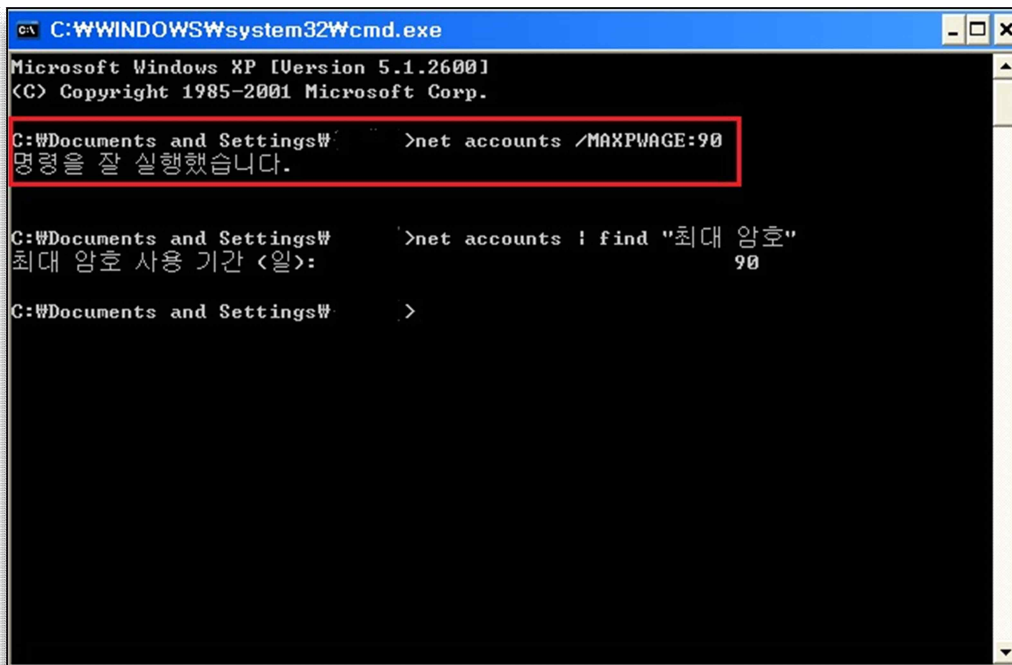
(시작 > 실행 > "gpedit.msc" 입력 > 컴퓨터 구성 > Windows 설정 > 보안 설정 > 계정 정책 > 암호 설정)

3. "최대 암호 사용 기간" 속성을 "90일"로 설정





4. CMD 명령어를 이용하여 설정을 변경하는 방법 (※ 관리자 권한으로 cmd 실행: 부록 참조)
- Windows 7: 관리자 권한으로 "cmd.exe" 실행 후 "net accounts /MAXPWAGE:90" 입력
  - Windows XP: 시작> 실행> "cmd" 입력> "net accounts /MAXPWAGE:90" 입력



|         |             |
|---------|-------------|
| 조치 시 영향 | 일반적으로 영향 없음 |
|---------|-------------|

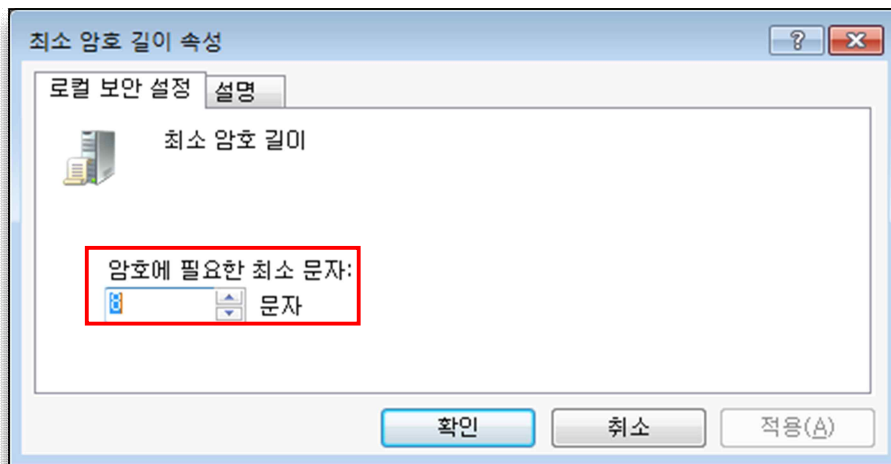
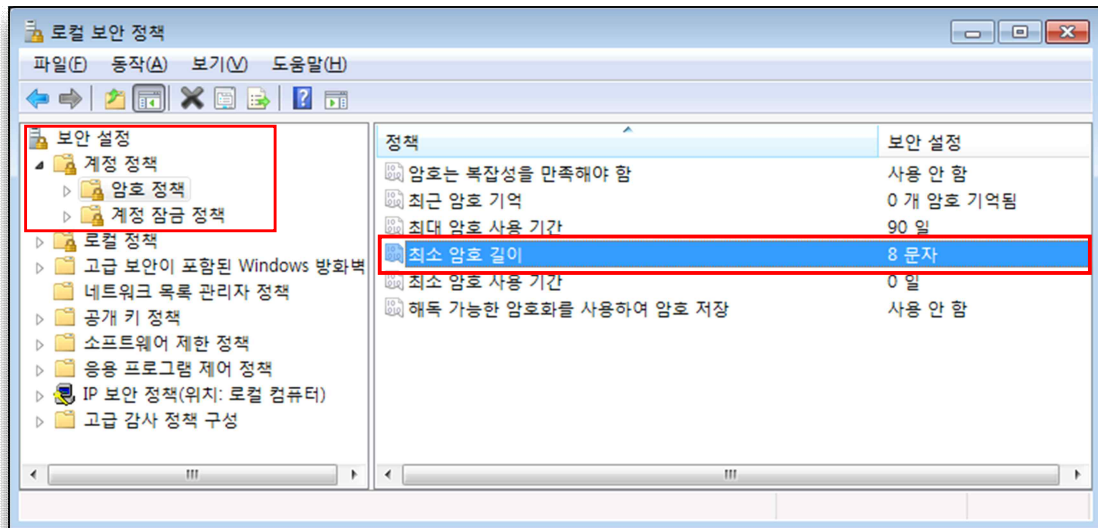


## PC

| 취약점 항목                                                                                                                                                                                                                                                     | 1.2. 패스워드 정책이 해당 기관의 보안 정책에 적합하게 설정                                                                                                                                                                                                                                               |     |   |      |       |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----|---|------|-------|
| 대상 OS                                                                                                                                                                                                                                                      | Windows XP, Windows 7                                                                                                                                                                                                                                                             | 위험도 | 상 | Code | PC-02 |
| 취약점 개요                                                                                                                                                                                                                                                     | 대부분의 환경에서 3종류(영문·숫자·특수문자) 조합의 경우 8자리 패스워드 사용, 2종류(영문·숫자) 조합의 경우 10자리 암호 사용을 권고하고 있음. 패스워드 정책에 적합하게 패스워드가 설정된 경우 *무작위 대입 공격(Brute Force Attack)이나 패스워드 추측 공격>Password Guessing)에 대한 대비가 가능함.<br><br>*무작위 대입 공격(Brute Force Attack): 컴퓨터로 암호를 해독하기 위해 가능한 모든 키를 하나하나 추론해 보는 시도를 말함. |     |   |      |       |
| 보안대책                                                                                                                                                                                                                                                       |                                                                                                                                                                                                                                                                                   |     |   |      |       |
| 판단기준                                                                                                                                                                                                                                                       | 양호: 최소 암호 길이가 해당 기관의 보안 정책을 반영하여 설정되어 있는 경우<br>취약: 암호를 사용하지 않거나, 추측하기 쉬운 문자조합으로 이루어진 짧은 자릿수의 패스워드를 사용하는 경우                                                                                                                                                                        |     |   |      |       |
| 조치방법                                                                                                                                                                                                                                                       | 최소 암호 길이를 해당 기관의 보안 정책에 적합하게 설정                                                                                                                                                                                                                                                   |     |   |      |       |
| 보안설정방법                                                                                                                                                                                                                                                     |                                                                                                                                                                                                                                                                                   |     |   |      |       |
| < 패스워드 설정 기준 >                                                                                                                                                                                                                                             |                                                                                                                                                                                                                                                                                   |     |   |      |       |
| 1. 영문, 숫자, 특수문자를 조합하여 계정명과 상이한 8자 이상의 패스워드 설정<br>※ 다음 각 항목의 문자 종류 중 2종류 이상을 조합하여 최소 10자리 이상 또는, 3종류 이상을 조합하여 최소 8자리 이상의 길이로 구성<br>가. 영문 대문자(26개)<br>나. 영문 소문자(26개)<br>다. 숫자(10개)<br>라. 특수문자(32개)                                                           |                                                                                                                                                                                                                                                                                   |     |   |      |       |
| 2. 패스워드는 비인가자에 의한 추측이 어렵도록 다음의 사항을 반영하여 설계<br>(1) Null(공백) 패스워드 사용 금지<br>(2) 문자 또는 숫자만으로 구성 금지<br>(3) 사용자 ID와 동일하거나 유사하지 않은 패스워드 금지<br>(4) 연속적인 문자나 숫자 사용 (예) 1111, 1234, abcd) 사용 금지<br>(5) 주기성 패스워드 재사용 금지<br>(6) 전화번호, 생일과 같이 추측하기 쉬운 개인정보를 패스워드로 사용 금지 |                                                                                                                                                                                                                                                                                   |     |   |      |       |
| 3. SAM 파일에 암호를 저장하기 위해 사용되는 LANMan 알고리즘은 8자 단위로 글자를 나누어 암호화하기 때문에 8의 배수가 되는 암호 사용을 권장 (8자로 이루어진 암호 사용 권장)                                                                                                                                                  |                                                                                                                                                                                                                                                                                   |     |   |      |       |
| 4. 아래와 같은 암호 설정 지양<br>Null, 계정과 동일하거나 유사한 스트링, 지역명, 부서명, 담당자명, 대표 업무명<br>"root", "rootroot", "root123", "123root", "admin", "admin123", "123admin", "osadmin", "adminos"                                                                                   |                                                                                                                                                                                                                                                                                   |     |   |      |       |

## ■ Windows XP, Windows 7

- 제어판 > 관리 도구 > 로컬 보안 정책 > 보안 설정 > 계정 정책 > 암호 정책  
(시작 > 실행 > "gpedit.msc" 입력 > 컴퓨터 구성 > Windows 설정 > 보안 설정 > 계정 정책 > 암호 설정)
- "최소 암호 길이 속성"을 "8문자(이상)"으로 설정



- CMD 명령어를 이용하여 설정을 변경하는 방법 (※ 관리자 권한으로 cmd 실행 방법 부록 참조)
  - Windows 7: 관리자 권한으로 "cmd.exe" 실행 후 "net accounts /MINPWLEN:8" 입력
  - Windows XP: 시작 > 실행 > "cmd" 입력 > "net accounts /MINPWLEN:8" 입력

PC

```
C:\>net accounts /MINPWLEN:8
명령을 잘 실행했습니다.

C:\>net accounts /MINPWLEN:8 ! find "최소 암호 길이"

C:\>net accounts ! find "최소 암호 길이"
최소 암호 길이: 8

C:\>
```

|         |             |
|---------|-------------|
| 조치 시 영향 | 일반적으로 영향 없음 |
|---------|-------------|

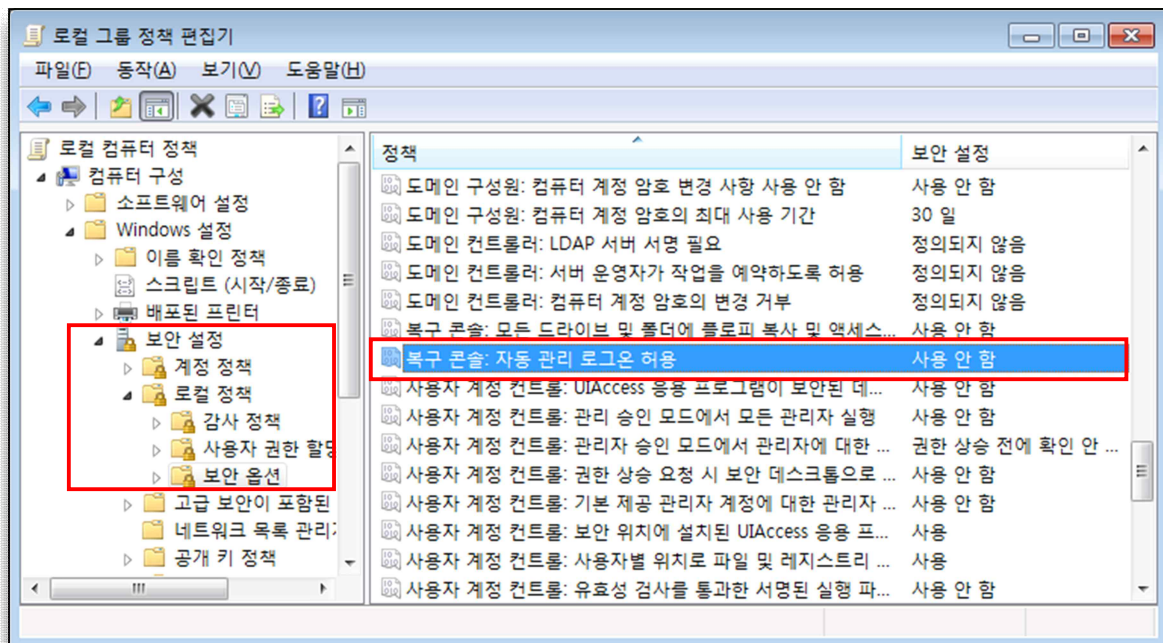


## PC

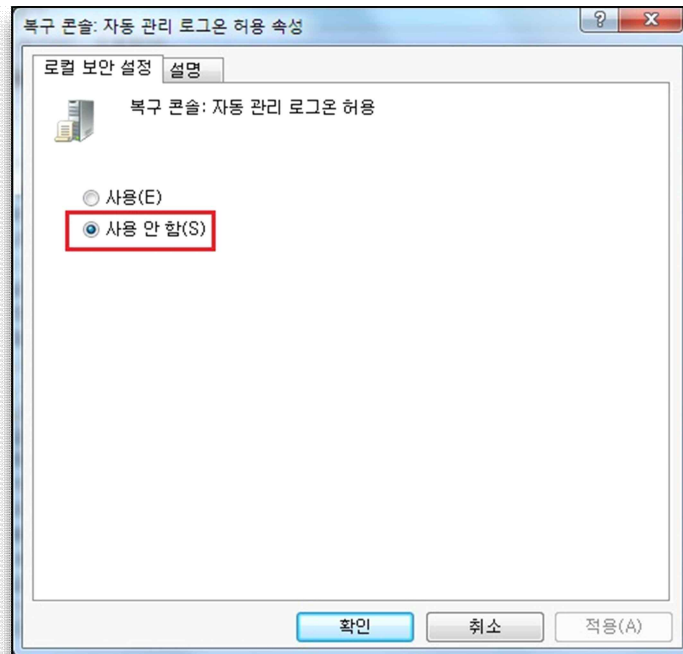
| 취약점 항목 | 1.3. 복구 콘솔 자동 로그인 금지 설정                                                                                                                                                                                             |     |   |      |       |
|--------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----|---|------|-------|
| 대상 OS  | Windows XP, Windows 7                                                                                                                                                                                               | 위험도 | 중 | Code | PC-03 |
| 취약점 개요 | <p>윈도우 *복구 콘솔(Recovery Console) 자동 로그인 설정은 시스템 액세스 허가 전 Administrator 계정의 암호 제공 여부를 결정하는 것으로 이 옵션을 사용하면 복구 콘솔에 암호를 입력하지 않아도 시스템에 자동으로 로그인됨. 이 경우 비인가자가 관리자 권한으로 시스템에 접근하여 주요 정보를 획득할 수 있는 위험이 있음.</p>               |     |   |      |       |
|        | <p>*복구 콘솔(Recovery Console): 윈도우 2000, 윈도우 XP, 윈도우 서버 2003 운영 체제의 기능 가운데 하나로 윈도우가 그래픽 사용자 인터페이스(GUI)가 나타날 때까지 시동이 되지 않는 상황에서 관리자들이 복구할 수 있게 하는 것이 주된 기능임. 이 콘솔을 통해 관리자들이 명령 줄 인터페이스를 이용하여 제한된 영역의 작업을 수행할 수 있음.</p> |     |   |      |       |
| 보안대책   |                                                                                                                                                                                                                     |     |   |      |       |
| 판단기준   | 양호: 복구 콘솔 자동 로그인 허용이 "사용 안 함"으로 설정되어 있는 경우                                                                                                                                                                          |     |   |      |       |
|        | 취약: 복구 콘솔 자동 로그인 허용이 "사용"으로 설정되어 있는 경우                                                                                                                                                                              |     |   |      |       |
| 조치방법   | 복구 콘솔 자동 로그인 허용 "사용 안 함"으로 설정                                                                                                                                                                                       |     |   |      |       |
| 보안설정방법 |                                                                                                                                                                                                                     |     |   |      |       |

## ■ Windows XP, Windows 7

- 제어판 > 관리 도구 > 로컬 보안 정책 > 보안 설정 > 로컬 정책 > 보안 옵션  
(시작 > 실행 > "gpedit.msc" 입력 > 컴퓨터 구성 > Windows 설정 > 보안 설정 > 로컬 정책 > 보안 옵션)
- 복구 콘솔: 자동 관리 로그인 허용 속성 : "사용 안 함" 설정



## PC



## 3. 레지스트리 값으로 설정하는 방법

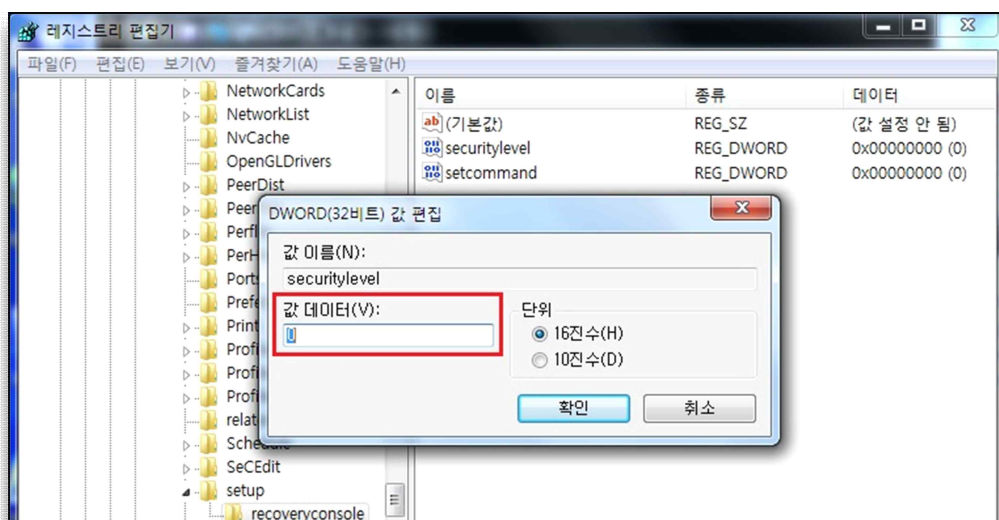
(1) 시작 &gt; 실행 &gt; "regedit" 입력

(2) 레지스트리 경로

HKLM\SOFTWARE\Microsoft\WindowsNT\CurrentVersion\Setup\RecoveryConsole

(3) 설정 값 입력

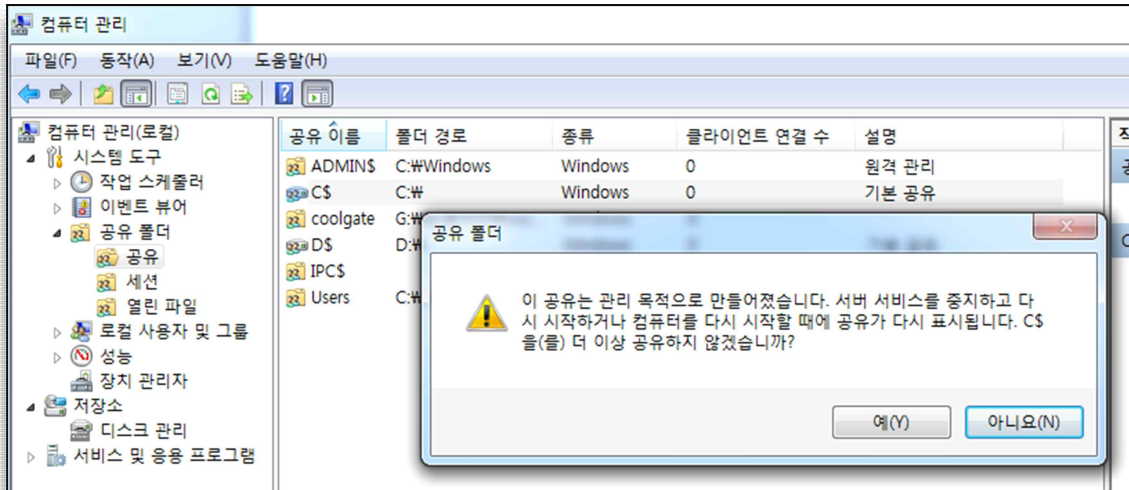
|                   |               |
|-------------------|---------------|
| <b>Value name</b> | SecurityLevel |
| <b>Data Type</b>  | DWORD 값       |
| <b>Value</b>      | 0(zero)       |



조치 시 영향 | 일반적으로 영향 없음

## 2. 서비스 관리

| 취약점 항목                                                                                                                                                                                                                                                                                                                                                                             |                                                                                                                                                                                                                                                                                                                                                                                                                 | 2.1. 공유 폴더 제거 |   |      |       |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------|---|------|-------|
| 대상 OS                                                                                                                                                                                                                                                                                                                                                                              | Windows XP , Windows 7                                                                                                                                                                                                                                                                                                                                                                                          | 위험도           | 상 | Code | PC-04 |
| 취약점 개요                                                                                                                                                                                                                                                                                                                                                                             | <p>시스템의 기본 공유 항목이 제거되지 않으면 모든 시스템 자원에 접근할 수 있는 위험한 상황이 발생할 수 있음. 2001년에 발생한 *Win32.Nimda 바이러스도 여러 가지 방법 중에서 이러한 공유 기능 침투의 한 경로를 이용한 것임.</p> <p>불필요한 공유라고 판단되면 공유를 해제해야 하며, 공유를 해제한 후에 레지스트리 AutoShareServer 값 설정을 통해 재부팅 시 기본 공유 폴더의 자동 공유 설정을 방지할 수 있음. (하드디스크 기본 공유 폴더 예: C\$, D\$, Admin\$, IPC\$ 등)</p> <p>또한, 기본 공유 폴더를 제외한 일반 공유 폴더의 권한이 Everyone으로 설정되었는지 확인하고, 공유 금지 설정을 통해 익명 사용자에게 의한 접근을 차단해야 함.</p> |               |   |      |       |
|                                                                                                                                                                                                                                                                                                                                                                                    | <p>*Win32.Nimda 바이러스: 2001년 9월 17일 미국·유럽·라틴아메리카에서 동시에 발생한 뒤 한국에서도 다음 날 저녁 발견될 정도로 빠르게 확산하는 악성 컴퓨터 바이러스임. 두 종류가 있는데, 하나는 정부를 뜻하는 영어 단어 'admin'의 철자를 거꾸로 나열해 명명한 것이고, 다른 하나는 제3차 세계대전을 뜻하는 'To 3W'를 거꾸로 나열한 'W32'임. 이 바이러스는 이메일뿐만 아니라 감염된 웹 사이트를 통해서도 전염되며, 네트워크상에서 패스워드 없이 읽기·쓰기가 가능한 공유 디렉터리를 통해서도 감염되는 특징을 가짐.</p>                                                                                             |               |   |      |       |
| 보안대책                                                                                                                                                                                                                                                                                                                                                                               |                                                                                                                                                                                                                                                                                                                                                                                                                 |               |   |      |       |
| 판단기준                                                                                                                                                                                                                                                                                                                                                                               | 양호: 불필요한 공유 폴더가 존재하지 않는 경우                                                                                                                                                                                                                                                                                                                                                                                      |               |   |      |       |
|                                                                                                                                                                                                                                                                                                                                                                                    | 취약: 불필요한 공유 폴더가 존재하는 경우                                                                                                                                                                                                                                                                                                                                                                                         |               |   |      |       |
| 조치방법                                                                                                                                                                                                                                                                                                                                                                               | 공유 폴더 불필요 시 삭제                                                                                                                                                                                                                                                                                                                                                                                                  |               |   |      |       |
|                                                                                                                                                                                                                                                                                                                                                                                    | 공유 폴더 필요시 적절한 접근권한 부여 및 암호 설정                                                                                                                                                                                                                                                                                                                                                                                   |               |   |      |       |
| 보안설정방법                                                                                                                                                                                                                                                                                                                                                                             |                                                                                                                                                                                                                                                                                                                                                                                                                 |               |   |      |       |
| <p>&lt; 공유 폴더 설정 기준 &gt;</p> <ol style="list-style-type: none"><li>1. C\$, D\$, Admin\$ 등의 기본 공유 폴더 제거</li><li>2. 기본 공유 폴더 제거 후 시스템 재부팅 시 “기본 공유 폴더가 자동으로 공유되는 것”을 방지하기 위해 해당 레지스트리의 AutoShareServer 값을 “0”으로 설정</li><li>3. 일반 공유 폴더 사용 시 공유 폴더 접근 권한에 “Everyone” 제거</li><li>4. 일반 공유 폴더 사용 시 접근이 필요한 계정에만 적절한 (읽기, 변경)권한 설정</li><li>5. 일반 공유 폴더 사용 시 공유 폴더 접근을 위한 암호 설정</li></ol> |                                                                                                                                                                                                                                                                                                                                                                                                                 |               |   |      |       |
| <p>■ Windows XP, Windows 7</p> <p>■ 기본 공유 폴더 상태 확인 및 공유 중지</p> <ol style="list-style-type: none"><li>1. 제어판&gt; 관리 도구&gt; 컴퓨터 관리&gt; 공유 폴더&gt; 공유<br/>(시작&gt; 실행&gt; “fsmgmt.msc” 입력&gt; 공유)</li><li>2. 불필요한 공유 폴더 확인&gt; 해당 공유 폴더 우클릭&gt; 공유 중지</li></ol>                                                                                                                         |                                                                                                                                                                                                                                                                                                                                                                                                                 |               |   |      |       |

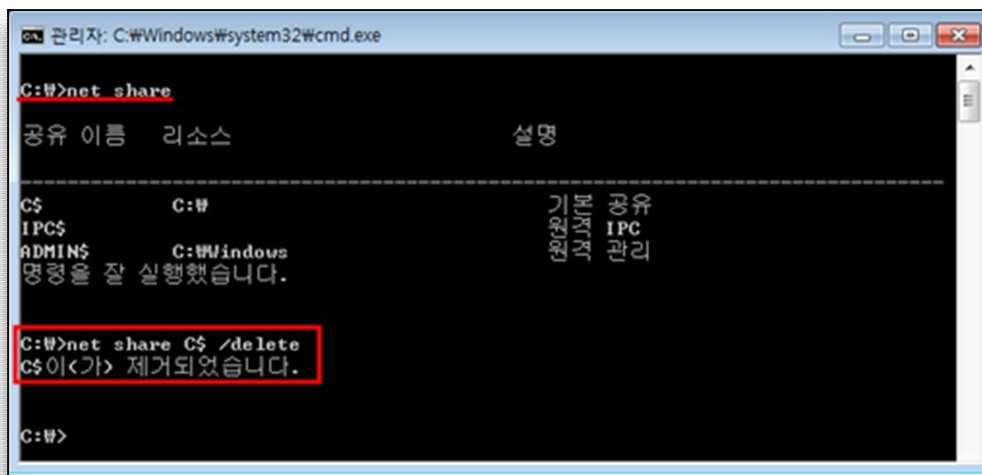


### 3. CMD 명령어를 이용하여 설정을 변경하는 방법 (※ 관리자 권한으로 cmd 실행 방법 부록 참조)

- Windows 7: 관리자 권한으로 "cmd.exe" 실행 후 "net share" 입력
- Windows XP: 시작> 실행> "cmd" 입력> "net share" 입력

C:\>net share 명령을 통해 공유 디렉터리 확인

C:\>net share "삭제할 공유 폴더명" /delete 명령을 통해 공유 디렉터리 삭제



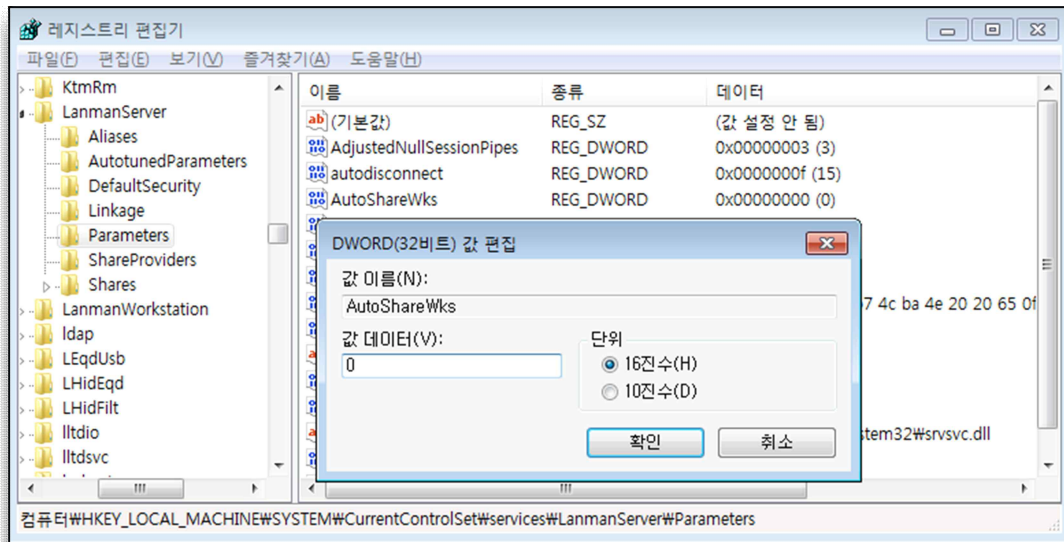
#### ■ 시스템 재부팅 후 기본 공유 폴더 자동 공유 방지 설정

1. 시작> 실행> "regedit" 입력
2. 레지스트리 경로  
HKLM\System\CurrentControlSet\Services\LanmanServer\Parameters
3. 설정 값 입력

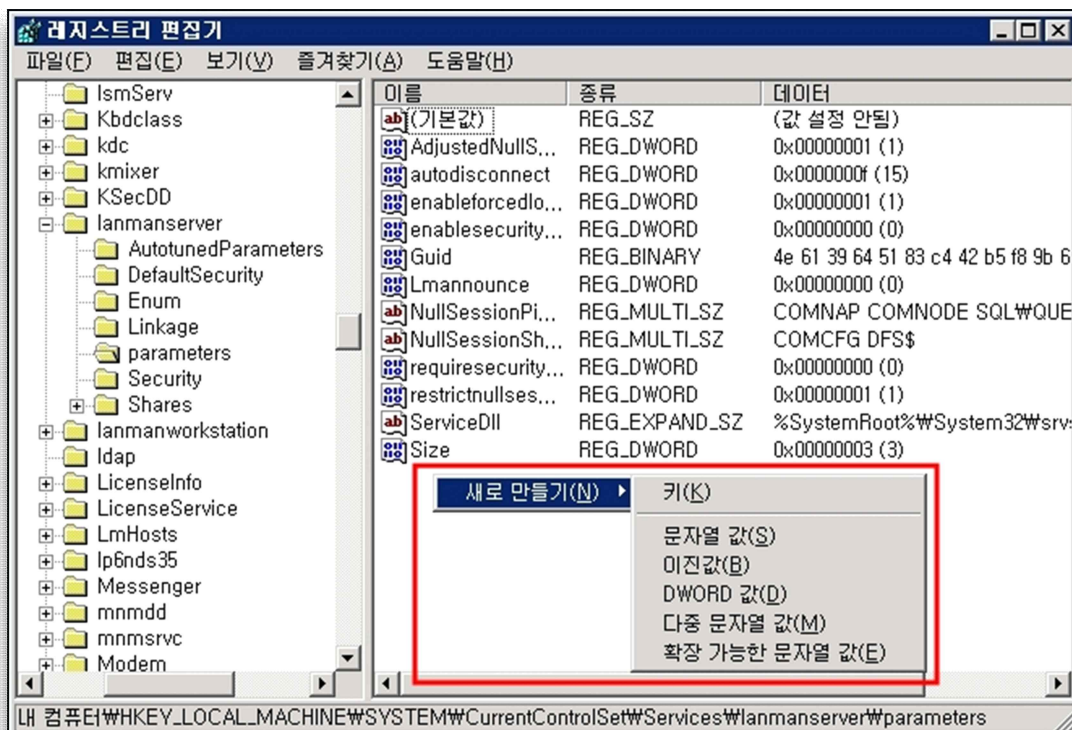
|            |                                 |
|------------|---------------------------------|
| Value name | AutoShareServer                 |
| Data Type  | DWORD 값                         |
| Value      | 0(zero)<br>※ Default 값: 0(zero) |

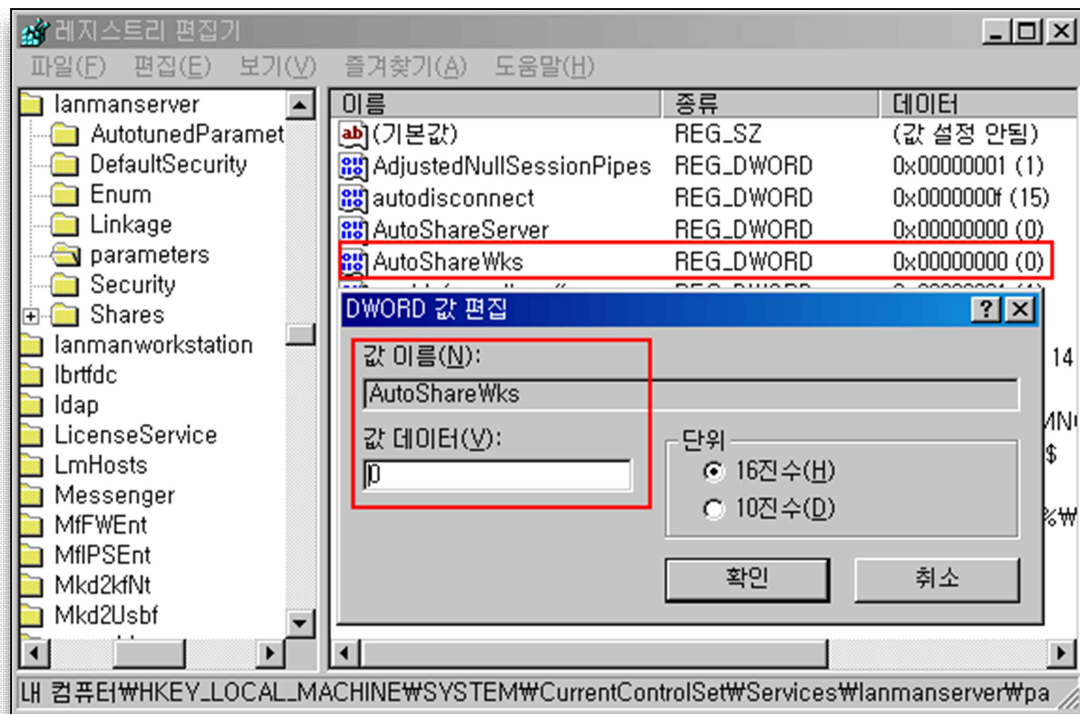


## PC



4. 값이 없는 경우, 새로 만들기> AutoShareServer(또는, AutoShareWks)를 추가하고 값을 "0"으로 입력  
아래 그림과 같이 AutoShareWks를 입력하며, 이때 값은 Default 값인 "0"으로 유지  
또한, 방화벽과 라우터에서 135,139(TCP/UDP)포트를 차단하여 외부로 부터의 위험을 제거함으로써  
보안성을 높일 수 있음

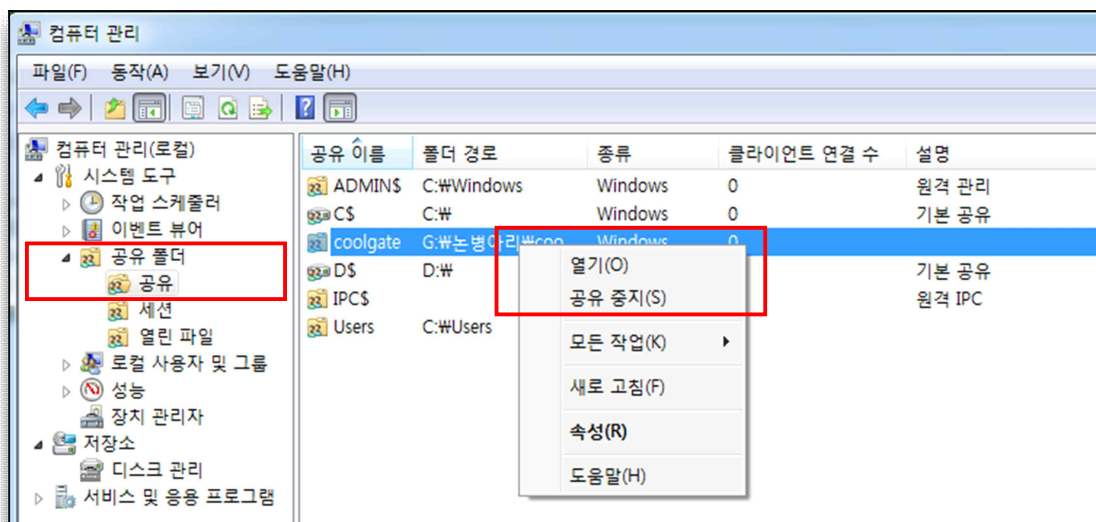




※ 기본 공유에 대한 조치 시 반드시 [기본 공유 삭제], [비활성화 레지스트리 값]을 모두 설정함

#### ■ 일반 공유 폴더 확인 및 공유 중지

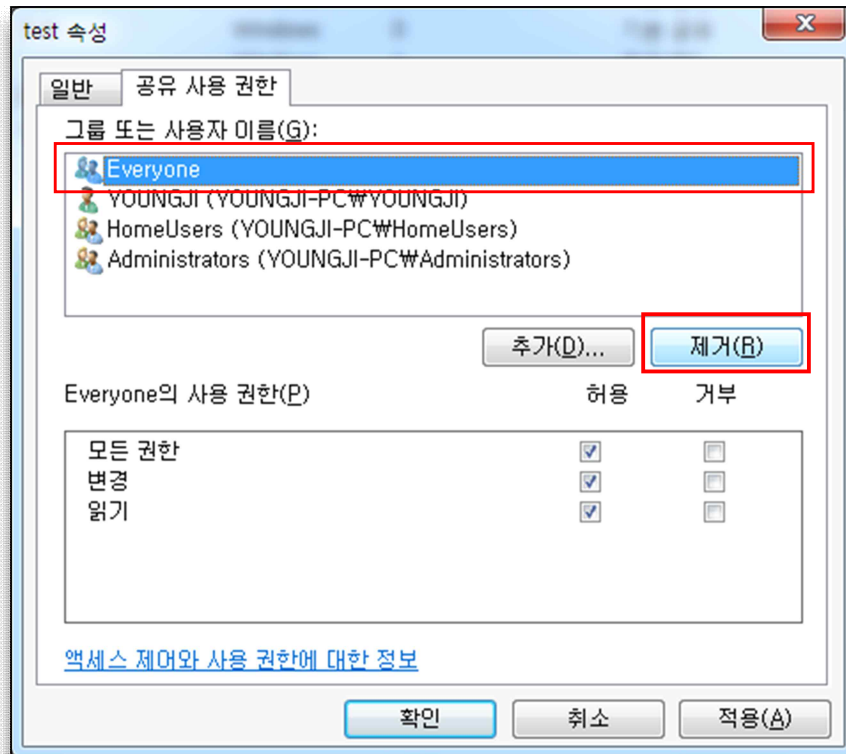
- 제어판 > 관리 도구 > 컴퓨터 관리 > 공유 폴더 > 공유  
(시작 > 실행 > "fsmgmt.msc" 입력 > 공유)
- 불필요한 공유 폴더 확인 > 해당 공유 폴더 우클릭 > 공유 중지



#### ■ 일반 공유 폴더 필요 시 권한 설정

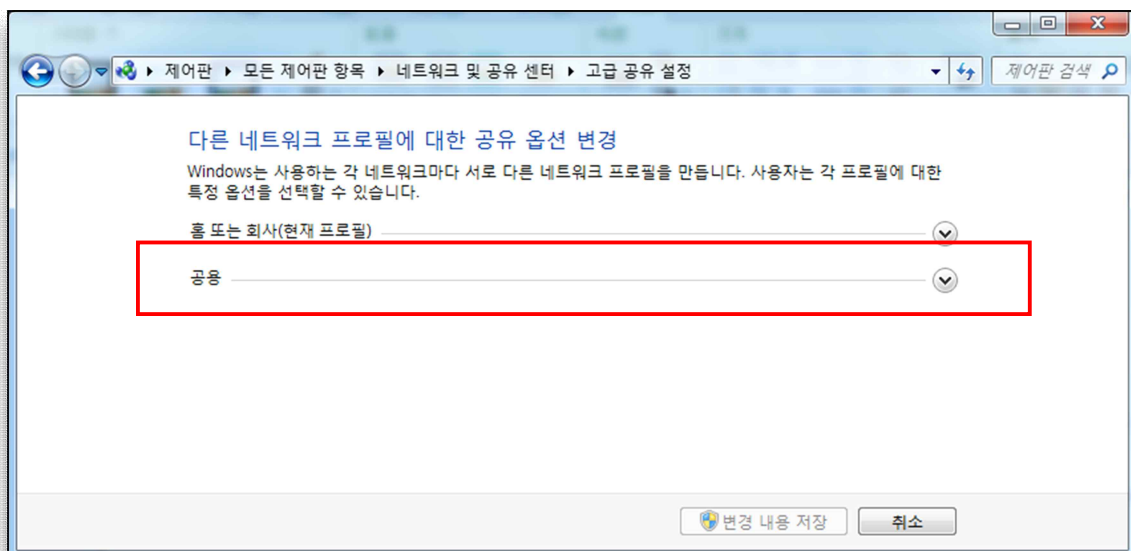
- 제어판 > 관리 도구 > 컴퓨터 관리 > 공유 폴더 > 공유  
(시작 > 실행 > "fsmgmt.msc" 입력 > 공유)

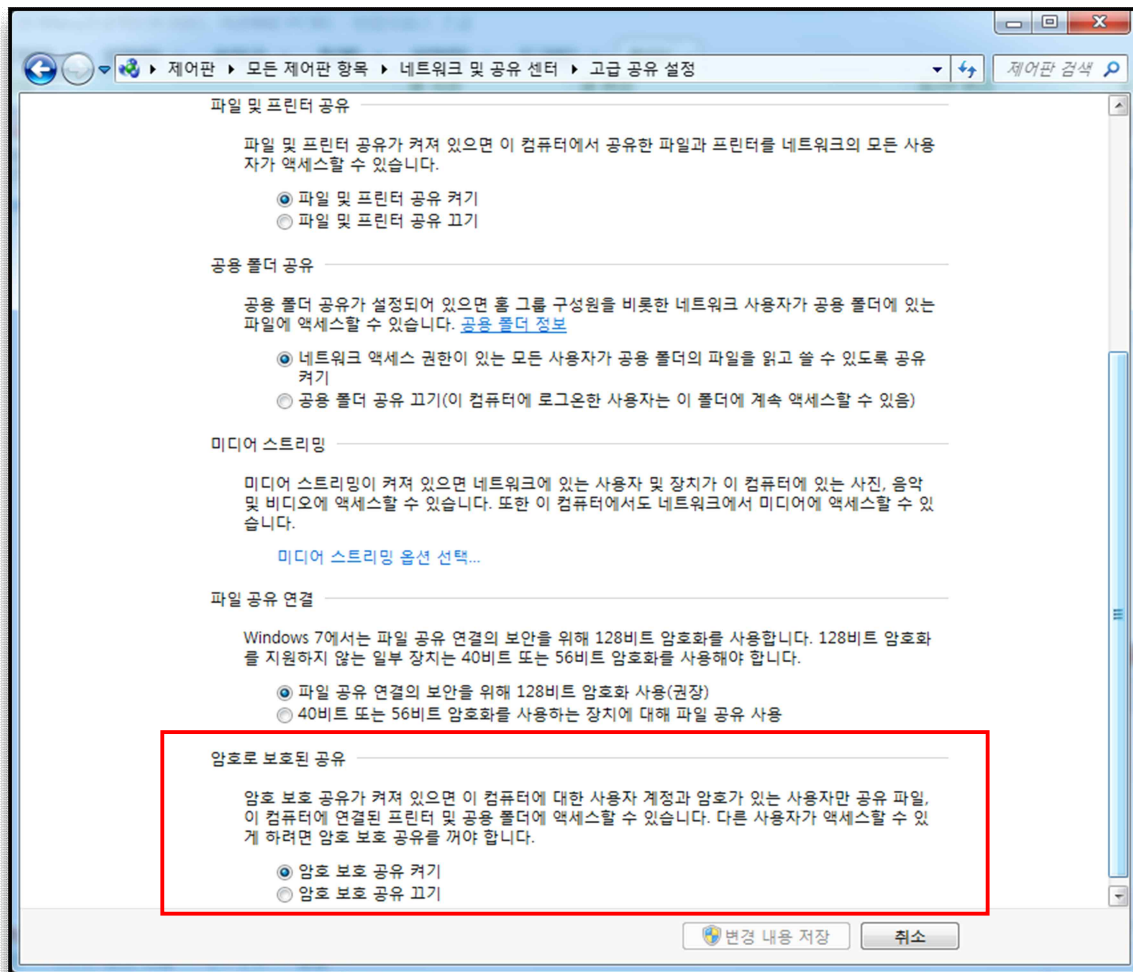
2. 사용할 공유 폴더 확인 선택 후 우클릭> 속성> [공유] 탭> [공유 사용 권한] 탭  
 “Everyone”으로 된 공유를 제거하고, 접근이 필요한 계정에만 적절한 권한 추가



#### ■ 공유 폴더 접근 암호 설정

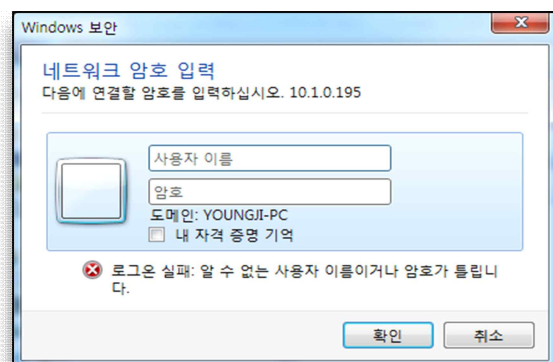
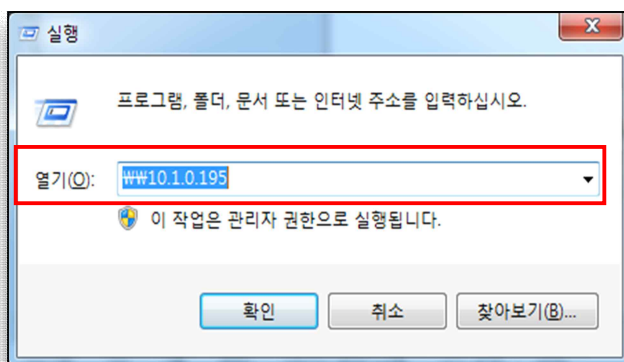
1. 제어판> 네트워크 및 공유 센터> 고급 공유 설정
2. “암호 보호 공유 켜기” 설정





### 3. 공유 폴더 접근 가능 여부 확인

시작> 실행> 공유 폴더 PC 계정명 또는, IP 주소 입력 후 패스워드 입력 팝업 확인



#### 조치 시 영향

업무에 필요한 공유 폴더 사용 시 사용자별 권한 부여 필요

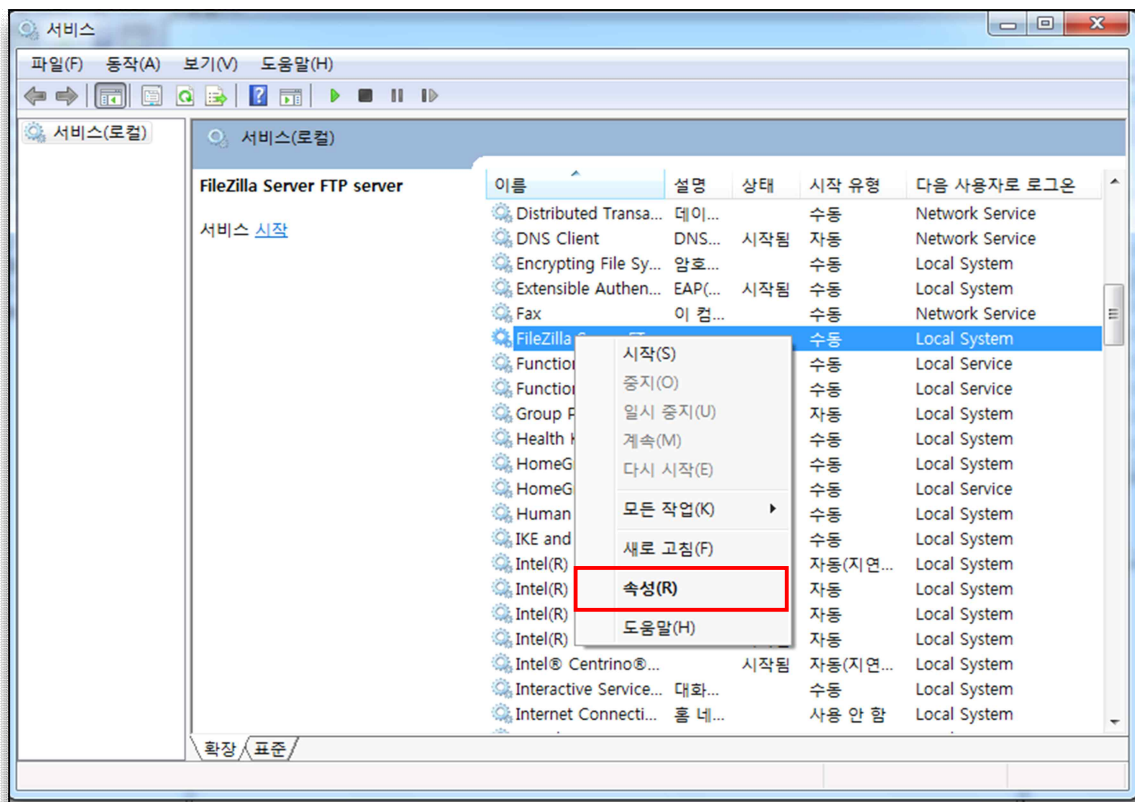


## PC

| 취약점 항목 | 2.2. 항목의 불필요한 서비스 제거                                                                                                                                                                                         |     |   |      |       |
|--------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----|---|------|-------|
| 대상 OS  | Windows XP, Windows 7                                                                                                                                                                                        | 위험도 | 상 | Code | PC-05 |
| 취약점 개요 | <p>불필요한 서비스가 시스템에 디폴트로 설치되어 실행되는 경우 시스템 자원을 낭비하게 될 뿐만 아니라, 이 서비스를 통해 악의적인 공격자가 침입할 수 있으므로 필요하지 않은 서비스는 중지시켜야 함.</p> <p>시스템 관리자는 대상 시스템의 용도를 정확히 파악한 후 특별한 목적으로 사용하는 업무 관련 서비스를 제외한 다른 불필요한 서비스를 제거하여야 함.</p> |     |   |      |       |
| 보안대책   |                                                                                                                                                                                                              |     |   |      |       |
| 판단기준   | 양호: 업무에 필요한 서비스만 실행되고 있는 경우                                                                                                                                                                                  |     |   |      |       |
|        | 취약: 디폴트로 설치된 서비스가 실행되고 있는 경우                                                                                                                                                                                 |     |   |      |       |
| 조치방법   | 불필요한 서비스 중지                                                                                                                                                                                                  |     |   |      |       |
| 보안설정방법 |                                                                                                                                                                                                              |     |   |      |       |

## ■ Windows XP, Windows 7

- 제어판 > 관리 도구 > 서비스 > 해당 서비스 선택 > 속성  
(시작 > 실행 > "services.msc" 입력 > 해당 서비스 선택 > 속성)
- 불필요한 서비스 -> 중지  
시작 유형 -> 사용 안 함



## 2. 각 서비스 마다 옵션을 설정할 수 있음

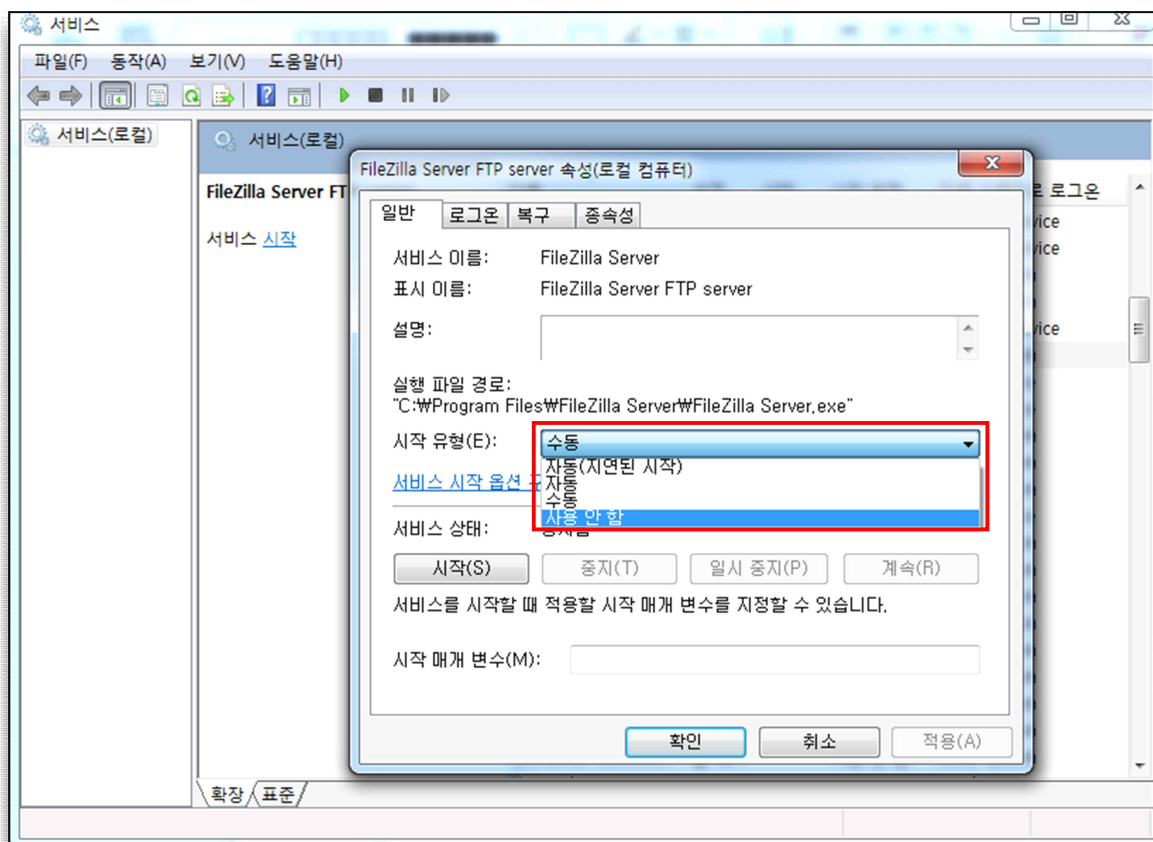
해당 서비스를 선택하고 더블 클릭하여 “시작 유형” 선택 및 “시작 시 로그인 계정” 별도 설정 가능  
 시스템 시작 시 자동으로 시작되게 하려면 [자동], 수동으로 서비스를 시작하려면 [수동], 서비스 자체를 사용하지 않으려면 [사용 안 함]을 선택한 후 [확인]을 클릭

| 서비스 시작 유형 | 설 명                                    |
|-----------|----------------------------------------|
| 사용 안 함    | 설치되어 있으나 실행되지 않음                       |
| 수동        | 다른 서비스나 응용 프로그램에서 당 기능을 필요로 할 때만 시작됨   |
| 자동        | 부팅 시에 해당 장치 드라이버가 로드된 후에 운영 체제에 의해 시작됨 |

※ 꼭 필요한 서비스만 사용하고 나머지는 “사용 안 함”으로 설정

※ 개인 방화벽 실행

※ 백신 등에서 제공하는 방화벽 기능 활성화 사용



## PC

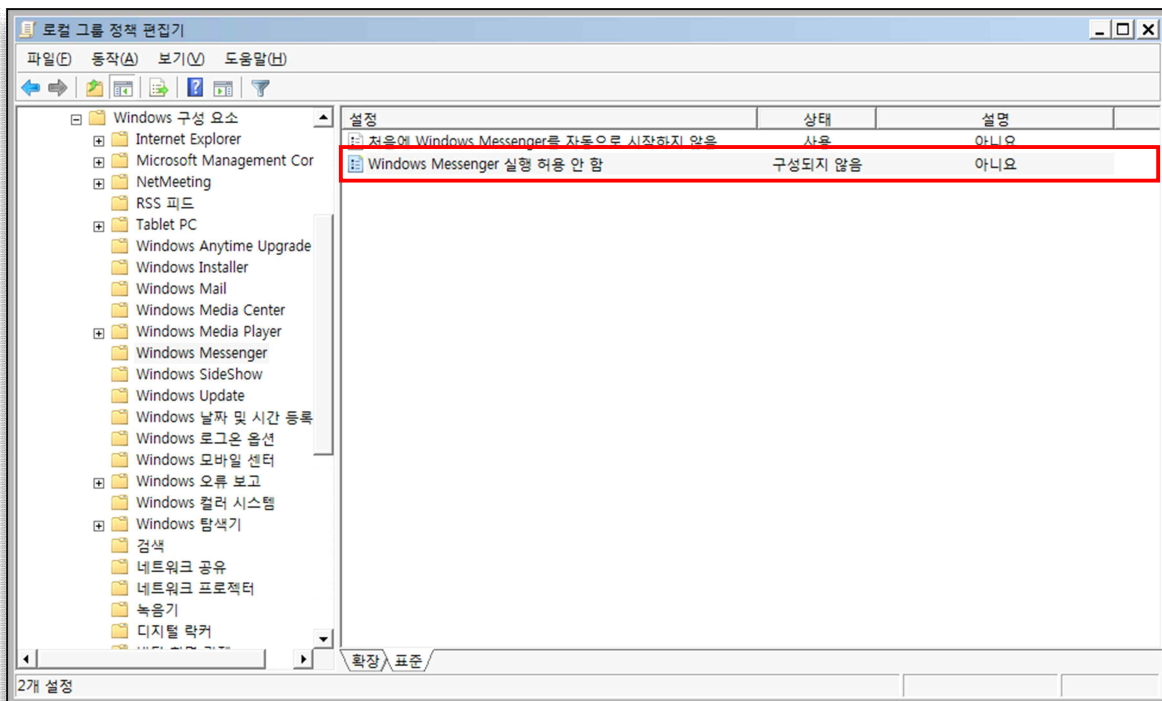
| 서비스 리스트                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 불필요한 서비스 리스트                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  | Windows 운영을 위한 최소한의 서비스                                                                                                                                                                                                                                                                                                                                                                                                                                |
| <ul style="list-style-type: none"> <li>- Alerter</li> <li>- Clipbook</li> <li>- ComputerBrowser</li> <li>- DHCP Client</li> <li>- FTP Publishing Service</li> <li>- InternetConnectionSharingService</li> <li>- IndexingService</li> <li>- InfraredMonitorService</li> <li>- Messenger</li> <li>- NetLogon</li> <li>- Network DDE</li> <li>- Network DDE DSDM</li> <li>- NetMeetingRemoteDesktopSharingService</li> <li>- Print spooler</li> <li>- RemoteRegistryService</li> <li>- RoutingandRemoteAccessService</li> <li>- SimpleTCP/IPService</li> <li>- SMTPService</li> <li>- TaskSchedulerService</li> <li>- TCPIP NetBIOS Helper</li> <li>- TerminalService</li> </ul> | <ul style="list-style-type: none"> <li>- Logical Logging Manager</li> <li>- NetworkConnections</li> <li>- NTLMSecuritySupportProvider</li> <li>- PlugandPlay</li> <li>- Server</li> <li>- Workstation</li> <li>- RemoveableStrage</li> <li>- SecurityAccountsManager</li> <li>- WindowsManagementInstrumentation</li> <li>- WindowsManagem nt Instrumentation driver extensions</li> <li>- WMDMPMSPService</li> <li>- ApplicationManagement</li> </ul> |
| <b>조치 시 영향</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                | "사용 안 함"으로 등록된 서비스 이용 불가                                                                                                                                                                                                                                                                                                                                                                                                                               |

## PC

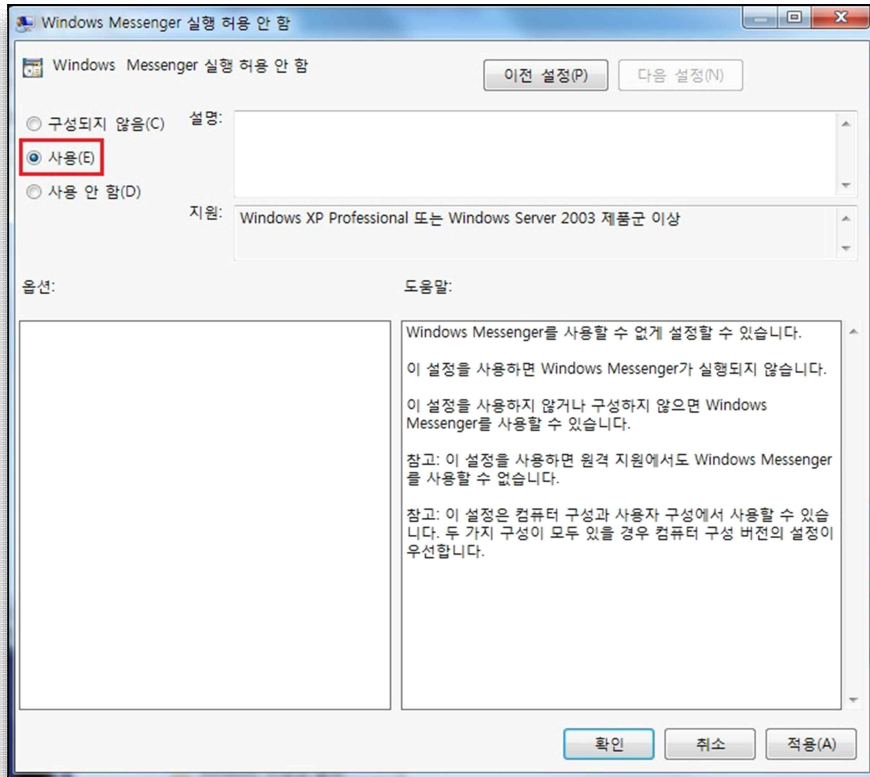
| 취약점 항목 | 2.3. Windows Messenger(MSN, .NET 메신저 등)와 같은 상용 메신저의 사용 금지                                                                                                                                            |     |   |      |       |
|--------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----|---|------|-------|
| 대상 OS  | Windows XP, Windows 7                                                                                                                                                                                | 위험도 | 상 | Code | PC-06 |
| 취약점 개요 | 일반 사용자 PC에서 Windows Messenger를 사용할 경우, *메신저(Messenger)를 통해서 주요 정보가 유출될 수 있을 뿐만 아니라 *악성코드가 유입될 수 있음.<br><br>*메신저(Messenger): 인터넷을 통해 실시간으로 대화를 나눌 수 있는 서비스.<br>*악성코드: 컴퓨터에 악영향을 끼칠 수 있는 모든 소프트웨어의 총칭. |     |   |      |       |
| 보안대책   |                                                                                                                                                                                                      |     |   |      |       |
| 판단기준   | 양호: Windows Messenger가 실행되고 있지 않은 경우                                                                                                                                                                 |     |   |      |       |
|        | 취약: Windows Messenger가 실행되고 있는 경우                                                                                                                                                                    |     |   |      |       |
| 조치방법   | Windows Messenger를 실행하지 않음 설정                                                                                                                                                                        |     |   |      |       |
| 보안설정방법 |                                                                                                                                                                                                      |     |   |      |       |

## ■ Windows XP, Windows 7

1. 시작> 실행> "gpedit.msc" 입력> 컴퓨터 구성> 관리 템플릿> Windows 구성 요소> Windows Messenger
2. "Windows Messenger를 실행 허용 안 함" 설정을 "사용"으로 설정







### 3. 레지스트리 값으로 설정하는 방법

(1) 시작 > 실행 > "regedit" 입력

(2) 레지스트리 경로

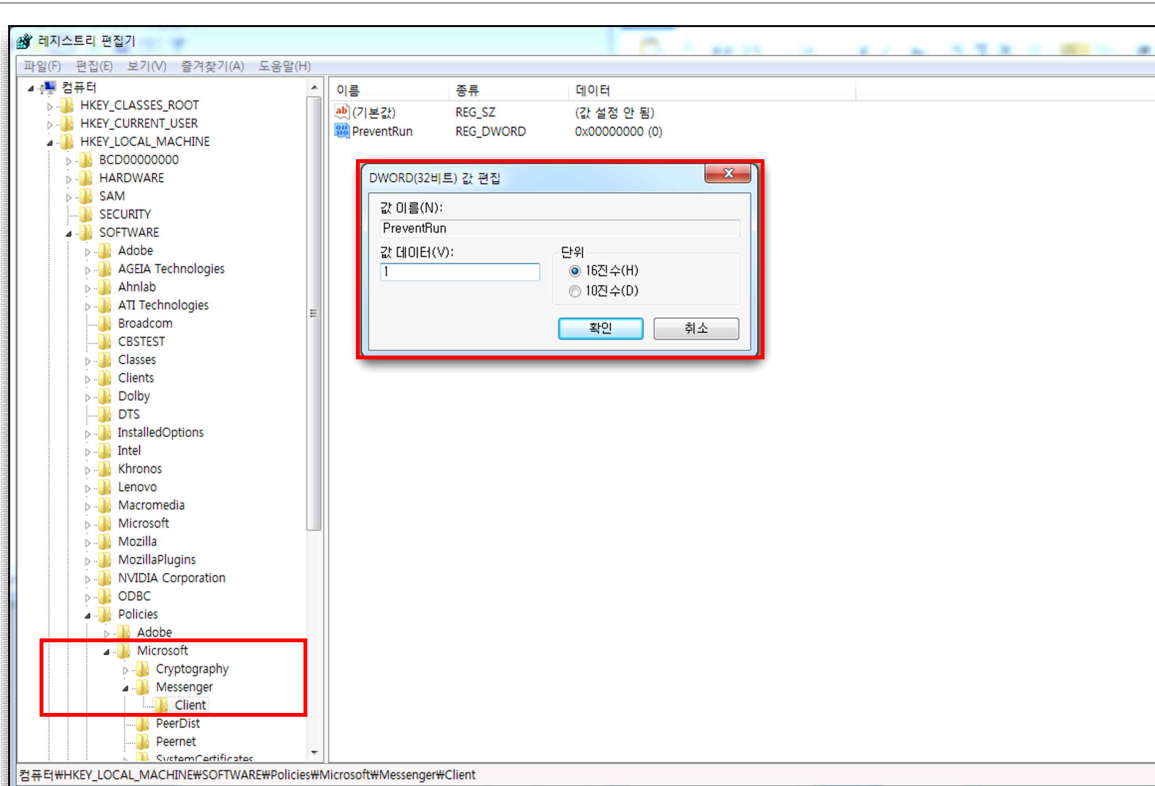
HKLM\Software\Policies\Microsoft\Messenger\Client

(3) 설정 값 입력

|                   |                           |
|-------------------|---------------------------|
| <b>Value name</b> | PreventRun                |
| <b>Data Type</b>  | DWORD 값                   |
| <b>Value</b>      | 1<br>※ Default 값: 0(zero) |

※ "Windows Messenger를 실행하지 않음" 설정이 "사용 안 함"으로 설정되어 있는 경우 레지스트리 편집기 내 Messenger 항목이 존재하며, "사용"인 경우는 존재하지 않음

## PC



## 조치 시 영향

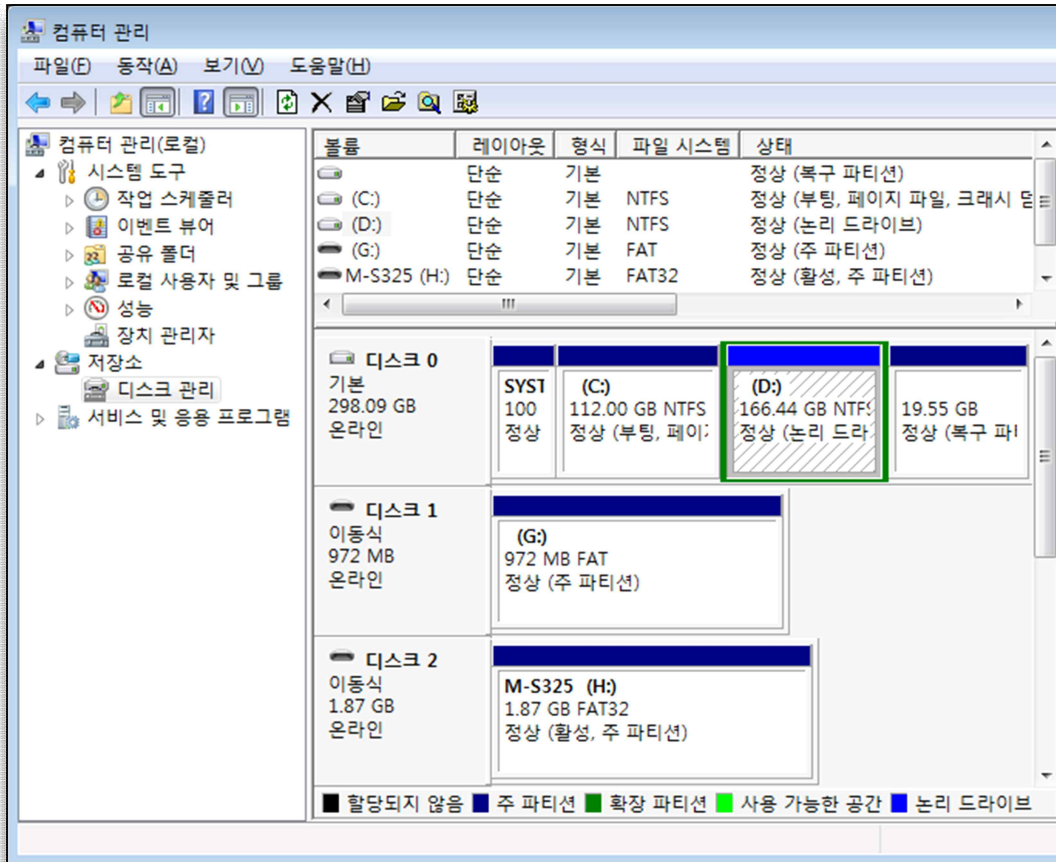
Windows Messenger 사용 불가

원격 지원에서도 Windows Messenger를 사용할 수 없음

## PC

| 취약점 항목                                                                                                   | 2.4. 파일 시스템을 NTFS로 포맷                                                                                                                                                                                                                                                       |     |   |      |       |
|----------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----|---|------|-------|
| 대상 OS                                                                                                    | Windows XP, Windows 7                                                                                                                                                                                                                                                       | 위험도 | 중 | Code | PC-07 |
| 취약점 개요                                                                                                   | *NTFS 파일 시스템은 포맷 시 모든 파일과 디렉터리에 소유권과 사용 권한 설정이 가능하고 ACL(접근 통제 목록)을 제공함으로써 *FAT32 파일 시스템에 비해 보다 강화된 보안 기능을 제공함.<br>기존에 FAT 파일 시스템을 사용하다가 NTFS로 변환하기 위해서는 convert.exe 명령을 사용할 수 있지만 FAT 파일 시스템으로 운영 중 변환해야 하는 경우 Default ACL이 적용되지 않으므로 가능한 초기 설치 시 NTFS 파일 시스템을 선택하는 것을 권장함. |     |   |      |       |
|                                                                                                          | *NTFS, FAT32 파일 시스템 비교: FAT32에는 NTFS가 제공하는 보안 기능이 없으므로 컴퓨터에 FAT32 파티션 또는, 볼륨이 있는 경우 컴퓨터에 액세스 가능한 모든 사용자가 파일을 읽을 수 있으며 FAT32에는 크기 제한이 있음.                                                                                                                                    |     |   |      |       |
|                                                                                                          |                                                                                                                                                                                                                                                                             |     |   |      |       |
| 보안대책                                                                                                     |                                                                                                                                                                                                                                                                             |     |   |      |       |
| 판단기준                                                                                                     | 양호: 모든 디스크 볼륨의 파일 시스템이 NTFS인 경우                                                                                                                                                                                                                                             |     |   |      |       |
|                                                                                                          | 취약: 모든 디스크 볼륨의 파일 시스템이 FAT32인 경우                                                                                                                                                                                                                                            |     |   |      |       |
| 조치방법                                                                                                     | 모든 디스크 볼륨에 대해 파일 시스템 NTFS로 변경                                                                                                                                                                                                                                               |     |   |      |       |
| 보안설정방법                                                                                                   |                                                                                                                                                                                                                                                                             |     |   |      |       |
| ■ Windows XP, Windows 7                                                                                  |                                                                                                                                                                                                                                                                             |     |   |      |       |
| 1. 디스크 볼륨의 파일 시스템이 "NTFS"인지 확인<br>제어판> 관리 도구> 컴퓨터 관리> 저장소> 디스크 관리<br>(시작> 실행> "diskmgmt.msc" 입력> 디스크 관리) |                                                                                                                                                                                                                                                                             |     |   |      |       |
| 2. 모든 디스크 볼륨의 파일 시스템이 "NTFS"가 아닌 경우 취약점 존재하므로, 모든 디스크 볼륨에 대해 파일 시스템 "NTFS"로 변경                           |                                                                                                                                                                                                                                                                             |     |   |      |       |

## PC



2. CMD 명령어를 이용하여 "NTFS" 포맷으로 설정을 변경하는 방법 (※ 관리자 권한으로 cmd 실행 방법 부록 참조)

- Windows 7: 관리자 권한으로 "cmd.exe" 실행 후 "convert 드라이브명:/fs:ntfs" 입력
- Windows XP: 시작> 실행> "cmd" 입력> "convert 드라이브명:/fs:ntfs" 입력

(예) convert h: /fs:ntfs 입력하면 H 드라이브는 NTFS 형식으로 포맷됨

## PC

```

관리자: C:\windows\system32\cmd.exe

C:\W>convert h:/fs:ntfs
파일 시스템 유형은 FAT32입니다.
KISA_TEST 볼륨을 2013-12-05 오후 4:36에 만들었습니다.
볼륨 일련 번호는 BE13-760C입니다.
파일과 폴더를 확인하는 중입니다...
파일과 폴더를 확인했습니다.
Windows에서 파일 시스템에 문제가 없음을 확인했습니다.

전체 디스크 공간: 2,000,650,240바이트
사용 가능한 디스크 공간: 2,000,646,144바이트

각 할당 단위: 4,096바이트
디스크의 전체 할당 단위 개수: 488,440개
디스크에서 사용 가능한 할당 단위 개수: 488,439개

파일 시스템 변환에 필요한 디스크 공간을 결정합니다.
전체 디스크 공간: 1957856KB
볼륨의 빈 공간: 1953756KB
변환에 필요한 공간: 14049KB
파일 시스템을 변환합니다.
변환이 끝났습니다.

C:\W>

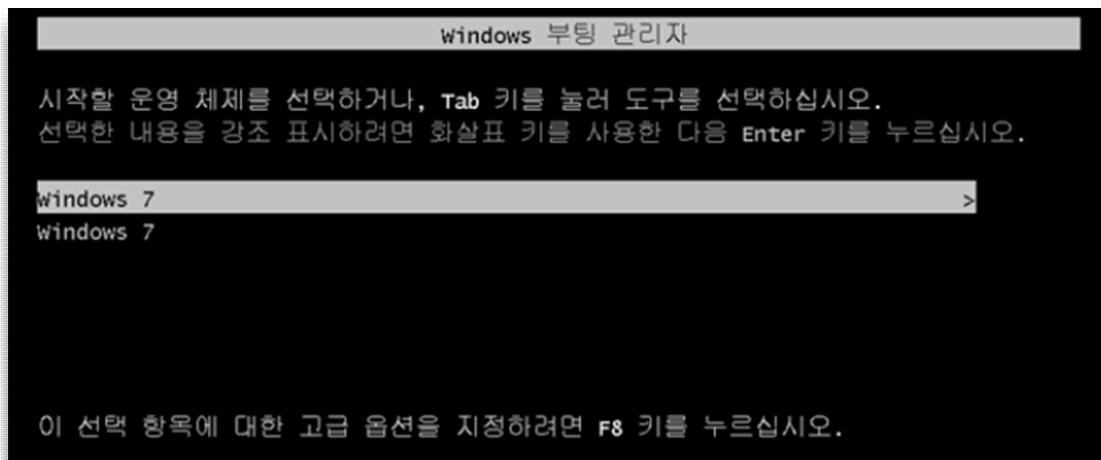
```

조치 시 영향

일반적으로 영향 없음

## PC

| 취약점 항목 | 2.5. 다른 OS로 멀티 부팅 금지                                                                                                                                                                                                                                                                                                                                                                                                      |     |   |      |       |
|--------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----|---|------|-------|
| 대상 OS  | Windows XP, Windows 7                                                                                                                                                                                                                                                                                                                                                                                                     | 위험도 | 중 | Code | PC-08 |
| 취약점 개요 | <p>윈도우 이외의 다른 OS로 *멀티 부팅(Multi booting, 다중 시동)이 가능하도록 설정할 수 있으며, 멀티 부팅이 가능한 경우, 공격자는 해당 PC의 주요 OS 이외에 다른 OS로 부팅하여 파일 시스템에 접근, 주요 정보를 획득할 수 있음.</p> <p>*멀티 부팅(Multi booting, 다중 시동): 한 대의 PC에서 2개 이상의 OS를 설치하는 것을 말하며, PC 전원을 켤 때 시동할 OS를 선택할 수 있음. 멀티 부팅은 개발, 테스트 목적을 위해 여러 운영 체제를 돌리려고 하는 소프트웨어 개발자들이 많이 사용하며, 한 대의 PC에 이러한 시스템을 갖추으로써 하드웨어 비용을 크게 낮출 수 있을 뿐만 아니라 새로운 운영 체제를 "별도의 포맷, 다시 설치 과정 없이" 사용할 수 있다는 장점이 있음.</p> |     |   |      |       |
| 보안대책   |                                                                                                                                                                                                                                                                                                                                                                                                                           |     |   |      |       |
| 판단기준   | 양호: PC 내에 하나의 OS만 설치되어 있는 경우                                                                                                                                                                                                                                                                                                                                                                                              |     |   |      |       |
|        | 취약: PC 내에 하나 이상의 OS가 설치되어 있는 경우                                                                                                                                                                                                                                                                                                                                                                                           |     |   |      |       |
| 조치방법   | 하나의 OS만 설치하여 운영함                                                                                                                                                                                                                                                                                                                                                                                                          |     |   |      |       |
| 보안설정방법 |                                                                                                                                                                                                                                                                                                                                                                                                                           |     |   |      |       |



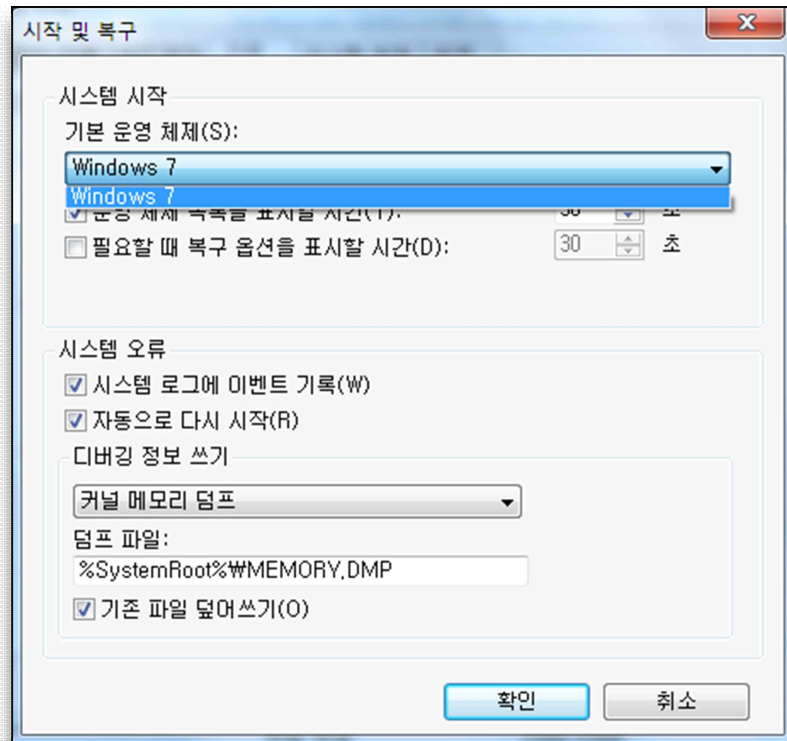
※ 하나 이상의 윈도우 운영체제가 설치된 경우, 시스템 부팅 시 위와 같이 Windows 부팅 관리자에서 시작할 운영 체제를 선택하는 메시지 출력

### ■ Windows XP, Windows 7

#### 1. PC 내 설치된 운영체제 확인

시작> 제어판> 시스템> 고급 시스템 설정> 시작 및 복구 항목의 [설정]  
(시작> 실행> "msconfig" 입력> 시스템 구성 [부팅] 탭에서도 확인 가능)

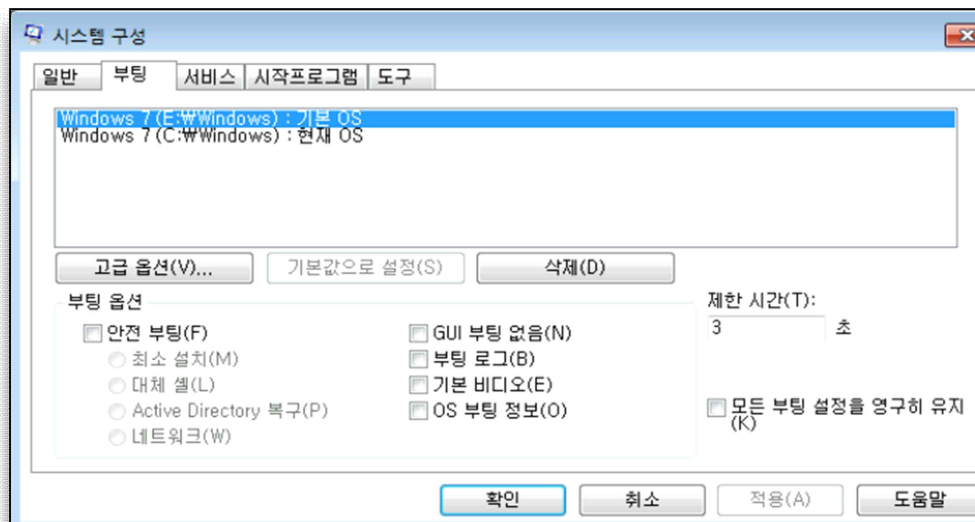
#### 2. "기본 운영 체제" 드롭다운 메뉴에서 2개 이상의 OS가 표시되면 취약점 존재



### 3. 기본 OS 외 설치된 OS 삭제 및 설정 변경

시작 > 실행 > "msconfig" 입력 > 시스템 구성 [부팅] 탭

하나의 OS만 설치하여 사용할 경우 삭제할 OS를 선택 후 [삭제]를 클릭함



※ CMD 명령어를 이용한 멀티 부팅 Windows의 정보 확인 방법 (※ 관리자 권한으로 cmd 실행 방법 부록 참조)

- Windows 7: 관리자 권한으로 "cmd.exe" 실행 후 "bcdedit" 입력
- Windows XP: 시작 > 실행 > "cmd" 입력 > "bcdedit" 입력

## PC

## Windows 부팅 관리자

```

identifier <bootmgr>
device partition=WDevice\HarddiskVolume1
description Windows Boot Manager
locale ko-KR
inherit <globalsettings>
default <default>
resumeobject <99e191ae-5d25-11e2-a2d9-baf82d539ab5>
displayorder <default>
toolsdisplayorder <current>
timeout <mendiag>
timeout 30

```

## Windows 부팅 로더

```

identifier <default>
device partition=E:
path \\Windows\system32\winload.exe
description Windows 7
locale ko-KR
inherit <bootloadersettings>
osdevice partition=E:
systemroot \\Windows
resumeobject <99e191ae-5d25-11e2-a2d9-baf82d539ab5>
nx OptIn

```

## Windows 부팅 로더

```

identifier <current>
device partition=C:
path \\Windows\system32\winload.exe
description Windows 7
locale ko-KR
inherit <bootloadersettings>
recoverysequence <99e191ac-5d25-11e2-a2d9-baf82d539ab5>
recoveryenabled Yes
osdevice partition=C:

```

|         |             |
|---------|-------------|
| 조치 시 영향 | 일반적으로 영향 없음 |
|---------|-------------|



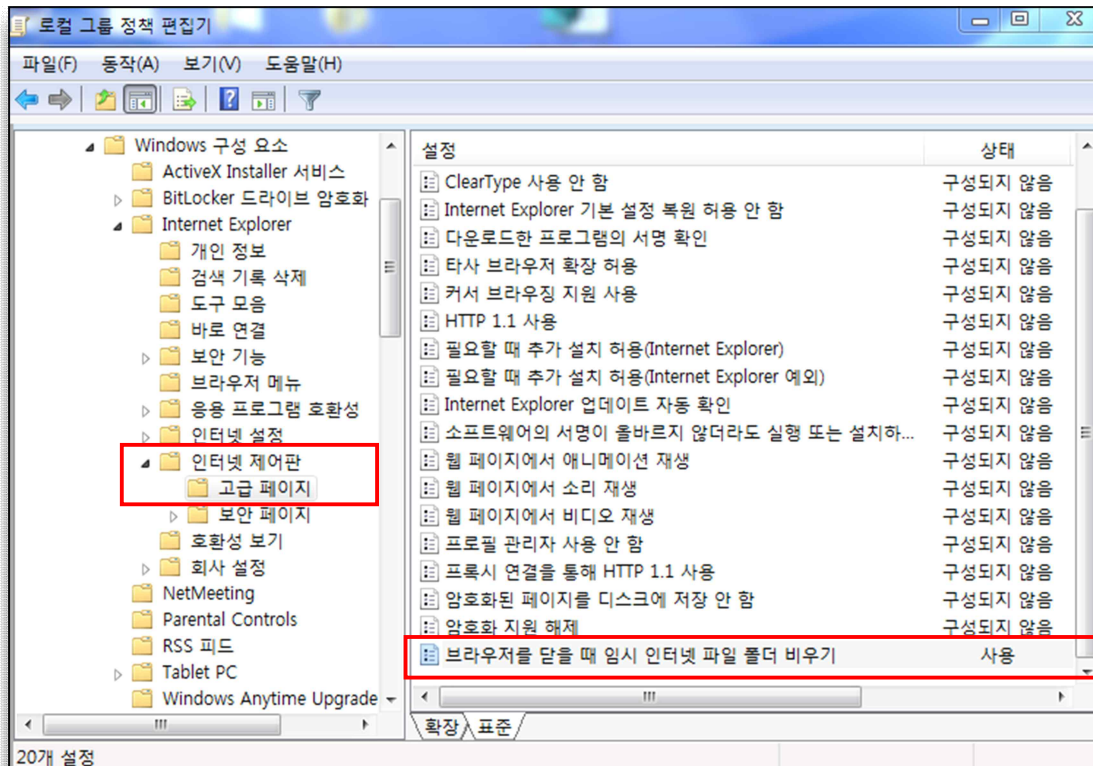


## PC

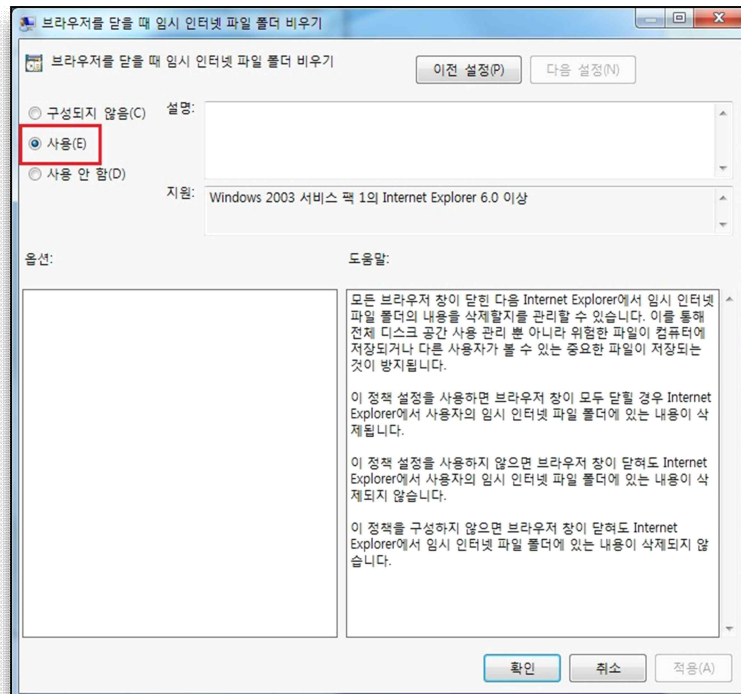
| 취약점 항목 | 2.6. 브라우저 종료 시 임시 인터넷 파일 폴더 내용 삭제                                                                                                                 |     |   |      |       |
|--------|---------------------------------------------------------------------------------------------------------------------------------------------------|-----|---|------|-------|
| 대상 OS  | Windows XP, Windows 7                                                                                                                             | 위험도 | 하 | Code | PC-09 |
| 취약점 개요 | 인터넷 사용 효율을 위해서 브라우저 종료 시 임시 인터넷 파일을 기록할 수 있음.<br>임시 인터넷 파일 폴더를 삭제하지 않을 경우, 다른 사람 계정에 저장된 임시 인터넷 파일 폴더를 통해 이메일 주소, 웹 사이트 접근 기록 등의 개인 정보를 획득할 수 있음. |     |   |      |       |
| 보안대책   |                                                                                                                                                   |     |   |      |       |
| 판단기준   | 양호: "브라우저를 닫을 때 임시 인터넷 파일 폴더 비우기" 설정이 "사용"으로 설정되어 있는 경우                                                                                           |     |   |      |       |
|        | 취약: "브라우저를 닫을 때 임시 인터넷 파일 폴더 비우기" 설정이 "사용"으로 설정되어 있지 않은 경우                                                                                        |     |   |      |       |
| 조치방법   | "브라우저를 닫을 때 임시 인터넷 파일 폴더 비우기"를 "사용"으로 설정                                                                                                          |     |   |      |       |
| 보안설정방법 |                                                                                                                                                   |     |   |      |       |

### ■ Windows XP, Windows 7

- 인터넷 제어판에서 "브라우저를 닫을 때 임시 인터넷 파일 폴더 비우기" 설정 여부 확인  
시작> 실행> "gpedit.msc" 입력> 컴퓨터 구성> 관리 템플릿> Windows 구성 요소>  
Internet Explorer> 인터넷 제어판> 고급 페이지



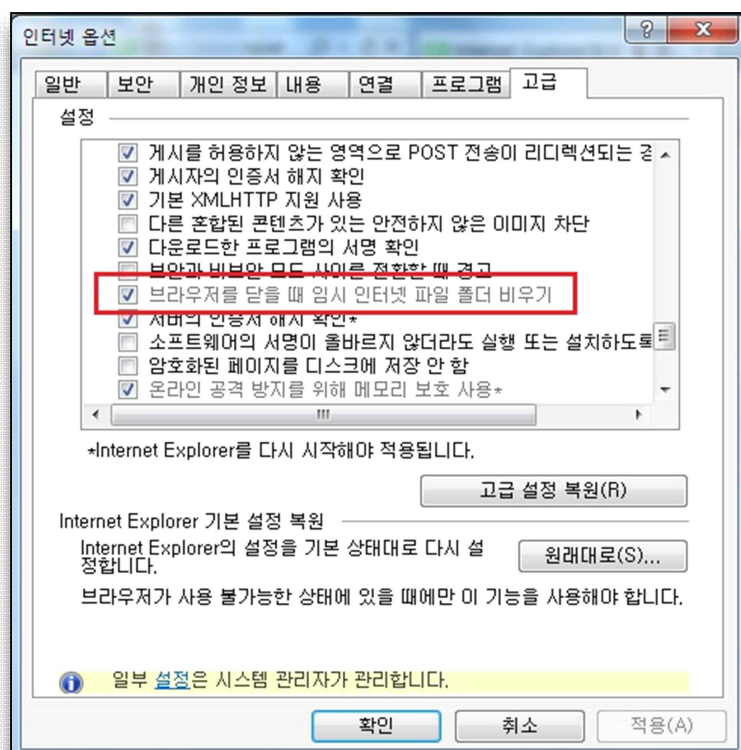
- "브라우저를 닫을 때 임시 인터넷 파일 폴더 비우기"를 선택하여 "사용"으로 속성 변경



### 3. 인터넷 익스플로러에서 설정을 변경하는 방법

인터넷 익스플로러 실행> 도구> 인터넷 옵션> [고급] 탭>

“브라우저를 닫을 때 임시 인터넷 파일 폴더 비우기” 설정을 “사용”으로 설정



## 4. 레지스트리 값으로 설정하는 방법

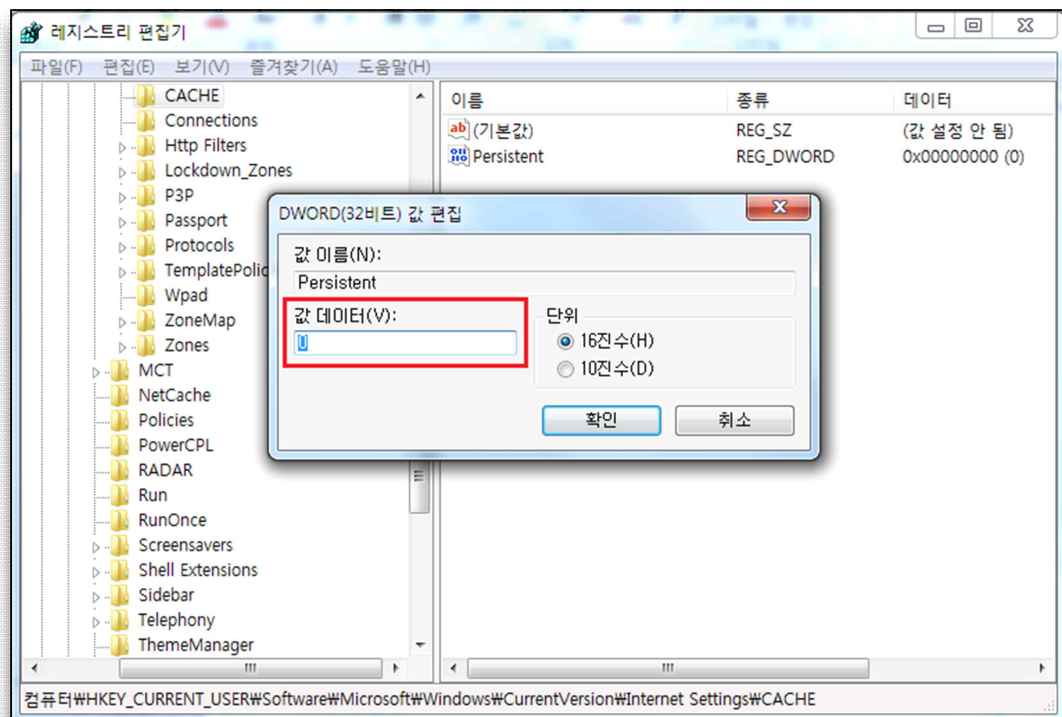
(1) 시작 &gt; 실행 &gt; "regedit" 입력

(2) 레지스트리 경로

HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\InternetSettings\Cache

(3) 설정 값 입력

|                   |            |
|-------------------|------------|
| <b>Value name</b> | Persistent |
| <b>Data Type</b>  | DWORD 값    |
| <b>Value</b>      | 0(zero)    |



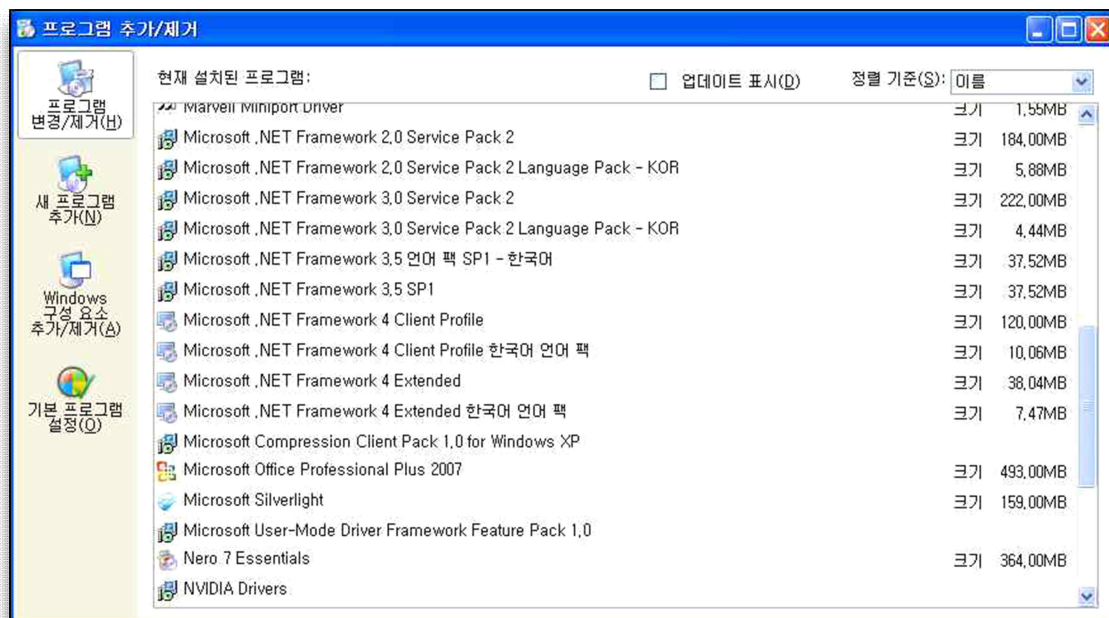
조치 시 영향 | 일반적으로 영향 없음

## 3. 패치 관리

| 취약점 항목 | 3.1. HOT FIX 등 최신 보안패치                                                                                                                                                                                  |     |   |      |       |
|--------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----|---|------|-------|
| 대상 OS  | Windows XP, Windows 7                                                                                                                                                                                   | 위험도 | 상 | Code | PC-10 |
| 취약점 개요 | <p>*HOT FIX 설치 및 자동 *업데이트가 설정되어 있지 않은 경우 취약점으로 인한 공격이 발생할 수 있으므로 Hot Fix 출시 즉시 신속하게 설치하고 항상 최신의 보안 업데이트가 이루어져야 함.</p>                                                                                   |     |   |      |       |
|        | <p>*Hot Fix: 즉시 교정되어야만 하는 주요한 취약점(주로 보안과 관련)을 패치하기 위해 배포되는 프로그램으로 서비스팩이 발표된 이후 패치가 추가될 필요가 있을 때 별도로 발표됨.</p> <p>*업데이트(Update): 문제를 예방 또는 해결하거나 컴퓨터 작동 방식을 향상시키거나 컴퓨팅 경험을 향상시킬 수 있도록 추가되는 소프트웨어를 말함.</p> |     |   |      |       |
| 보안대책   |                                                                                                                                                                                                         |     |   |      |       |
| 판단기준   | 양호: HOT FIX 설치 및 자동 업데이트 설정이 되어 있는 경우                                                                                                                                                                   |     |   |      |       |
|        | 취약: HOT FIX가 설치되어 있지 않은 경우                                                                                                                                                                              |     |   |      |       |
| 조치방법   | Windows Update 사이트에 접속하여 최신 패치 존재 여부 확인 및 패치 적용                                                                                                                                                         |     |   |      |       |
| 보안설정방법 |                                                                                                                                                                                                         |     |   |      |       |

## ■ Windows XP

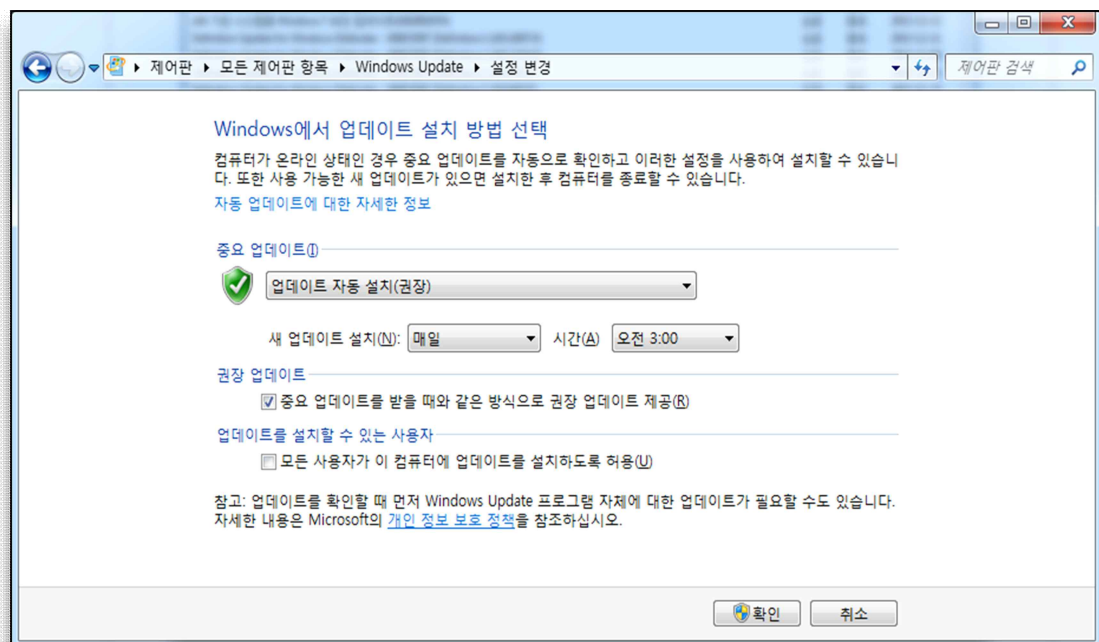
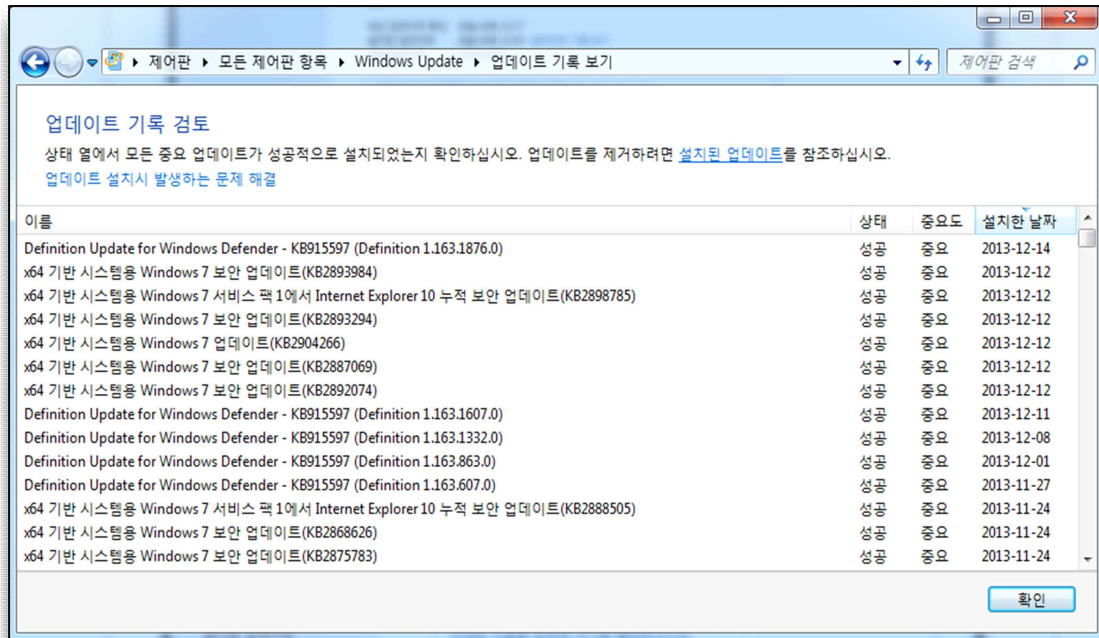
- 인터넷에 연결되는 경우 Windows Update 사이트에 접속하여 최신 패치 존재 여부 확인
- 제어판> 프로그램 추가/제거> HOT FIX, 최신 보안 업데이트 등의 설치 여부 확인  
(시작> 실행> "appwiz.cpl" 입력> 프로그램 추가/제거)  
※ 미설치 또는, 업데이트 필요 시 프로그램 추가/제거 목록 내 해당 프로그램에 [설치] 버튼 활성화



## PC

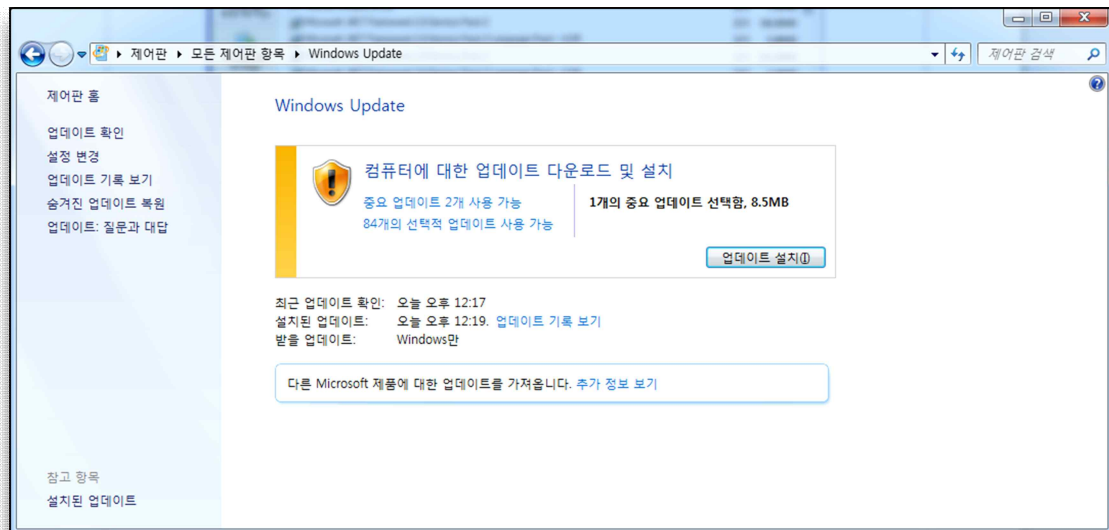
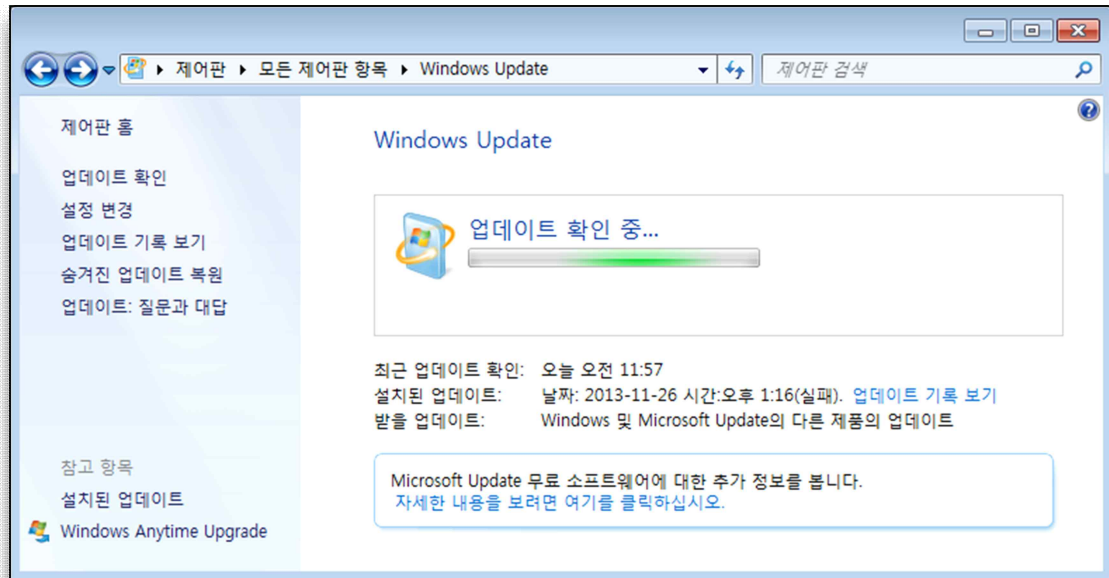
## ■ Windows 7

1. 인터넷에 연결되는 경우 Windows Update 사이트에 접속하여 최신 패치 존재 여부 확인
2. 제어판 > Windows Update > “업데이트 확인”, “설정 변경”, “업데이트 기록 보기”를 통하여 HOT FIX, 최신 보안 업데이트 등의 설치 여부 확인 및 설정 변경





## 3. 업데이트 확인 후 미설치 된 HOT FIX, 최신 보안 업데이트 등의 설치



조치 시 영향

일반적으로 영향 없음

## PC

| 취약점 항목 | 3.2. 항목 최신 서비스팩 적용                                                                                  |     |   |      |       |
|--------|-----------------------------------------------------------------------------------------------------|-----|---|------|-------|
| 대상 OS  | Windows XP, Windows 7                                                                               | 위험도 | 상 | Code | PC-11 |
| 취약점 개요 | 최신 *서비스팩을 적용하지 않을 경우, 공격에 쉽게 노출될 수 있음.                                                              |     |   |      |       |
|        | *서비스팩: Windows 시스템을 마이크로소프트에서 출시하고 난 뒤 Windows와 관련된 응용프로그램, 서비스, 실행 파일 등 여러 수정 파일들을 모아 놓은 프로그램을 말함. |     |   |      |       |
| 보안대책   |                                                                                                     |     |   |      |       |
| 판단기준   | 양호: 최신 서비스팩이 적용 되어 있는 경우                                                                            |     |   |      |       |
|        | 취약: 최신 서비스팩이 적용 되어 있지 않은 경우                                                                         |     |   |      |       |
| 조치방법   | Windows Update 사이트에 접속하여 최신 서비스팩 여부 확인 및 적용                                                         |     |   |      |       |
| 보안설정방법 |                                                                                                     |     |   |      |       |

## ■ Windows XP

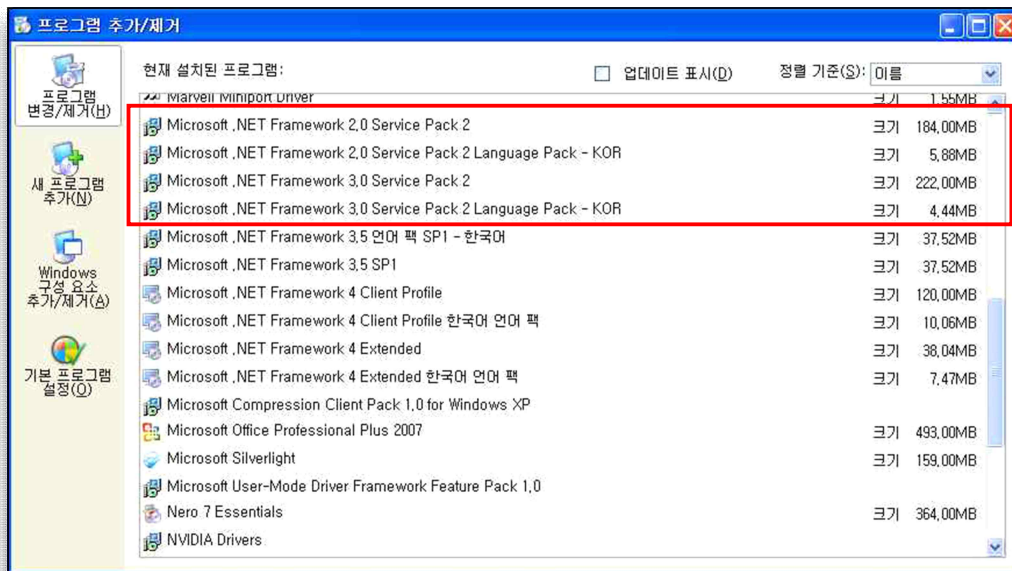
## 1. 현재 시스템에 설치되어 있는 서비스팩 확인

시작&gt; 실행&gt; "winver" 입력&gt; Windows 정보 확인



※ 제어판&gt; 프로그램 추가/제거에서도 설치된 서비스팩 확인 가능





## ■ Windows 7

### 1. 현재 시스템에 설치되어 있는 서비스팩 확인

시작 > 실행 > "winver" 입력 > Windows 정보 확인

### 2. 서비스팩 확인 후 최신 버전이 아닐 경우 Microsoft 홈페이지에서 다운로드하여 설치

※ 네트워크와 분리된 상태에서 서비스팩 설치를 권장함

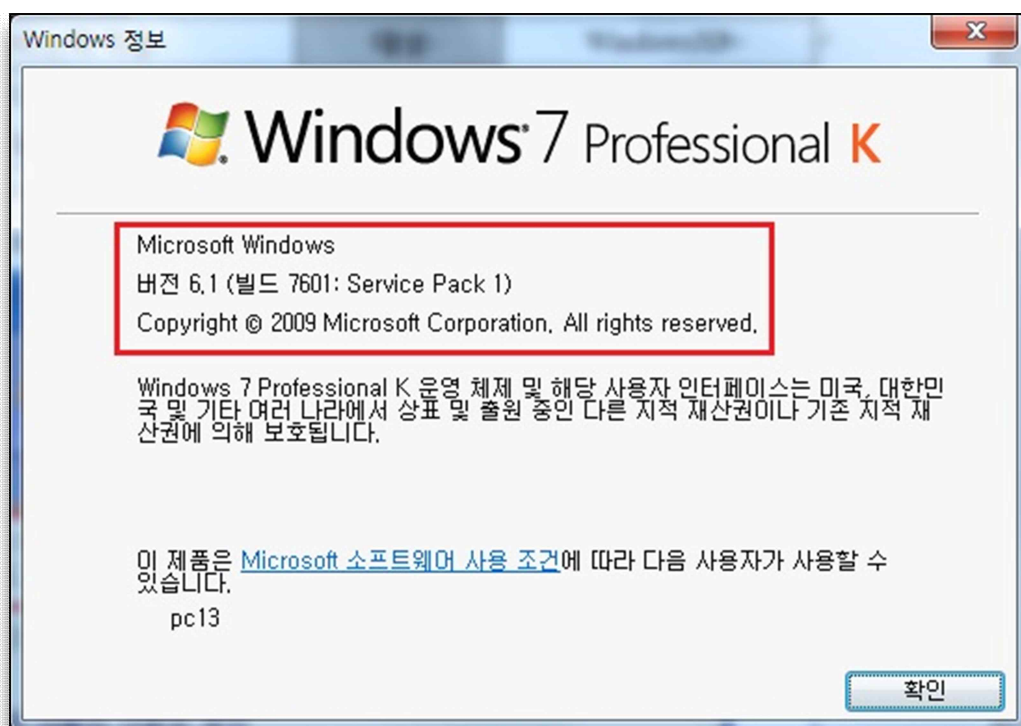
현재 많은 인터넷 \*웜(Worm)이 Windows의 취약점을 이용하여 공격하므로 OS 설치 후 곧바로 네트워크에 연결하는 것은 서버에 피해를 입을 수 있음

\*웜(Worm): 컴퓨터 바이러스의 하나로 컴퓨터 바이러스와는 달리 다른 프로그램을 감염시키지 않고 자기 자신을 복제하면서 통신망 등을 통해 널리 퍼지는 부정 프로그램을 말함.

※ 현재까지 발표된 가장 최신의 Windows 7 의 서비스팩은 SP1 이며,

아래의 Microsoft 홈페이지에서 다운로드 받을 수 있음

<http://windows.microsoft.com/ko-kr/windows/service-packs-download#sptabs=win7>



|         |             |
|---------|-------------|
| 조치 시 영향 | 일반적으로 영향 없음 |
|---------|-------------|

## PC

| 취약점 항목 | 3.3. MS-Office, 한글, 어도비 아크로벳 등의 응용 프로그램에 대한 최신 보안패치 및 벤더 권고사항 적용                                                                                                                          |     |   |      |       |
|--------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----|---|------|-------|
| 대상 OS  | Windows XP, Windows 7                                                                                                                                                                     | 위험도 | 상 | Code | PC-12 |
| 취약점 개요 | 운영체제를 대상으로 한 공격에서 응용프로그램 대상 공격으로 공격 추세가 전환되고 있음. 응용 프로그램 중 국가·공공기관에서 널리 쓰이며, 공격이 용이한 프로그램으로는 MS-Office, 한글, 어도비 아크로벳 등이 있으며 이러한 프로그램들은 해당 응용 프로그램 패치를 적용하여 시스템 권한 획득과 같은 위협으로부터 보호할 수 있음. |     |   |      |       |
| 보안대책   |                                                                                                                                                                                           |     |   |      |       |
| 판단기준   | 양호: 설치된 응용 프로그램의 최신 패치가 적용되어 있는 경우                                                                                                                                                        |     |   |      |       |
|        | 취약: 설치된 응용 프로그램의 최신 패치가 적용되어 있지 않은 경우                                                                                                                                                     |     |   |      |       |
| 조치방법   | 설치된 응용 프로그램의 최신 보안 패치 적용                                                                                                                                                                  |     |   |      |       |
| 보안설정방법 |                                                                                                                                                                                           |     |   |      |       |

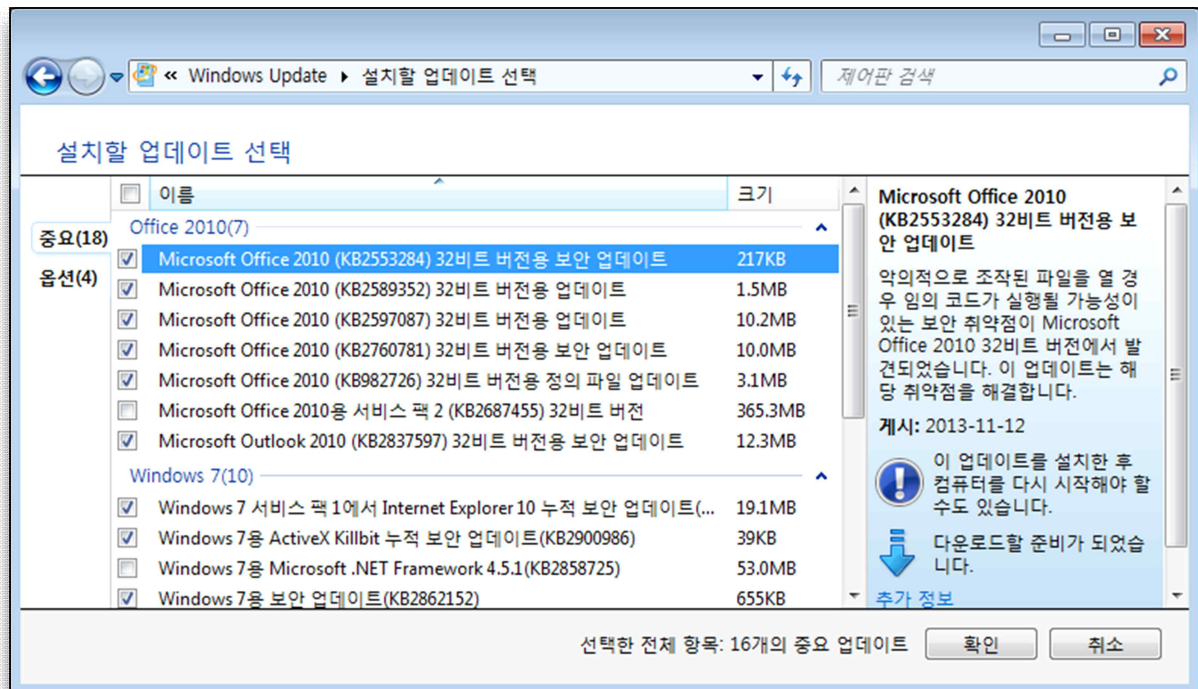
## ■ Windows XP, Windows 7

## ■ MS-Office 관련 업데이트

## 1. MS-Office 관련 업데이트 적용 여부 확인

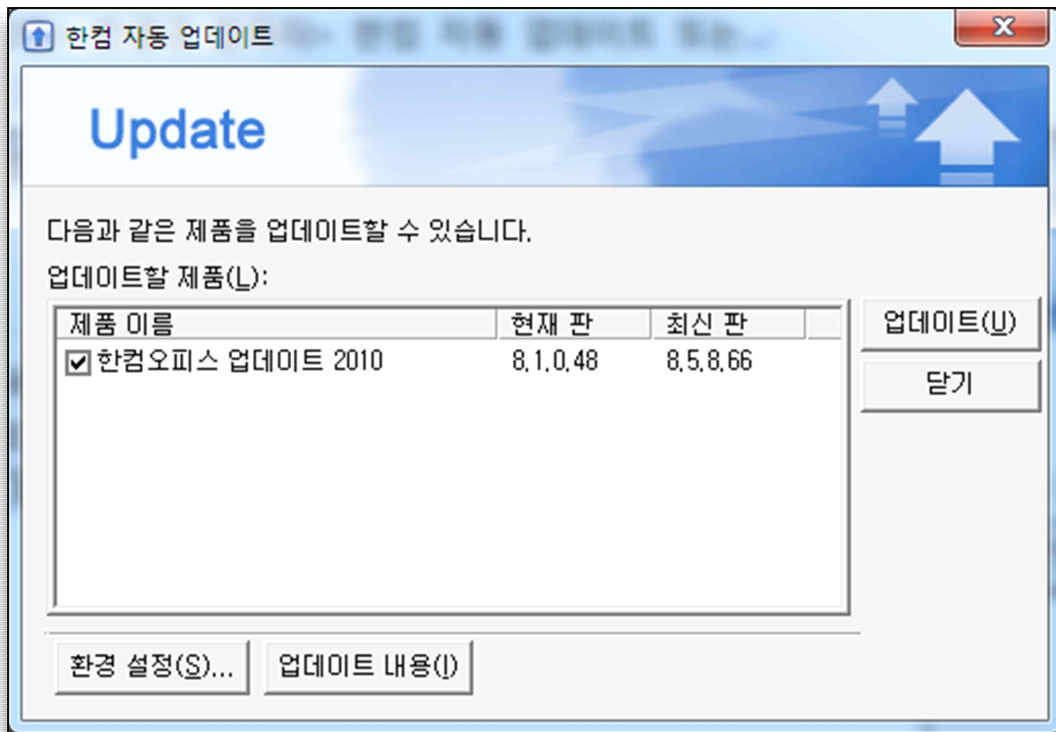
- Windows 7: 제어판> Windows Update> 업데이트 확인> “중요 업데이트” 확인
- Windows XP: Windows XP: 제어판> 프로그램 추가/제거> “중요 업데이트” 확인

## 2. MS-Office 관련 업데이트 적용



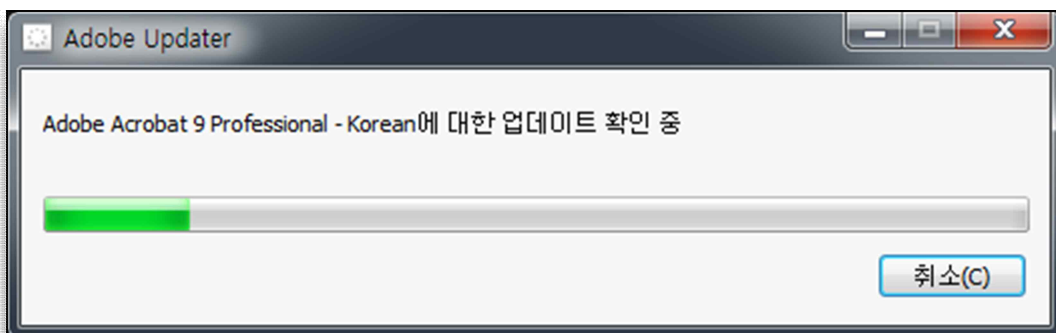
## ■ 한글 업데이트

1. 시작> 프로그램> 한글과 컴퓨터> 한컴 자동 업데이트 또는,  
[한글] 실행> [도움말] 탭> 한글과 컴퓨터 자동 업데이트



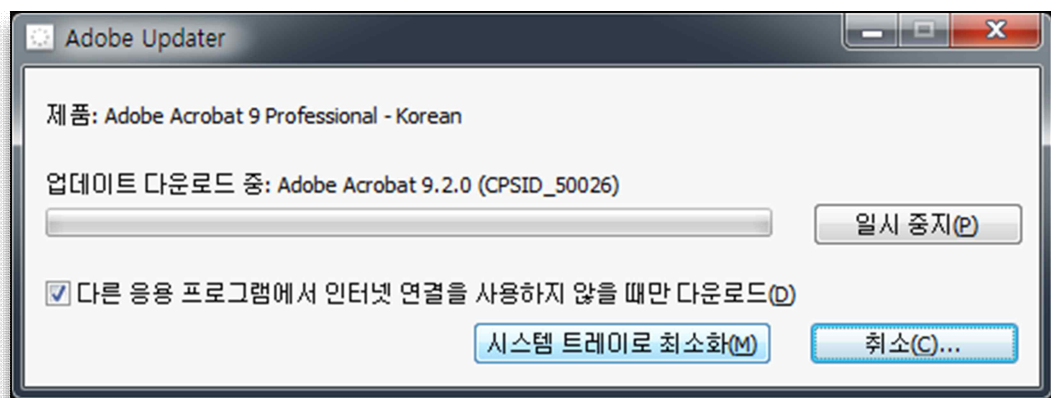
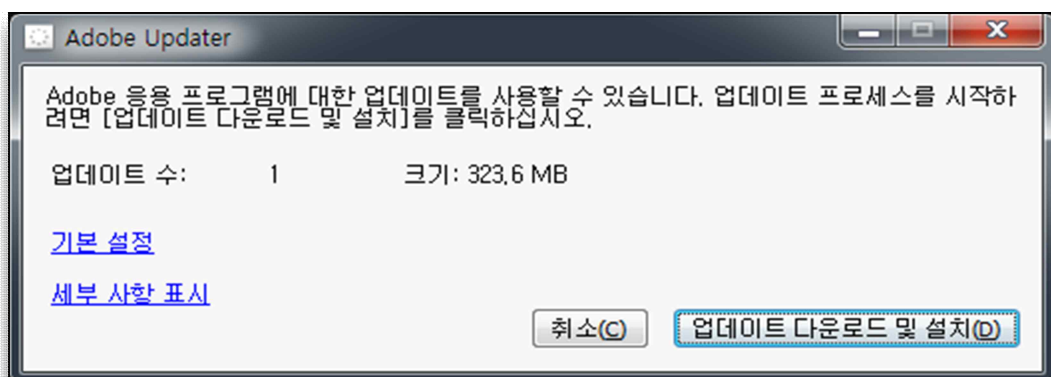
## ■ 어도비 아크로벳 업데이트

1. 어도비 아크로벳 업데이트 확인  
[Adobe Reader] 실행> 도움말> [업데이트 확인] 탭> 업데이트 존재 여부 확인



## PC

## 2. 업데이트 항목 존재 시 [업데이트 다운로드 및 설치]를 클릭하여 진행



|         |             |
|---------|-------------|
| 조치 시 영향 | 일반적으로 영향 없음 |
|---------|-------------|

## 4. 보안 관리

| 취약점 항목 | 4.1. 바이러스 백신 프로그램 설치 및 주기적 업데이트                                                                                                                                                                                                                                                                                                                                                                          |     |   |      |       |
|--------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----|---|------|-------|
| 대상 OS  | Windows XP , Windows 7                                                                                                                                                                                                                                                                                                                                                                                   | 위험도 | 상 | Code | PC-13 |
| 취약점 개요 | <p>바이러스 백신 프로그램은 *바이러스, *웜 등으로부터 시스템을 보호하기 위한 중요한 보안 요소임. 최신 바이러스 탐지를 위하여 패턴 업데이트가 자주 발생하므로 이를 즉각적으로 반영하는 것이 중요함.</p>                                                                                                                                                                                                                                                                                    |     |   |      |       |
|        | <p>*바이러스(Virus): 바이러스는 스스로를 복제하려는 명백한 의도를 갖고 만들어진 코드 사용을 통해 호스트 프로그램에 침투하여 컴퓨터 사이에서 확산을 시도함. 호스트가 실행되면 바이러스도 함께 실행되어 새로운 숙주를 감염시키는 등 시스템에 직접적인 피해를 줌. 이메일이나 다른 외부저장장치를 통해서 다른 PC들로도 전파가 가능하고 전염성이 매우 강해서 PC 내로 들어오면 다른 파일들까지 급속하게 감염시킴.</p> <p>*웜(Worm): 컴퓨터 바이러스의 하나로 컴퓨터 바이러스와 비슷하지만, 바이러스가 다른 실행 프로그램에 기생하여 실행되는 데 반해 웜은 독자적으로 실행되며, 다른 프로그램을 감염시키지 않고 자기 자신을 복제하면서 통신망 등을 통해 널리 퍼지는 부정 프로그램을 말함.</p> |     |   |      |       |
| 보안대책   |                                                                                                                                                                                                                                                                                                                                                                                                          |     |   |      |       |
| 판단기준   | 양호: 백신이 설치되어 있고, 최신 업데이트가 적용 되어 있는 경우                                                                                                                                                                                                                                                                                                                                                                    |     |   |      |       |
|        | 취약: 백신이 설치되어 있지 않거나, 최신 업데이트가 적용 되어 있지 않은 경우                                                                                                                                                                                                                                                                                                                                                             |     |   |      |       |
| 조치방법   | 바이러스 백신 설치 및 최신 업데이트 적용                                                                                                                                                                                                                                                                                                                                                                                  |     |   |      |       |
| 보안설정방법 |                                                                                                                                                                                                                                                                                                                                                                                                          |     |   |      |       |

## ■ Windows XP (V3 스마트 업데이트 사용 예시)

## 1. [V3] 실행&gt; [업데이트] 실행

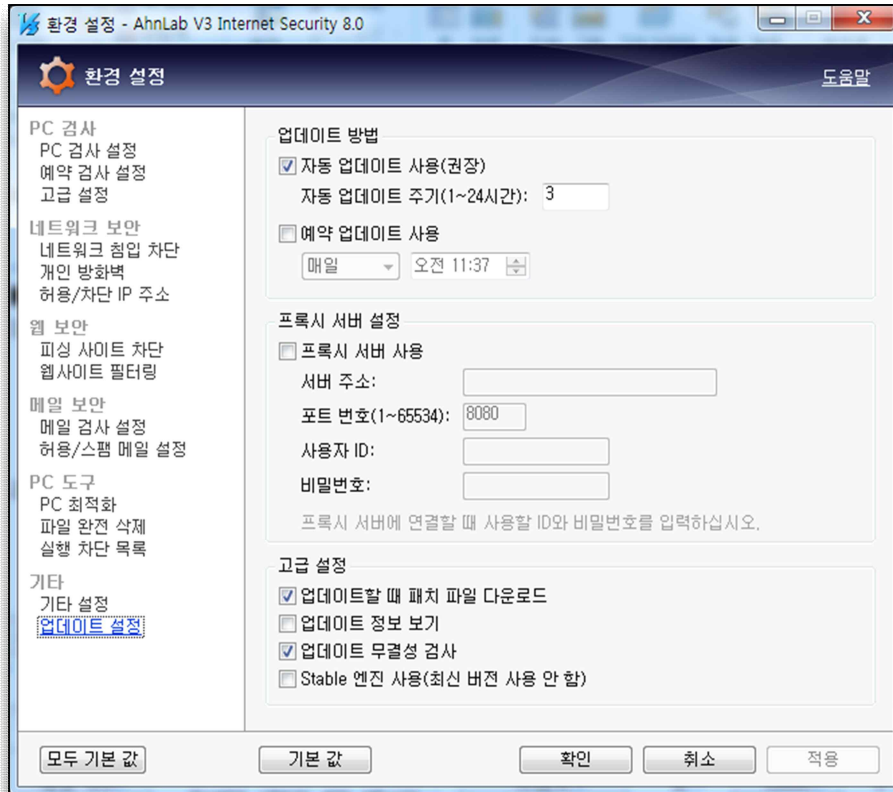




## PC

## ■ Windows 7 (V3 Internet Security 8.0 사용 예시)

1. V3 Internet security 8.0 설치 여부 및 업데이트 설정 확인
2. V3 Internet security 8.0 업데이트 적용



조치 시 영향 | 일반적으로 영향 없음

## PC

| 취약점 항목 | 4.2. 바이러스 백신 프로그램에서 제공하는 실시간 감시 기능 활성화                                                                                                                                                                                                                                                                                                                                                                                                                                           |     |   |      |       |
|--------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----|---|------|-------|
| 대상 OS  | Windows XP, Windows 7                                                                                                                                                                                                                                                                                                                                                                                                                                                            | 위험도 | 상 | Code | PC-14 |
| 취약점 개요 | <p>바이러스 백신 프로그램의 실시간 감시 기능으로 *바이러스, *스파이웨어 탐지 및 방화벽 설정 등이 가능함. 시스템에 대한 위협 발생 시 즉시 대응이 가능하도록 실시간 감시 기능을 사용할 것을 권고함.</p> <p>*바이러스(Virus): 바이러스는 스스로를 복제하려는 명백한 의도를 갖고 만들어진 코드 사용을 통해 호스트 프로그램에 침투하여 컴퓨터 사이에서 확산을 시도함. 호스트가 실행되면 바이러스도 함께 실행되어 새로운 숙주를 감염시키는 등 시스템에 직접적인 피해를 줌. 이메일이나 다른 외부저장장치를 통해서 다른 PC들로도 전파가 가능하고 전염성이 매우 강해서 PC 내로 들어오면 다른 파일들까지 급속하게 감염시킴.</p> <p>*스파이웨어: 사용자의 동의 없이 설치되어 컴퓨터의 정보를 수집하고 전송하는 악성코드로, 신용카드와 같은 금융정보 및 주민등록번호와 같은 신상정보, 암호를 비롯한 각종 정보를 수집함.</p> |     |   |      |       |
| 보안대책   |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |     |   |      |       |
| 판단기준   | 양호: 설치된 백신의 실시간 감시 기능이 활성화 되어 있는 경우                                                                                                                                                                                                                                                                                                                                                                                                                                              |     |   |      |       |
|        | 취약: 백신이 설치되어 있지 않거나, 실시간 감시 기능이 비활성화 되어 있는 경우                                                                                                                                                                                                                                                                                                                                                                                                                                    |     |   |      |       |
| 조치방법   | 백신을 설치하고 실시간 감시 기능을 활성화함                                                                                                                                                                                                                                                                                                                                                                                                                                                         |     |   |      |       |
| 보안설정방법 |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |     |   |      |       |

## ■ Windows XP (V3 스마트 업데이트 사용 예시)

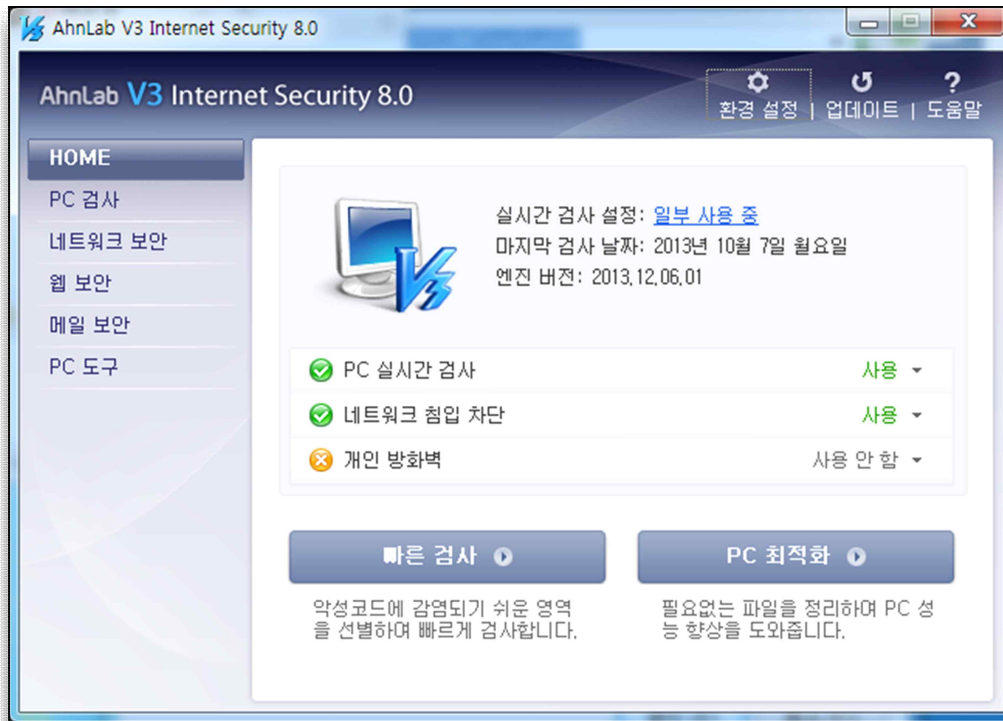
### 1. 백신의 실시간 검사 기능 활성화





## ■ Windows 7 (V3 Internet Security 8.0 사용 예시)

### 1. 백신의 실시간 검사 기능 활성화



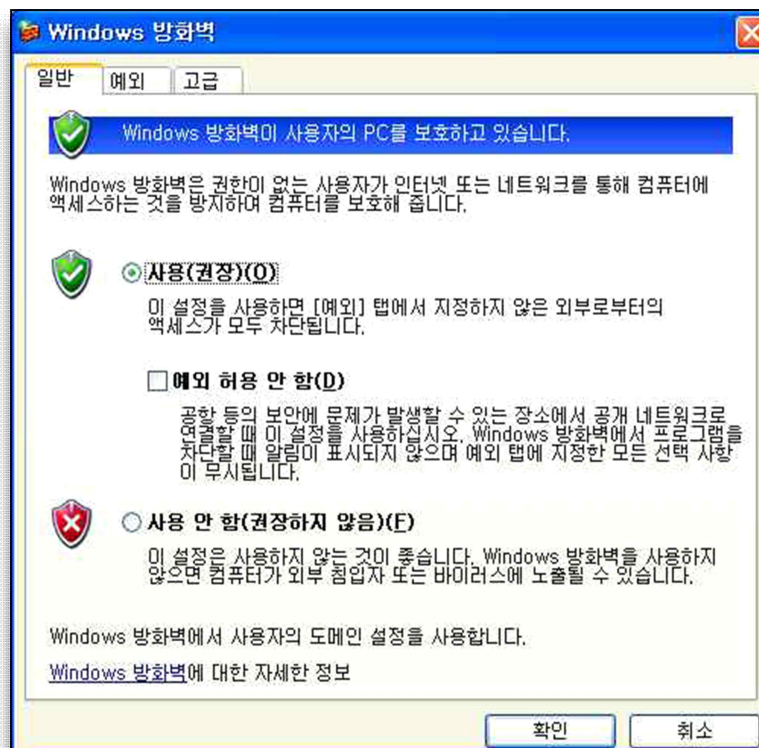
|         |             |
|---------|-------------|
| 조치 시 영향 | 일반적으로 영향 없음 |
|---------|-------------|

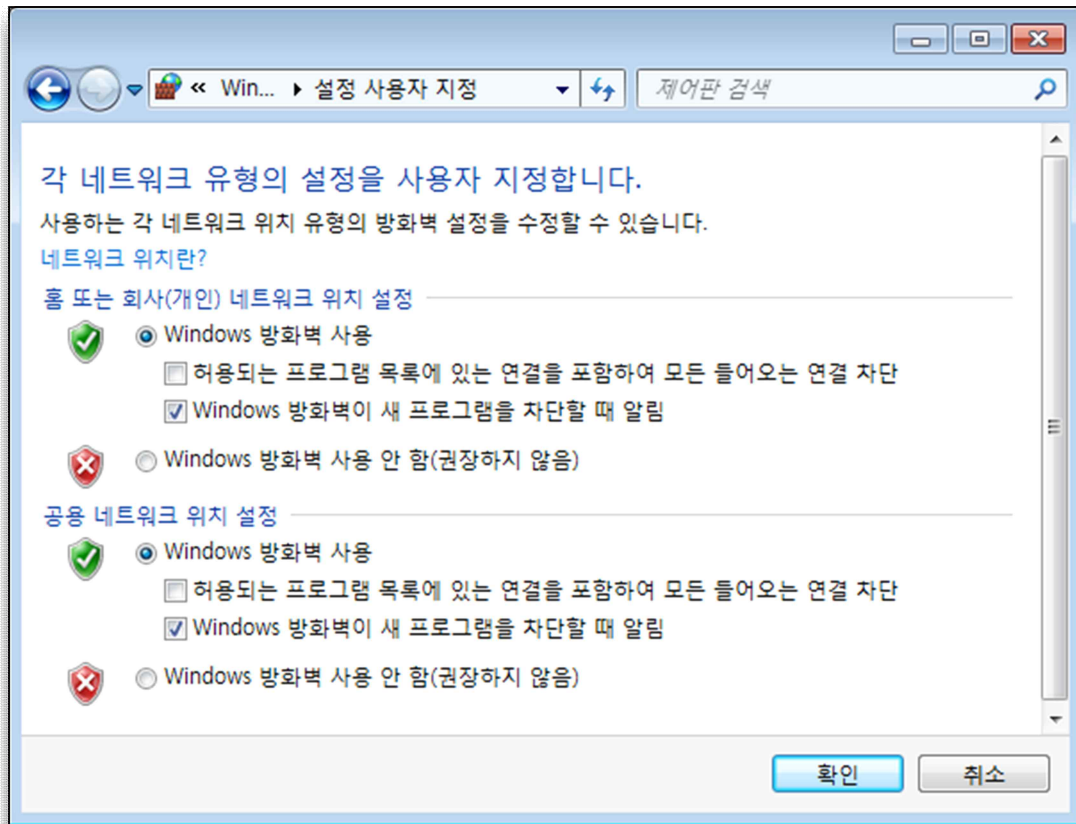
## PC

| 취약점 항목 | 4.3. OS에서 제공하는 침입차단 기능 활성화                                                                                                                                      |     |   |      |       |
|--------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------|-----|---|------|-------|
| 대상 OS  | Windows XP, Windows 7                                                                                                                                           | 위험도 | 상 | Code | PC-15 |
| 취약점 개요 | <p>윈도우에서 제공하는 침입차단 기능인 윈도우 방화벽을 사용함으로써 PC의 자료 유출 방지, 불법 접근 차단 등을 가능하게 함.</p> <p>네트워크 방화벽과 더불어 각각의 PC에 윈도우 방화벽과 같은 호스트 기반의 방화벽을 구현할 때 네트워크의 방어 수준이 향상될 수 있음.</p> |     |   |      |       |
| 보안대책   |                                                                                                                                                                 |     |   |      |       |
| 판단기준   | 양호: Windows 방화벽 "사용"으로 설정되어 있는 경우                                                                                                                               |     |   |      |       |
|        | 취약: Windows 방화벽 "사용 안 함"으로 설정되어 있는 경우                                                                                                                           |     |   |      |       |
| 조치방법   | Windows 방화벽 "사용"으로 설정                                                                                                                                           |     |   |      |       |
| 보안설정방법 |                                                                                                                                                                 |     |   |      |       |

### ■ Windows XP, Windows 7

1. 시작> 제어판> Windows 방화벽> Windows 방화벽 설정 또는 해제  
(시작> 실행> “firewall.cpl” 입력)
2. Windows 방화벽 “사용” 설정  
(Windows XP의 경우 [일반] 탭에서 “사용(권장)” 설정)





## 2. 레지스트리 값으로 설정하는 방법

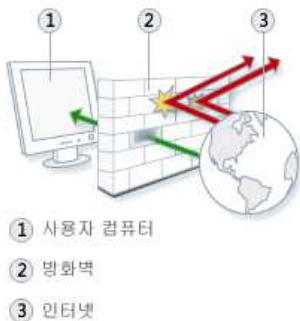
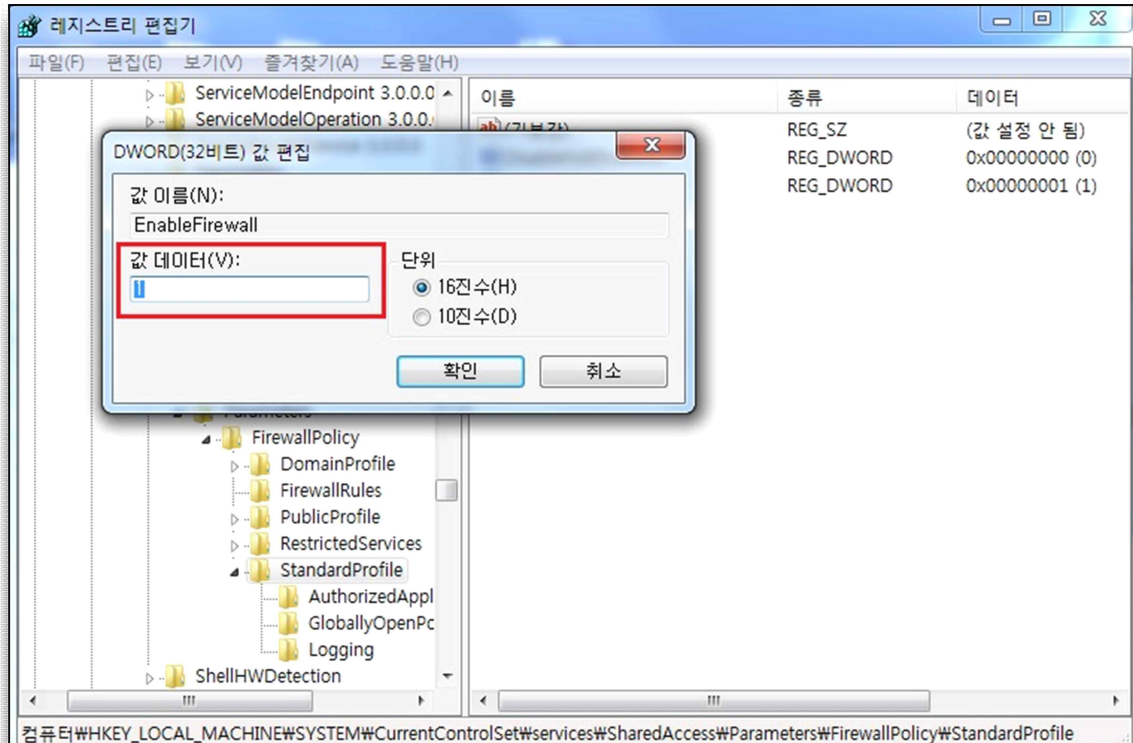
(1) 시작 > 실행 > "regedit" 입력

(2) 레지스트리 경로

HKLM\SYSTEM\CurrentControlSet\Services\SharedAccess\Parameters\  
FirewallPolicy\StandardProfile

(3) 설정 값 입력

|                   |                |
|-------------------|----------------|
| <b>Value name</b> | EnableFirewall |
| <b>Data Type</b>  | DWORD 값        |
| <b>Value</b>      | 1              |



#### ※ 방화벽이란?

방화벽은 인터넷 또는 네트워크에서 들어오는 정보를 확인한 다음 방화벽 설정에 따라 이를 컴퓨터로 전달하는 것을 차단하거나 허용하는 소프트웨어 또는 하드웨어를 말함

방화벽은 해커 또는 악성 소프트웨어가 네트워크나 인터넷을 통해 사용자 컴퓨터에 액세스하지 못하도록 방지하며, 사용자 컴퓨터에서 다른 컴퓨터로 악성 소프트웨어를 보내지 못하도록 방지함

방화벽은 바이러스 백신 프로그램이 아니며, 컴퓨터를 안전하게 보호하기 위해서는 방화벽, 바이러스 백신 및 맬웨어 방지 프로그램이 모두 설치되어야 함

조치 시 영향

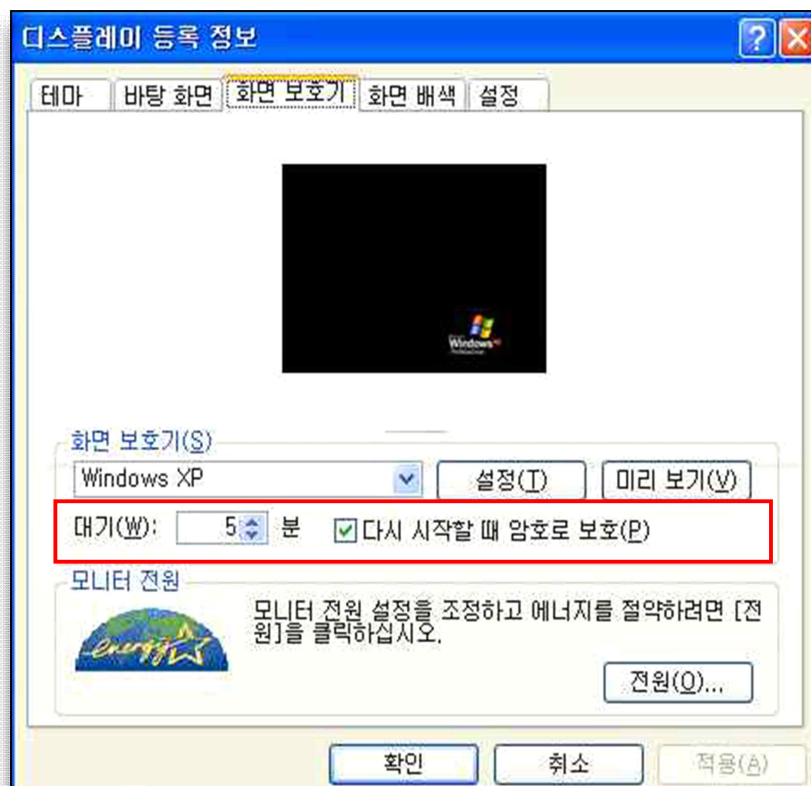
일반적으로 영향 없음

## PC

| 취약점 항목 | 4.4. 화면보호기 대기 시간 설정 및 재시작 시 암호 보호 설정                                                                                                                                                                                         |     |   |      |       |
|--------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----|---|------|-------|
| 대상 OS  | Windows XP, Windows 7                                                                                                                                                                                                        | 위험도 | 상 | Code | PC-16 |
| 취약점 개요 | 사용자가 일정 시간 동안 아무런 작업을 수행하지 않을 경우 자동으로 로그오프되거나 워크스테이션이 잠기도록 설정하여야 함. 해당 기능을 설정하지 않은 경우 사용자가 자리를 비운 사이에 임의의 사용자가 해당 시스템에 접근하여 중요 정보를 유출하거나, 악의적인 행위를 통해 시스템 운영에 악영향을 미칠 수 있으므로 화면보호기 대기 시간 및 암호 사용 설정을 이용해서 비인가자의 물리적 접근을 차단함. |     |   |      |       |
| 보안대책   |                                                                                                                                                                                                                              |     |   |      |       |
| 판단기준   | 양호: 화면보호기 설정 및 암호로 보호가 설정되어 있는 경우                                                                                                                                                                                            |     |   |      |       |
|        | 취약: 화면보호기 설정 및 암호로 보호가 설정되어 있지 않은 경우                                                                                                                                                                                         |     |   |      |       |
| 조치방법   | 화면보호기 설정 및 암호로 보호 설정                                                                                                                                                                                                         |     |   |      |       |
| 보안설정방법 |                                                                                                                                                                                                                              |     |   |      |       |

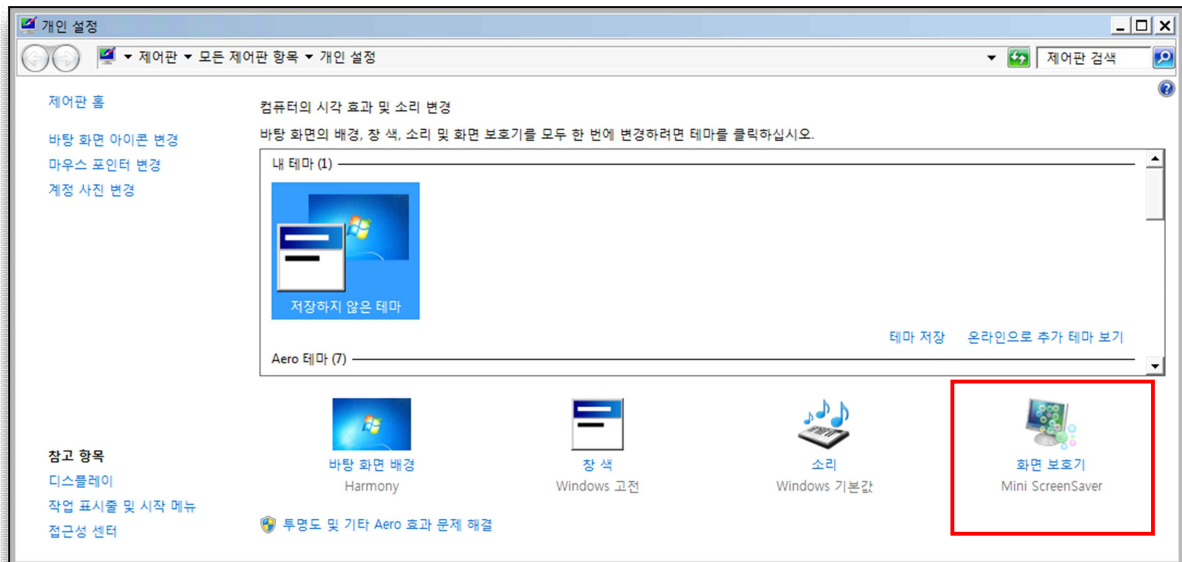
## ■ Windows XP

1. 시작> 제어판> 디스플레이> 디스플레이 등록 정보 [화면 보호기] 탭
2. 대기 시간을 5분~10분 사이로 설정 후 “다시 시작할 때 암호로 보호” 체크



## ■ Windows 7

1. 시작> 제어판> 개인 설정> 화면보호기
2. 대기 시간을 5분~10분 사이로 설정 후 “다시 시작할 때 로그인 화면 표시(R)” 체크



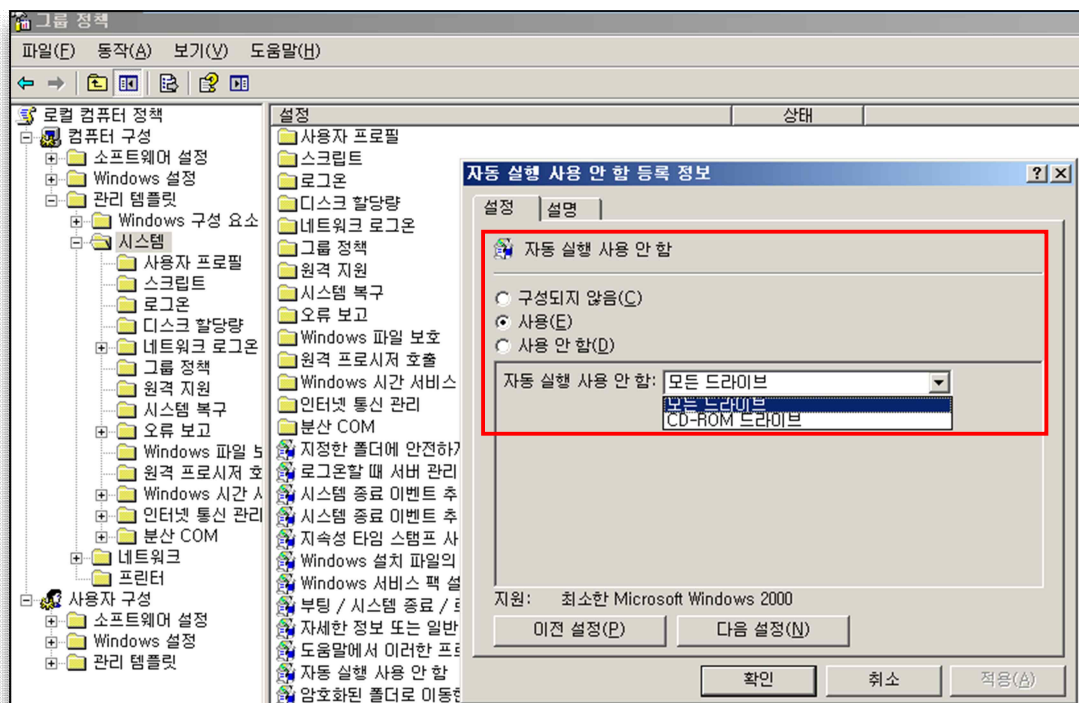
조치 시 영향      일반적으로 영향 없음



| 취약점 항목 | 4.5. CD, DVD, USB 메모리 등과 같은 미디어의 자동실행 방지 등<br>이동식 미디어에 대한 보안대책 수립                                                                                                                                                                                                                                              |     |   |      |       |
|--------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----|---|------|-------|
| 대상 OS  | Windows XP, Windows 7                                                                                                                                                                                                                                                                                          | 위험도 | 상 | Code | PC-17 |
| 취약점 개요 | <p>CD/DVD, USB 메모리 등과 같은 미디어에 탑재된 *Autorun.inf 파일을 통해 다른 응용 프로그램이 자동 실행될 수 있음. 대부분의 USB 관련 악성코드들은 Autorun.inf 파일을 통해 자동 실행되도록 제작되므로 이를 통해 악성코드가 PC로 쉽게 유입될 수 있음.</p> <p>*Autorun.inf 파일: 윈도우 운영체제의 AutoRun, AutoPlay 기능에 사용되는 텍스트 파일. 미디어 장치의 루트 디렉터리에 위치하며, 미디어(CD/DVD, USB) 연결 시 특정 프로그램이 자동으로 실행되도록 제어함</p> |     |   |      |       |
| 보안대책   |                                                                                                                                                                                                                                                                                                                |     |   |      |       |
| 판단기준   | 양호: 미디어 사용 시 자동 실행되지 않는 경우                                                                                                                                                                                                                                                                                     |     |   |      |       |
|        | 취약: 미디어 사용 시 자동 실행되는 경우                                                                                                                                                                                                                                                                                        |     |   |      |       |
| 조치방법   | 미디어 자동실행 방지 설정                                                                                                                                                                                                                                                                                                 |     |   |      |       |
| 보안설정방법 |                                                                                                                                                                                                                                                                                                                |     |   |      |       |

## ■ Windows XP

- 시작> 설정> 제어판> 관리도구> 서비스  
(시작> 실행> "gpedit.msc" 입력> 컴퓨터 구성> 관리 템플릿> Windows 구성 요소> 자동 실행 정책)
- "자동 실행 사용 안 함" 정책을 "사용-모든 드라이브"로 설정



## PC

## 3. 레지스트리 값으로 설정하는 방법

(1) 시작 &gt; 실행 &gt; "regedit" 입력

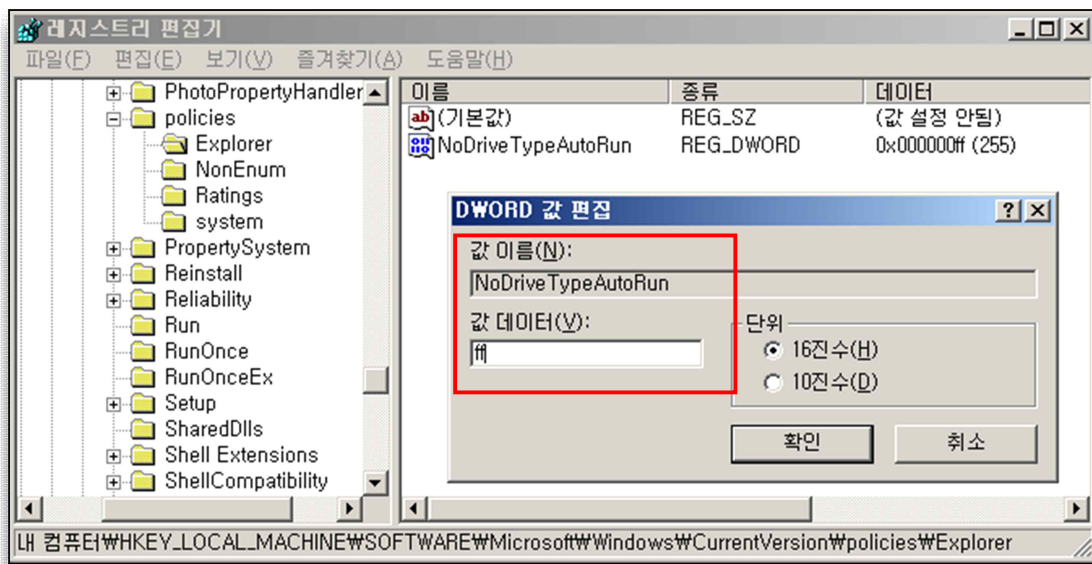
(2) 레지스트리 경로

HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Explorer

(3) 설정 값 입력

|            |                    |
|------------|--------------------|
| Value name | NoDriveTypeAutoRun |
| Data Type  | DWORD 값            |
| Value      | 255(ff)            |

※ NoDriveTypeAutoRun 값이 없을 경우 생성 후 255(ff) 설정



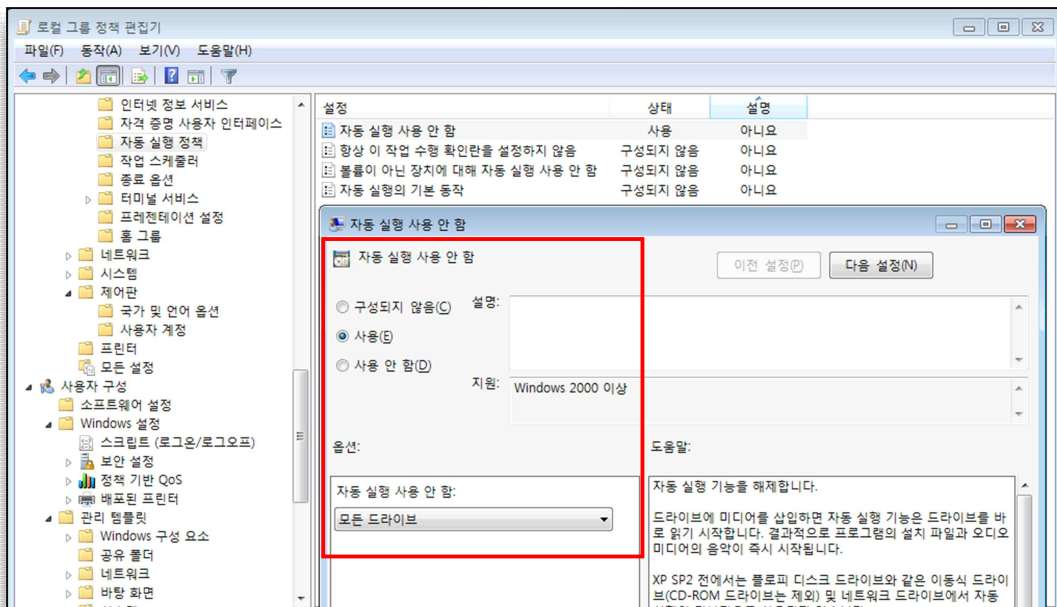
## ■ Windows 7

1. 시작 &gt; 설정 &gt; 제어판 &gt; 관리도구 &gt; 서비스

(시작 &gt; 실행 &gt; "gpedit.msc" 입력 &gt; 컴퓨터 구성 &gt; 관리 템플릿 &gt; Windows 구성 요소 &gt; 자동 실행 정책)

2. "자동 실행 사용 안 함" 정책을 "사용-모든 드라이브"로 설정





### 3. 레지스트리 값으로 설정하는 방법

(1) 시작 > 실행 > "regedit" 입력

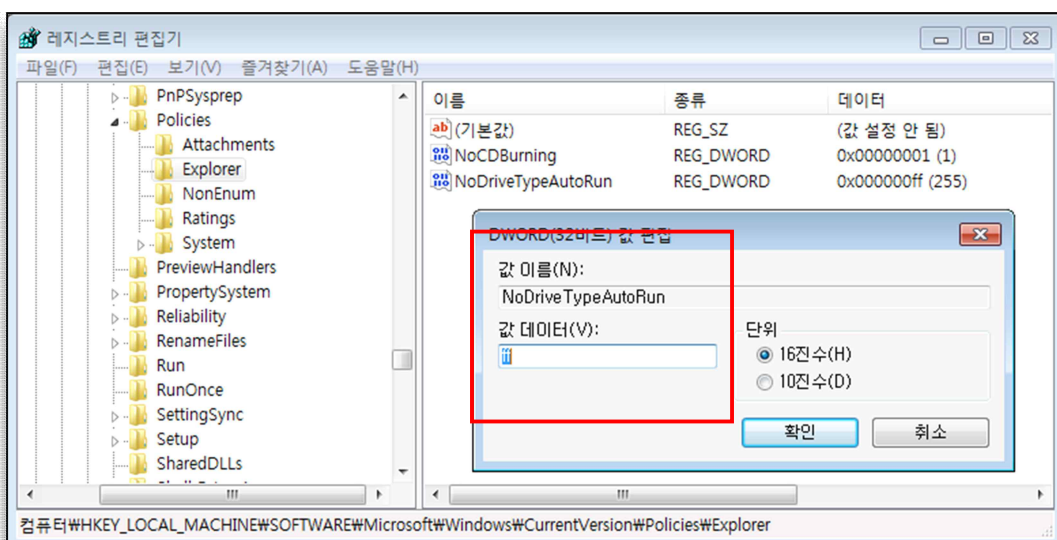
(2) 레지스트리 경로

HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Explorer

(3) 설정 값 입력

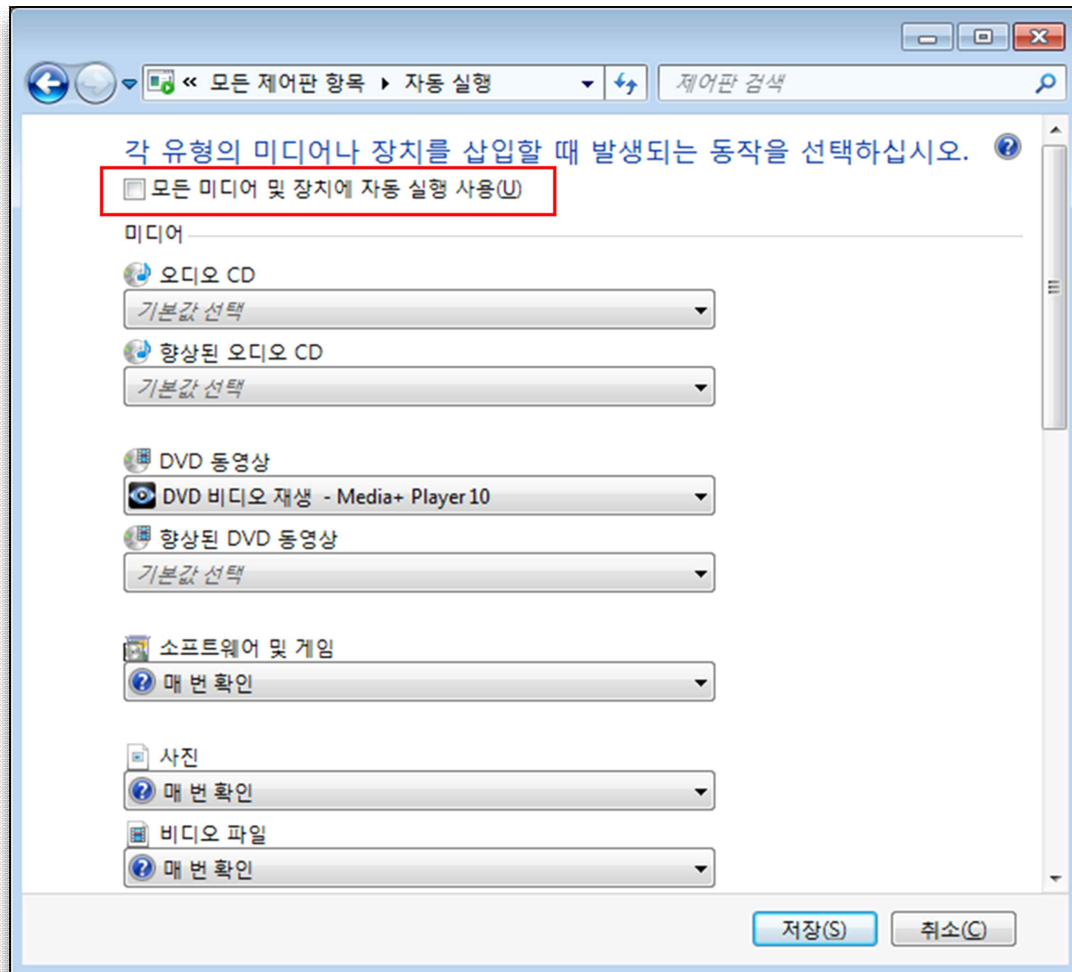
| Value name | NoDriveTypeAutoRun |
|------------|--------------------|
| Data Type  | DWORD 값            |
| Value      | 255(ff)            |

※ NoDriveTypeAutoRun 값이 없을 경우 생성 후 255(ff) 설정



## 4. 제어판에서 자동 실행 기능 설정

시작&gt; 제어판&gt; 자동 실행&gt; “모든 미디어 및 장치에 자동 실행 사용(U)” 체크 해제



조치 시 영향

일반적으로 영향 없음

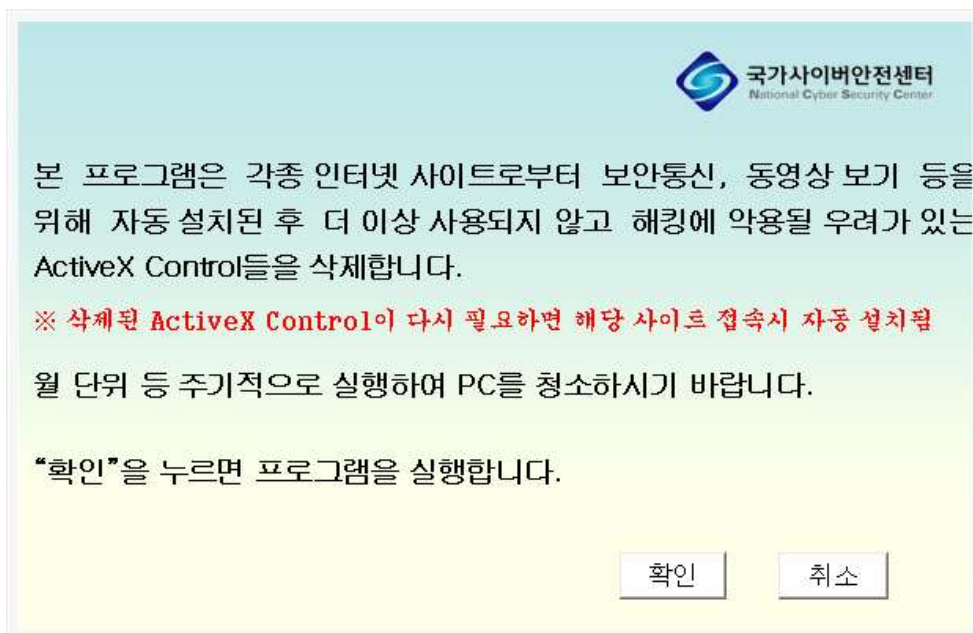
## PC

| 취약점 항목 | 4.6. PC 내부의 미사용(3개월) ActiveX 제거                                                                                                                                                                                                                                             |     |   |      |       |
|--------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----|---|------|-------|
| 대상 OS  | Windows XP, Windows 7                                                                                                                                                                                                                                                       | 위험도 | 상 | Code | PC-18 |
| 취약점 개요 | <p>*액티브X(ActiveX) 프로그램의 경우 각종 인터넷 사이트 등에서 동영상 보기, 금융결제 등을 위해 PC에 설치됨. 사용하지 않는 불필요한 ActiveX에 취약점이 존재할 경우 시스템 해킹 발생 가능성이 증가할 수 있으므로 주기적인 점검 및 삭제가 이루어져야 함.</p> <p>*액티브X(ActiveX): 마이크로소프트사가 개발한 재사용 가능한 객체 지향적인 소프트웨어 구성 요소 개발에 사용되는 기술로 www로부터 다운로드 받은 콘텐츠들을 이용하는 데 이용됨.</p> |     |   |      |       |
| 보안대책   |                                                                                                                                                                                                                                                                             |     |   |      |       |
| 판단기준   | <b>양호:</b> 설치된 ActiveX를 주기적으로 점검하고 불필요한 ActiveX를 삭제하는 경우                                                                                                                                                                                                                    |     |   |      |       |
|        | <b>취약:</b> 설치된 ActiveX에 대한 점검 및 삭제가 이루어지지 않는 경우                                                                                                                                                                                                                             |     |   |      |       |
| 조치방법   | 미사용 ActiveX 삭제                                                                                                                                                                                                                                                              |     |   |      |       |
| 보안설정방법 |                                                                                                                                                                                                                                                                             |     |   |      |       |

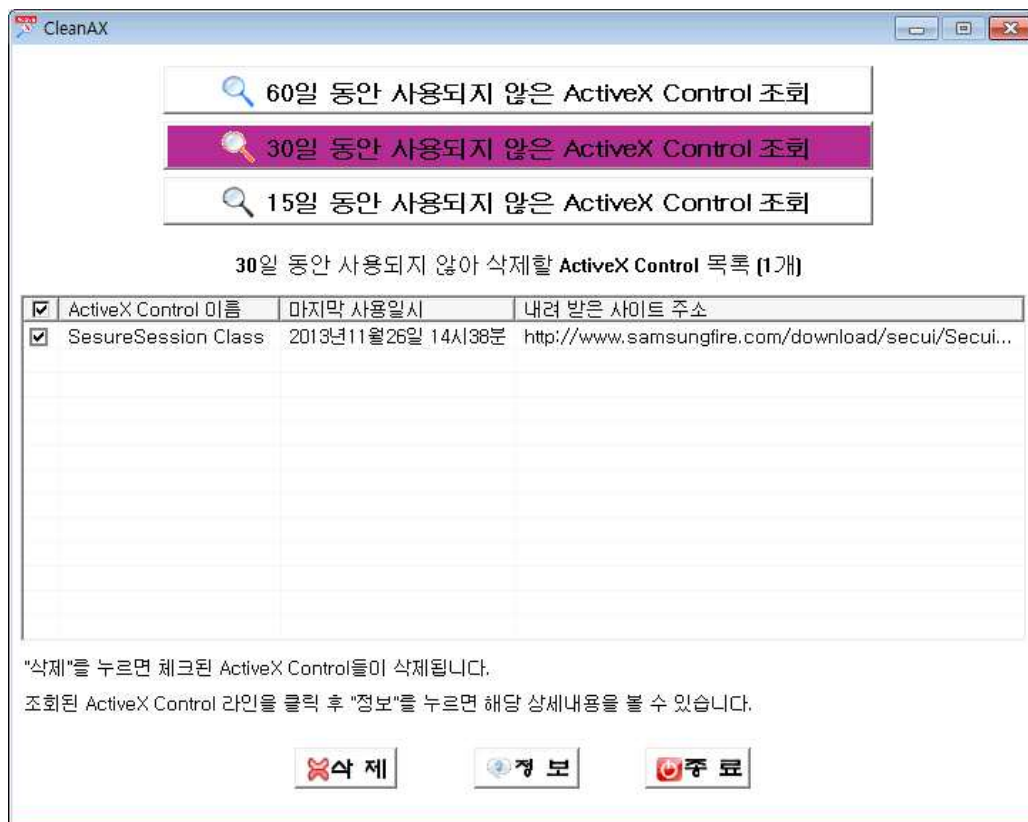
#### ■ Windows XP, Windows 7

- ※ 3개월 이내에 사용되지 않은 ActiveX의 경우 삭제 권고
- ※ "Clean ActiveX" 등의 점검 프로그램을 통해 ActiveX 점검 가능

1. 국가사이버안전센터> 자료실> 보안권고문 [121번]> ActiveX Control 삭제 프로그램 'CleanAX' 배포  
<http://service1.nis.go.kr/safe/securityRecomm.jsp?pArticleNo=1357&pListNo=121&mode=view>



## PC



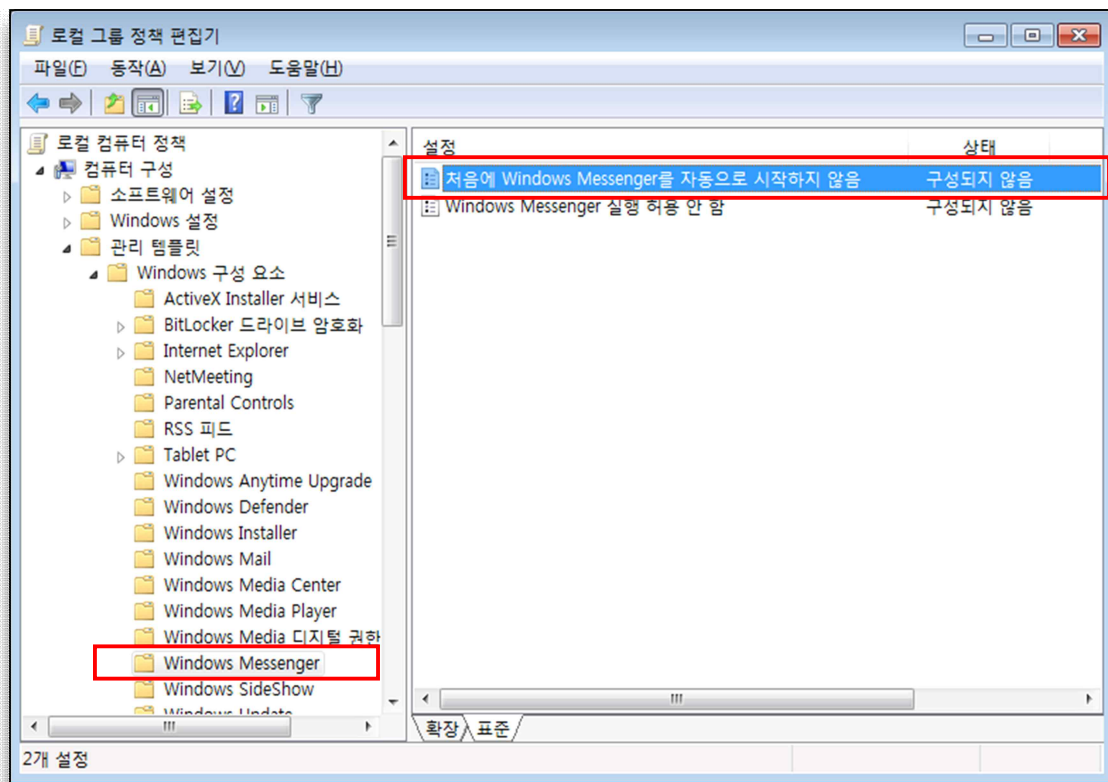
**조치 시 영향**   삭제된 ActiveX 사용 불가 (사용 시 설치 후 사용)

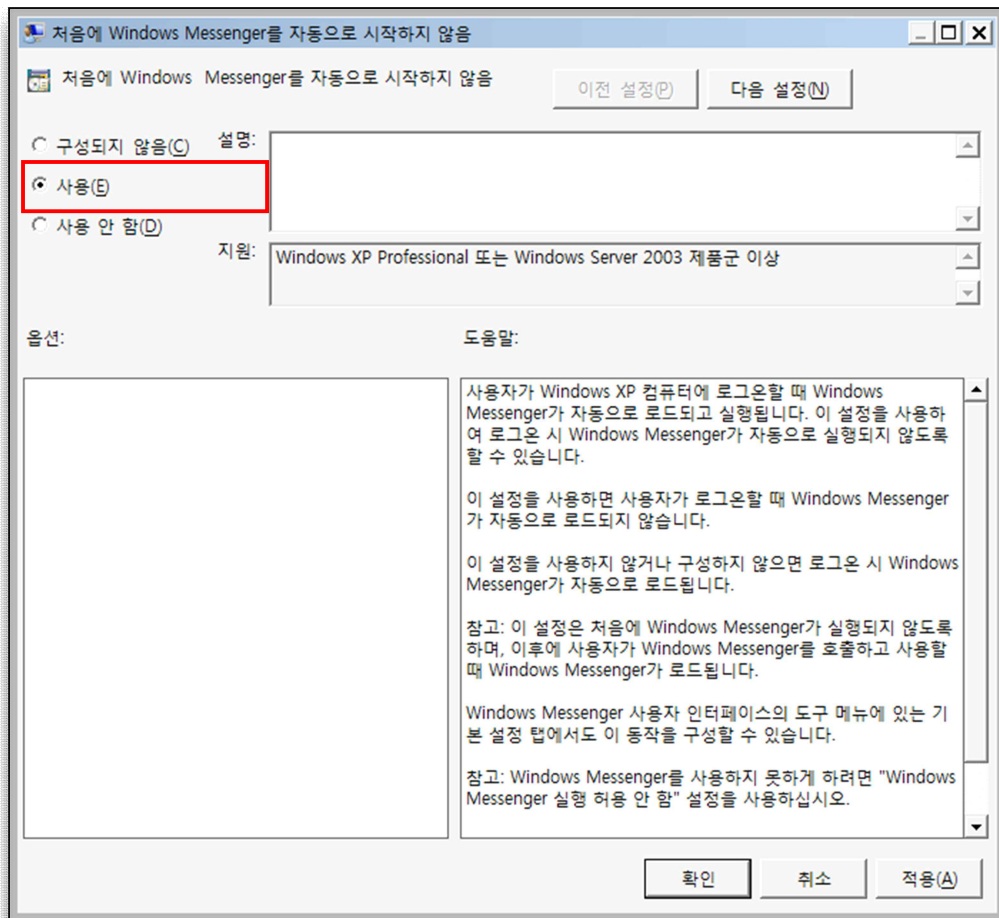
## PC

| 취약점 항목 | 4.7. 시스템 부팅 시 Windows Messenger 자동시작 금지                                                                                        |     |   |      |       |
|--------|--------------------------------------------------------------------------------------------------------------------------------|-----|---|------|-------|
| 대상 OS  | Windows XP, Windows 7                                                                                                          | 위험도 | 중 | Code | PC-19 |
| 취약점 개요 | 윈도우 시작 시 자동으로 Windows Messenger가 시작되도록 설정할 수 있으나 Messenger를 통한 정보 유출 및 악성코드 유입이 발생할 수 있으므로 자동시작으로 설정된 경우 시스템에 대한 위협이 증가할 수 있음. |     |   |      |       |
| 보안대책   |                                                                                                                                |     |   |      |       |
| 판단기준   | 양호: Windows Messenger 자동시작 금지 설정이 되어있는 경우                                                                                      |     |   |      |       |
|        | 취약: Windows Messenger 자동시작 금지 설정이 되어있지 않는 경우                                                                                   |     |   |      |       |
| 조치방법   | Windows Messenger 자동시작 금지 설정                                                                                                   |     |   |      |       |
| 보안설정방법 |                                                                                                                                |     |   |      |       |

### ■ Windows XP, Windows 7

1. 시작> 실행> "gpedit.msc" 입력> 컴퓨터 구성> 관리 템플릿> Windows 구성 요소> Windows Messenger
2. "Windows Messenger를 자동으로 시작하지 않음" 설정을 "사용"으로 설정





### 3. 레지스트리 값으로 설정하는 방법

(1) 시작 > 실행 > "regedit" 입력

(2) 레지스트리 경로

HKLM\Software\Policies\Microsoft\Messenger\Client

(3) 설정 값 입력

|                   |                           |
|-------------------|---------------------------|
| <b>Value name</b> | PreventAutoRun            |
| <b>Data Type</b>  | DWORD 값                   |
| <b>Value</b>      | 1<br>※ Default 값: 0(zero) |

※ "Windows Messenger를 실행하지 않음" 설정이 "사용 안 함"으로 설정되어 있는 경우 레지스트리 편집기 내 Messenger 항목이 존재하며, "사용"인 경우는 존재하지 않음

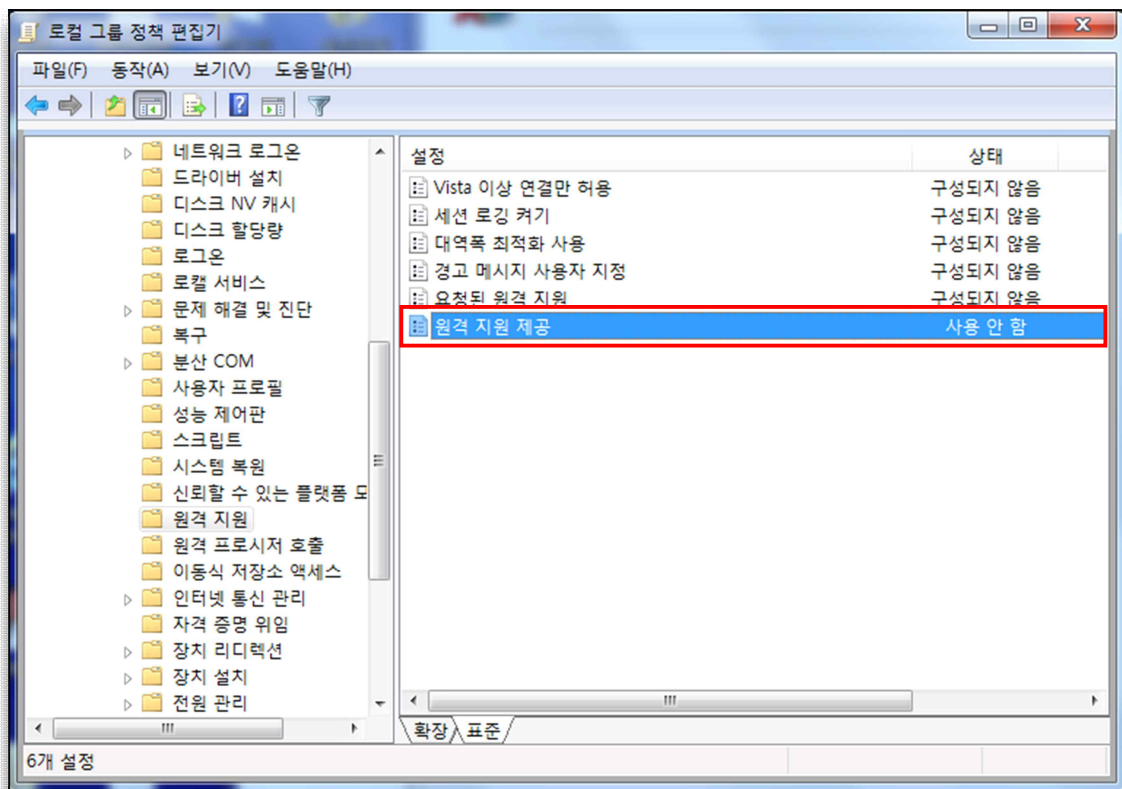
**조치 시 영향**      일반적으로 영향 없음

## PC

| 취약점 항목 | 4.8. 항목 원격 지원 금지 정책 설정                                                          |     |   |      |       |
|--------|---------------------------------------------------------------------------------|-----|---|------|-------|
| 대상 OS  | Windows XP, Windows 7                                                           | 위험도 | 중 | Code | PC-20 |
| 취약점 개요 | 시스템 관리 등의 목적으로 원격 지원 기능을 활용할 수 있으나 원격 지원 기능이 비인가자에게 허용될 경우 시스템 제어 권한이 악용될 수 있음. |     |   |      |       |
| 보안대책   |                                                                                 |     |   |      |       |
| 판단기준   | 양호: 원격 지원이 "사용 안함"으로 설정되어 있는 경우                                                 |     |   |      |       |
|        | 취약: 원격 지원이 "사용"으로 설정되어 있는 경우                                                    |     |   |      |       |
| 조치방법   | 원격 지원 서비스 제거                                                                    |     |   |      |       |
| 보안설정방법 |                                                                                 |     |   |      |       |

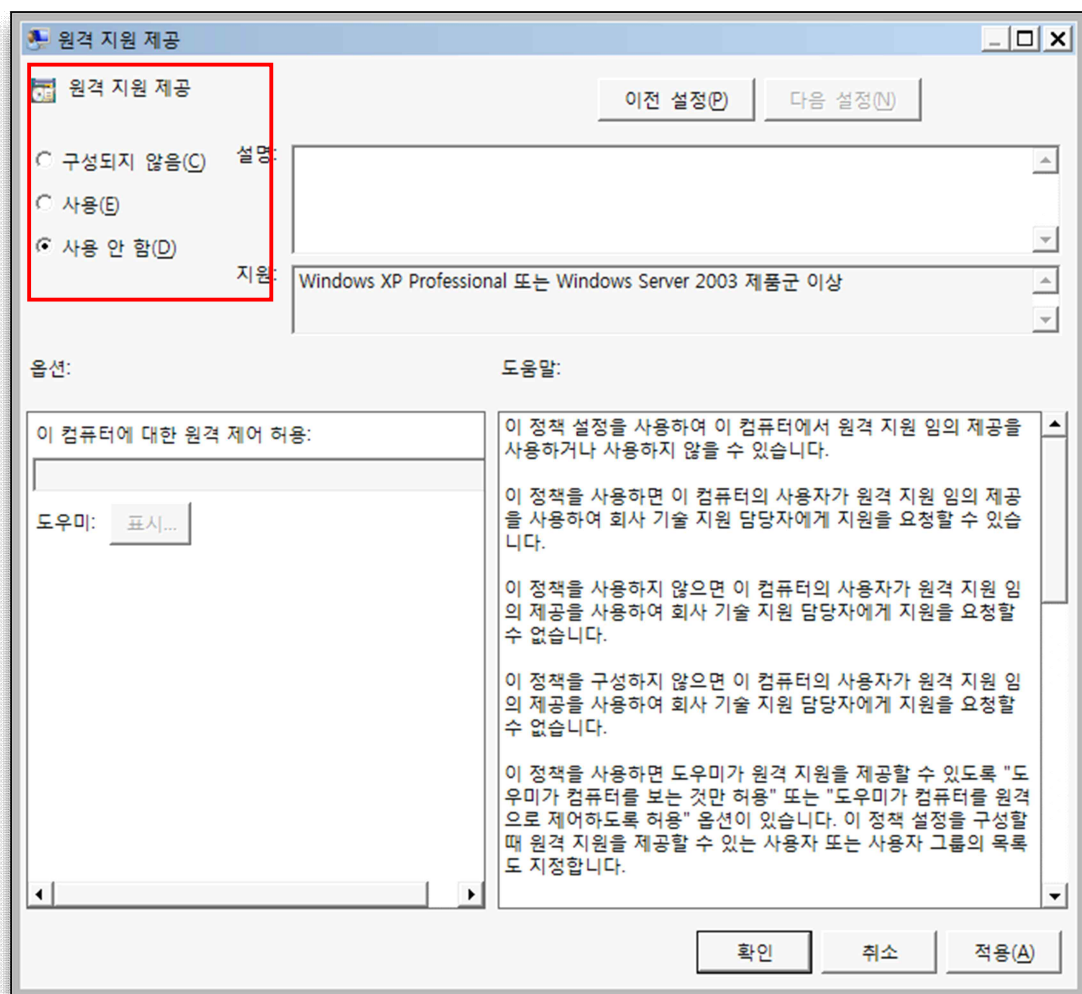
## ■ Windows XP, Windows 7

1. 시작> 실행> "gpedit.msc" 입력> 컴퓨터 구성> 관리 템플릿> 시스템> 원격 지원
2. "원격 지원 제공"을 "사용 안 함"으로 설정





## PC



조치 시 영향 원격 지원 기능 사용 불가





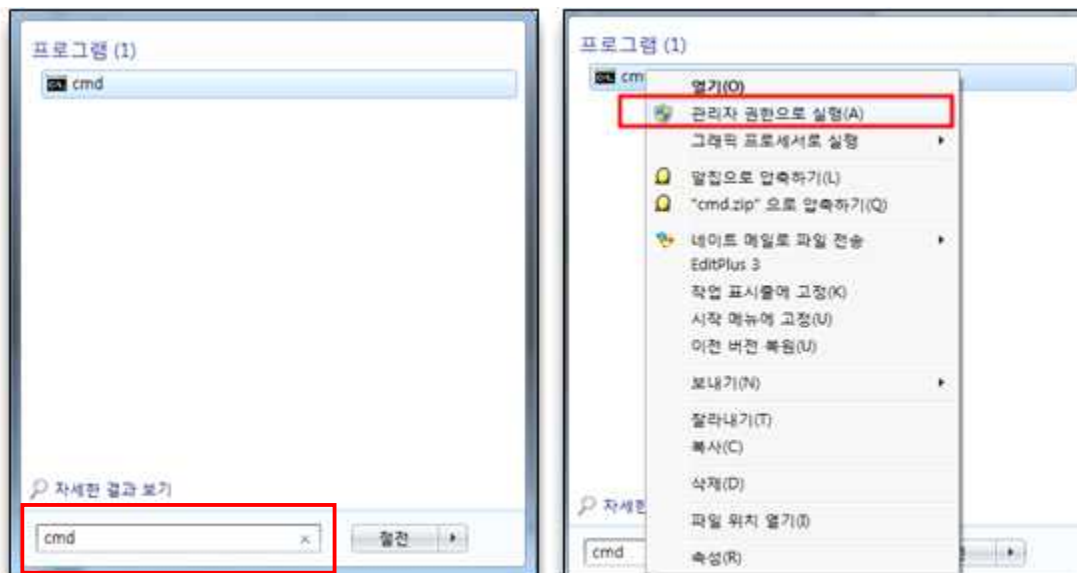
## 부 록

## 01. Windows 명령어 모음

| 시스템 관련       |                    | 컴퓨터 관련      |              |
|--------------|--------------------|-------------|--------------|
| 문자표          | chamap             | 컴퓨터 관리      | compmgmt.msc |
| 제어판          | control            | 장치 관리자      | devmgmt.msc  |
| 마우스 속성       | main.cpl           | 이벤트 뷰어      | eventvwr.msc |
| 전원 옵션        | powercfg.cpl       | 성능 모니터뷰     | perfmon.msc  |
| 관리 도구        | control admintools | 정책의 결과와 집합  | rsop.msc     |
| 레지스트리 편집기    | regedit            | 서비스         | services.msc |
| 윈도우 버전 확인    | winver             | 공유 폴더       | fsmgmt.msc   |
| 작업 관리자       | taskmgr            | 디스크 관리      | diskmgmt.msc |
| 이벤트 뷰어       | eventvwr           | 디스크 조각 모음   | dfrg.msc     |
| 사용자 계정       | netplwiz           | 디스크 조각 모음   | dfrgui       |
| 시스템 정보       | msinfo32           | 디스크 정리      | cleanmgr     |
| 서비스 관리자      | services.msc       | 로컬 컴퓨터 정책   | gpedit.msc   |
| 인터넷 속성       | Inetcpl.cpl        | 로컬 사용자 및 그룹 | lusrmgr.msc  |
| 시스템 등록정보     | Sysdm.cpl          | 로컬 보안 설정    | secpol.msc   |
| 포로그램 추가/제거   | appwiz.cpl         | 시스템 구성      | msconfig     |
| 디스플레이 등록정보   | Desk.cpl           | 방화벽         | firewall.cpl |
| 사운드 및 오디오 장치 | mmsys.cpl          |             |              |
| 원격 데스크톱 연결   | mstsc              |             |              |

## 02. 관리자 권한으로 cmd 명령어를 실행하는 방법 (※ Windows 7 해당)

시작> "cmd.exe"검색> 우클릭> "관리자 권한"으로 실행 또는,  
 "C:\Windows\System32" 경로로 찾아가 "cmd.exe" 파일 우클릭 "관리자 권한"으로 실행



# DBMS 보안가이드라인

2014. 01



안전행정부 *희망의 새시대*

## DBMS 취약점 분석·평가 항목

| 분류      | 점검항목                                                           | 항목<br>중요도 | 항목코드 |
|---------|----------------------------------------------------------------|-----------|------|
| 1. 계정관리 | 기본 계정의 패스워드, 정책 등을 변경하여 사용                                     | 상         | D-01 |
|         | scott 등 Demonstration 및 불필요 계정을 제거하거나 잠금 설정 후 사용               | 상         | D-02 |
|         | 패스워드의 사용기간 및 복잡도 기관 정책에 맞도록 설정                                 | 상         | D-03 |
|         | 데이터베이스 관리자 권한을 꼭 필요한 계정 및 그룹에 허용                               | 상         | D-04 |
|         | 패스워드 재사용에 대한 제약                                                | 중         | D-05 |
|         | DB 사용자 계정 개별적 부여                                               | 중         | D-06 |
| 2. 접근관리 | 원격에서 DB 서버로의 접속 제한                                             | 상         | D-07 |
|         | DBA이외의 인가되지 않은 사용자 시스템 테이블 접근 제한 설정                            | 상         | D-08 |
|         | 오라클 데이터베이스의 경우 리스너 패스워드 설정                                     | 상         | D-09 |
|         | 불필요한 ODBC/OLE-DB 데이터 소스와 드라이브 제거                               | 중         | D-10 |
|         | 일정 횟수의 로그인 실패 시 잠금 정책 설정                                       | 중         | D-11 |
|         | 데이터베이스의 주요 파일 보호 등을 위해 DB 계정의 umask를 022이상으로 설정                | 하         | D-12 |
|         | 데이터베이스의 주요 설정파일, 패스워드 파일 등 주요 파일들의 접근 권한 설정                    | 중         | D-13 |
|         | 관리자 이외의 사용자가 오라클 리스너의 접속을 통해 리스너 로그 및 trace 파일에 대한 변경 권한 제한    | 하         | D-14 |
| 3. 옵션관리 | 응용프로그램 또는 DBA 계정의 Role이 Public으로 설정되지 않도록 조정                   | 상         | D-15 |
|         | OS_ROLES, REMOTE_OS_AUTHENTICATION, REMOTE_OS_ROLES를 FALSE로 설정 | 상         | D-16 |
|         | 패스워드 확인함수가 설정되어 적용되는가?                                         | 중         | D-17 |
|         | 인가되지 않은 Object Owner가 존재하지 않는가?                                | 하         | D-18 |
|         | grant option이 role에 의해 부여되도록 설정                                | 중         | D-19 |
|         | 데이터베이스의 자원 제한 기능을 TRUE로 설정                                     | 하         | D-20 |
| 4. 패치관리 | 데이터베이스에 대해 최신 보안패치와 밴더 권고 사항을 모두 적용                            | 상         | D-21 |
|         | 데이터베이스의 접근, 변경, 삭제 등의 감사기록이 기관의 감사기록 정책에 적합하도록 설정              | 상         | D-22 |
|         | 보안에 취약하지 않은 버전의 데이터베이스를 사용하고 있는가?                              | 중         | D-23 |
| 5. 로그관리 | Audit Table은 데이터베이스 관리자 계정에 속해 있도록 설정                          | 하         | D-24 |

## 1. 계정관리

| 취약점 항목                                             |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                | 1.1. 기본 계정의 패스워드, 정책 등을 변경하여 사용 |   |        |      |  |
|----------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------|---|--------|------|--|
| 대상                                                 | Oracle, MSSQL, MySQL                                                                                                                                                                                                                                                                                                                                                                                                                                                                           | 위험도                             | 상 | Code   | D-01 |  |
| 취약점 개요                                             | <div>■ <b>Oracle</b> - 데이터베이스의 기본 계정(system, scott 등)의 패스워드 또는, 접근제어 정책을 변경하지 않고 사용할 경우 공격자는 알려진 정보를 이용하여 데이터베이스에 쉽게 접근할 수 있는 취약점이 존재함.</div> <div>■ <b>MSSQL</b> - sa 계정 null 암호 취약점은 비인가자에 의해 sa 계정으로 데이터베이스에 침입하여 정보 삭제, 변경 등의 행위를 할 수 있는 위험이 있음.</div> <div>■ <b>MySQL</b> - root 계정의 패스워드가 디폴트 설정 값인 null을 사용할 경우, 시스템에 접근한 임의의 모든 사용자가 root 권한으로 접속하여 mysql의 모든 작업을 할 수 있어 mysql DB에 저장된 모든 정보가 유출 되는 등의 침해사고를 일으킬 위험이 있음. 기본 계정을 변경하지 않고 사용하는 경우 공격자에게 정보가 노출될 가능성이 있으므로 변경하여야 함.</div> |                                 |   |        |      |  |
| 보안대책                                               |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |                                 |   |        |      |  |
| 판단기준                                               | 양호: 기본 계정의 패스워드를 변경하여 사용하는 경우                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |                                 |   |        |      |  |
|                                                    | 취약: 기본 계정의 디폴트 설정을 변경하지 않고 사용하는 경우                                                                                                                                                                                                                                                                                                                                                                                                                                                             |                                 |   |        |      |  |
| 조치방법                                               | 기본(관리자) 계정의 패스워드 및 정책 변경                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |                                 |   |        |      |  |
| 보안설정방법                                             |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |                                 |   |        |      |  |
| ■ <b>Oracle</b>                                    |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |                                 |   |        |      |  |
| 1. 불필요한 계정인 경우 계정 삭제                               |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |                                 |   |        |      |  |
| SQL> DROP USER username;                           |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |                                 |   |        |      |  |
| 2. 사용되는 계정인 경우 계정의 기본 패스워드 변경 후 사용                 |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |                                 |   |        |      |  |
| SQL> alter user username identified by new_passwd; |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |                                 |   |        |      |  |
| ※ 그 이외에 객체 권한 부여 및 기본 role 확인 및 변경 수행              |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |                                 |   |        |      |  |
| ※ DBSNMP 파일의 접근권한 설정이 필요함                          |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |                                 |   |        |      |  |
| chmod 700 snmp_rw.ora (결과값 -rwx-----snmp_rw.ora)   |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |                                 |   |        |      |  |
| Oracle 설치 시 생성되는 디폴트 계정 정보                         |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |                                 |   |        |      |  |
| User                                               |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                | Password                        |   | User   |      |  |
| scott                                              |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                | tiger or tigger                 |   | system |      |  |
| dbsnmp                                             |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                | dbsnmp                          |   | sys    |      |  |
| tracesvr                                           |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                | trace                           |   | outln  |      |  |
| ordplugins                                         |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                | ordplugins                      |   | ordsys |      |  |
| ctxsys                                             |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                | ctxsys                          |   | mdsys  |      |  |
| adams                                              |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                | wood                            |   | blake  |      |  |
| clark                                              |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                | clth                            |   | jones  |      |  |
| lbacsys                                            |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                | lbacsys                         |   |        |      |  |

## ■ MS SQL

sa 계정 패스워드 변경

```
Alter login sa with password='new password'
```

## ■ MySQL

root 계정 패스워드 변경

```
mysql> use mysql
```

```
mysql> update user set password=password('new password') where user='root';
```

```
mysql> flush privileges; 또는,
```

```
mysql> set password for root=password('new password')
```

※ 패스워드가 취약하게 설정된 경우 패스워드를 아래 기준을 준수하여 변경함

### < 패스워드 관리 방법 >

1. 영문, 숫자, 특수문자를 조합하여 계정명과 상이한 8자 이상의 패스워드 설정

※ 다음 각 목의 문자 종류 중 2종류 이상을 조합하여 최소 10자리 이상 또는, 3종류 이상을 조합하여 최소 8자리 이상의 길이로 구성

가. 영문 대문자(26개)

나. 영문 소문자(26개)

다. 숫자(10개)

라. 특수문자(32개)

2. 시스템마다 상이한 패스워드 사용

3. 패스워드를 기록해 놓을 경우 변형하여 기록

4. 가급적 자주 패스워드를 변경할 것

### 조치 시 영향

불필요한 계정 사용 불가

## DBMS

| 취약점 항목                                                                                                                                                                                                                                                                                                                                                                                 | 1.2. scott 등 Demonstration 및 불필요 계정을 제거하거나 잠금 설정 후 사용                                                                                       |     |   |      |      |
|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------|-----|---|------|------|
| 대상                                                                                                                                                                                                                                                                                                                                                                                     | Oracle, MSSQL, MySQL                                                                                                                        | 위험도 | 상 | Code | D-02 |
| 취약점 개요                                                                                                                                                                                                                                                                                                                                                                                 | 데이터베이스의 계정 중 실질적으로 업무에 사용하지 않는 SCOTT, PM, ADAMS, CLARK 등의 Demonstration 계정이 삭제되지 않고 존재하면 공격자가 데이터베이스 시스템에 쉽게 접근하여 데이터를 열람, 삭제, 수정할 위험이 존재함. |     |   |      |      |
| 보안대책                                                                                                                                                                                                                                                                                                                                                                                   |                                                                                                                                             |     |   |      |      |
| 판단기준                                                                                                                                                                                                                                                                                                                                                                                   | 양호: 계정 정보를 확인하여 불필요한 계정이 없는 경우                                                                                                              |     |   |      |      |
|                                                                                                                                                                                                                                                                                                                                                                                        | 취약: 인가되지 않은 계정, 퇴직자 계정, 테스트 계정 등 불필요한 계정이 존재하는 경우                                                                                           |     |   |      |      |
| 조치방법                                                                                                                                                                                                                                                                                                                                                                                   | 기본 계정 외 계정의 용도를 파악 후 불필요한 계정 삭제                                                                                                             |     |   |      |      |
| 보안설정방법                                                                                                                                                                                                                                                                                                                                                                                 |                                                                                                                                             |     |   |      |      |
| <div>■ Oracle</div> <div>1. 불필요한 Demonstration 계정 및 오브젝트 삭제</div> <div>SQL&gt; DROP USER '삭제할 계정'</div> <div>2. 계정 잠금/만료</div> <div>SQL&gt; ALTER USER '잠금/만료 계정' ACCOUNT LOCK PASSWORD EXPIRE</div> <div>■ MSSQL</div> <div>불필요한 계정 삭제</div> <div>Exec sp_droplogin '삭제할 계정'</div> <div>■ MySQL</div> <div>불필요한 계정 삭제</div> <div>mysql&gt; Delete from user where user='삭제할 계정'</div> |                                                                                                                                             |     |   |      |      |
| 조치 시 영향                                                                                                                                                                                                                                                                                                                                                                                | Demonstration 계정 / 오브젝트 사용 불가 / 삭제된 계정 사용 불가                                                                                                |     |   |      |      |

## DBMS

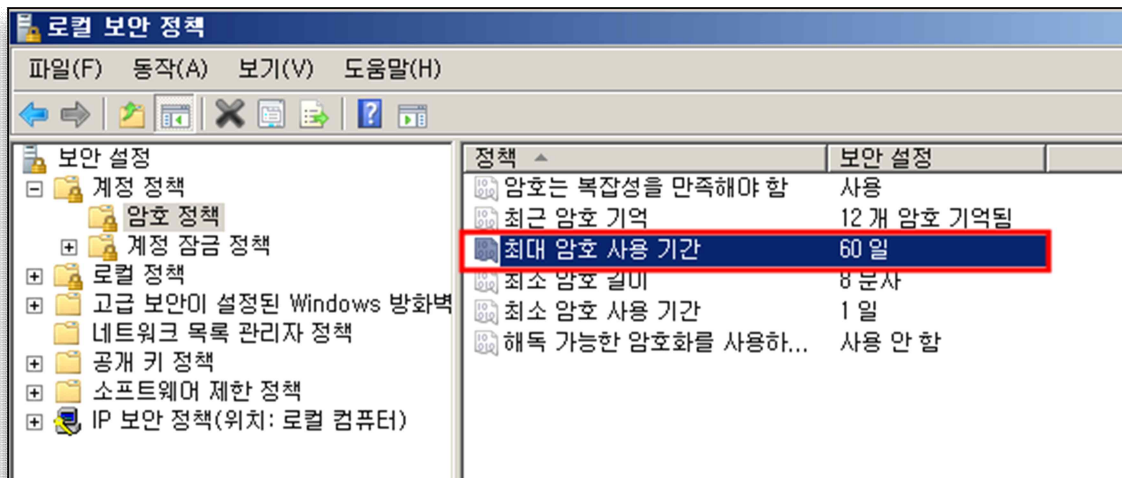
| 취약점 항목                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  | 1.3. 패스워드의 사용기간 및 복잡도 기관 정책에 맞도록 설정                                                                                                                |     |   |      |      |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------|-----|---|------|------|
| 대상                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      | Oracle, MSSQL, MySQL                                                                                                                               | 위험도 | 상 | Code | D-03 |
| 취약점 개요                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  | 주기적인 패스워드 변경이 없을 경우 공격자는 Brute force 공격을 통하여 패스워드를 획득할 위험이 존재함.<br><br>■ <b>Oracle</b> - PASSWORD_LIFE_TIME 값은 패스워드가 만기된 이후에 사용가능한 일수에 대한 제한을 제공함. |     |   |      |      |
| 보안대책                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |                                                                                                                                                    |     |   |      |      |
| 판단기준                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    | 양호: 패스워드를 주기적으로 변경하고, 패스워드 정책이 적용되어 있는 경우                                                                                                          |     |   |      |      |
|                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         | 취약: 패스워드를 주기적으로 변경하지 않거나, 패스워드 정책이 없는 경우                                                                                                           |     |   |      |      |
| 조치방법                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    | 주기적 패스워드 변경, 패스워드 적용 정책 마련                                                                                                                         |     |   |      |      |
| 보안설정방법                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |                                                                                                                                                    |     |   |      |      |
| <div>■ <b>Oracle</b></div> <div>1. PASSWORD_LIFE_TIME 프로파일 파라미터 변경</div> <div>SQL&gt; ALTER PROFILE LIMIT PASSWORD_LIFE_TIME xx</div> <div>2. 프로파일 값과 관련된 사용자 변경</div> <div>SQL&gt; ALTER USER PROFILE</div> <div>3. 패스워드 설정 변경</div> <div>SQL&gt; CREATE PROFILE grace_5 LIMIT</div> <div>FAILED_LOGIN_ATTEMPTS 3 (패스워드 실패 3번 까지만 가능)</div> <div>PASSWORD_LIFE_TIME 30 (30일 동안만 패스워드 사용 가능)</div> <div>PASSWORD_REUSE_TIME 30 (사용한 패스워드 30일 후부터 재사용 가능)</div> <div>PASSWORD_VERIFY_FUNCTION verify_function</div> <div>PASSWORD_GRACE_TIME 5 ; (life time이 끝나고 5일 동안 메시지를 보여줌)</div> <div>■ <b>MSSQL</b></div> <div>1. 패스워드 변경 주기가 60일 이내로 설정되지 않은 경우 패스워드 변경 주기 설정</div> <div>MSSQL에서 '암호 만료 강제 적용'을 체크함으로써 주기적으로 변경이 가능하며, 변경기간은 OS의 '암호정책'에서 적용 받으므로 '암호 정책 &gt; 최대 암호 사용 기간' 설정도 같이 변경해야 함</div> <div>2. 암호 만료 강제 적용</div> <div>[보안]&gt; [로그인]&gt; [각 로그인 계정]&gt; [속성]&gt;</div> <div>암호 만료 강제 적용: 설정(체크) 확인</div> |                                                                                                                                                    |     |   |      |      |



### 3. OS의 암호 정책 설정

[관리도구]> [로컬 보안 정책]> [보안 설정]> [계정 정책]> [암호 정책]

'최대 암호 사용 기간 : '60일' 설정



## ■ MySQL

### 1. 패스워드 설정 규칙 적용

패스워드 설정 규칙에 맞추어 패스워드를 설정할 수 있도록 시스템 차원에서 기능 제공

### 2. 패스워드 관리 적용

패스워드 신규 적용 및 초기화 시 설정 규칙에 맞추어 관리하고, 저장 시에는 일방향 암호 알고리즘을 통한 암호화 처리(One-Way Encryption)

### 3. 패스워드 변경기능 구현

사용자가 패스워드 설정규칙 내에서 스스로 패스워드를 변경할 수 있도록 기능 제공

## DBMS

패스워드 설정은 다음과 같은 방법으로 가능

```
mysql> use mysql
```

```
mysql> update user set password=password('new password') where user='user name';
```

```
mysql> flush privileges; 또는,
```

```
mysql> set password for 'user name'@'%'=password('new password')
```

```
mysql> flush privileges;
```

**조치 시 영향**

주기적인 패스워드 교체 필요

## DBMS

| 취약점 항목                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   | 1.4. 데이터베이스 관리자 권한을 꼭 필요한 계정 및 그룹에 허용                                                                  |     |   |      |      |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------|-----|---|------|------|
| 대상                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       | Oracle                                                                                                 | 위험도 | 상 | Code | D-04 |
| 취약점 개요                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   | DBA에게만 허용되어야 하는 SYSDBA 권한이 응용프로그램 계정 또는 일반 사용자 계정에 허용되어 있는 경우 공격자는 이를 이용하여 쉽게 DBA 권한으로 데이터베이스에 접근 가능함. |     |   |      |      |
| 보안대책                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |                                                                                                        |     |   |      |      |
| 판단기준                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     | 양호: 계정별 관리자권한이 차등 부여 되어 있는 경우                                                                          |     |   |      |      |
|                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          | 취약: 일반 사용자 계정에 불필요하게 관리자 권한이 부여되어 있는 경우                                                                |     |   |      |      |
| 조치방법                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     | 계정별 관리자 권한 차등 부여, 삭제                                                                                   |     |   |      |      |
| 보안설정방법                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |                                                                                                        |     |   |      |      |
| <div>■ Oracle</div> <div>1. SYSDBA 권한 점검</div> <div>SQL&gt; SELECT USERNAME FROM V\$PWFILE_USERS WHERE USERNAME NOT IN (SELECT GRANTEE FROM DBA_ROLE_PRIVS WHERE GRANTED_ROLE='DBA') and USERNAME !='INTERNAL' and sysdba='TRUE'; (어떠한 계정이라도 나오는 경우 취약)</div> <div>2. Admin에 부적합 계정 존재 여부 점검</div> <div>SQL&gt; select grantee, privilege from dba_sys_privs where grantee not in ( 'SYS', 'SYSTEM', 'AQ_ADMINISTRATOR_ROLE' , 'DBA ' , 'MDSYS' , 'LBACSYS', 'SCHEDULER_ADMIN', 'WMSYS') and admin_option='YES' and grantee not in (select grantee from dba_role_privs where granted_role='DBA'); (어떠한 계정이라도 나오는 경우 취약)</div> <div>※ 불필요하게 시스템 권한을 부여한 계정의 권한 변경 필요</div> <div>※ 시스템 권한 부여가 필요한 경우 필요한 테이블별 권한 부여</div> <div>※ 인가된 사용자는 관리자 권한에 role을 grant한 후, 시스템 권한을 grant하고 role을 인가된 사용자에게 grant 함</div> <div>■ MSSQL</div> <div>1. sysadmin 서버 역할의 계정 목록을 확인 후 해당 서버 역할에 불필요한 계정이 있는 경우 서버 역할에서 삭제</div> <div>sysadmin 서버 역할에서 불필요한 계정 삭제</div> <div>Exec sp_droprolemember 'user_name', 'sysadmin'</div> <div>(예) Exec sp_dropsvrolemember 'user01', 'sysadmin'</div> <div>(user01 계정을 sysadmin 서버 역할에서 삭제)</div> |                                                                                                        |     |   |      |      |

## ■ MySQL

1. mysql.user 테이블에 적용된 권한은 모든 데이터베이스에 적용되므로 host, user, password를 제외한 나머지 권한은 허용하지 않음('N')으로 설정

- 사용자 등록

```
mysql> insert into mysql.user (host, name, password) values('%', 'user name', password('password')) ※ 디폴트로 모든 권한 'N' 설정
```

- 권한 변경

```
mysql> update mysql.user set <권한>='N' where user='user name'
```

2. 각 사용자는 접근하고자 하는 DB를 mysql.db에 등록 후 접근 권한을 부여하여 사용

- DB등록 시 권한 부여

```
mysql> insert into mysql.db values('%','DB name', 'username', 'Y', 'Y', 'Y', 'Y', 'Y', 'Y', 'Y', 'Y', 'Y', 'Y', 'Y', 'Y', 'Y', 'Y', 'Y')
```

```
mysql> flush privileges
```

- DB 권한 업데이트

```
mysql> update mysql.db set <권한>='Y' where db=<DB name> and user='user name'
```

```
mysql> flush privileges
```

|         |             |
|---------|-------------|
| 조치 시 영향 | 일반적으로 영향 없음 |
|---------|-------------|

## DBMS

| 취약점 항목                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   | 1.5. 패스워드 재사용에 대한 제약                                                                                                        |     |   |      |      |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------|-----|---|------|------|
| 대상                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       | Oracle                                                                                                                      | 위험도 | 중 | Code | D-05 |
| 취약점 개요                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   | PASSWORD_REUSE_TIME 값은 패스워드가 재사용될 수 있기 전에 일수를 명시하는 파라미터이며, PASSWORD_REUSE_MAX는 횟수 설정 파라미터임.<br>파라미터 미설정 시 패스워드 노출 가능성이 증가함. |     |   |      |      |
| 보안대책                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |                                                                                                                             |     |   |      |      |
| 판단기준                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     | 양호: PASSWORD_REUSE_TIME, PASSWORD_REUSE_MAX 파라미터 설정이 적용된 경우                                                                 |     |   |      |      |
|                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          | 취약: PASSWORD_REUSE_TIME, PASSWORD_REUSE_MAX 파라미터 설정이 적용되지 않은 경우                                                             |     |   |      |      |
| 조치방법                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     | PASSWORD_REUSE_TIME, PASSWORD_REUSE_MAX 파라미터 설정                                                                             |     |   |      |      |
| 보안설정방법                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |                                                                                                                             |     |   |      |      |
| <div>■ Oracle</div> <div>1. 설정확인(SQL*Plus)</div> <div>-- Check for both reuse max and reuse time not set:</div> <div>select profile from DBA_PROFILES where (resource_name='PASSWORD_REUSE_MAX' and limit in ('UNLIMITED','NULL')) or profile in (select profile from DBA_PROFILES where resource_name='PASSWORD_REUSE_TIME') and limit in ('UNLIMITED','NULL');</div> <div>-- Check for reuse max with value that is less than allowed minimum</div> <div>select profile from DBA_PROFILES where resource_name='PASSWORD_REUSE_MAX' and limit not in ('UNLIMITED','NULL') and limit &lt; '10';</div> <div>-- Check for reuse time that is less than allowed minimum</div> <div>select profile from DBA_PROFILES where resource_name='PASSWORD_REUSE_TIME' and limit not in ('UNLIMITED','NULL')and limit &lt; '365';</div> <div>2. PASSWORD_REUSE_TIME 및 프로파일 파라미터 수정</div> <div>SQL&gt; alter profile default limit password_reuse_time 365 password_reuse_max 10;</div> <div>SQL&gt; alter profile [profile name] limit password_reuse_time default password_reuse_max default;</div> |                                                                                                                             |     |   |      |      |
| 조치 시 영향                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  | 일반적으로 영향 없음                                                                                                                 |     |   |      |      |

## DBMS

| 취약점 항목                                                                                                                                                                                                                                                                                                                                                                                                                              | 1.6. DB 사용자 계정 개별적 부여                                                                                                            |     |   |      |      |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------|-----|---|------|------|
| 대상                                                                                                                                                                                                                                                                                                                                                                                                                                  | Oracle, MSSQL, MySQL                                                                                                             | 위험도 | 중 | Code | D-06 |
| 취약점 개요                                                                                                                                                                                                                                                                                                                                                                                                                              | 데이터베이스의 사용자 계정이 사용자, 프로세스와 응용 프로그램 등에 동일하게 사용하게 될 경우 침해사고 발생 시 책임 추적에 영향을 주며, 계정별 권한 부여가 불가능해지고 사용하지 않는 계정을 이용한 비인가 사용자 접속이 가능함. |     |   |      |      |
| 보안대책                                                                                                                                                                                                                                                                                                                                                                                                                                |                                                                                                                                  |     |   |      |      |
| 판단기준                                                                                                                                                                                                                                                                                                                                                                                                                                | 양호: 사용자별 계정을 사용하고 있는 경우                                                                                                          |     |   |      |      |
|                                                                                                                                                                                                                                                                                                                                                                                                                                     | 취약: 공용 계정을 사용하고 있는 경우                                                                                                            |     |   |      |      |
| 조치방법                                                                                                                                                                                                                                                                                                                                                                                                                                | 사용자별 계정 생성 및 권한 부여                                                                                                               |     |   |      |      |
| 보안설정방법                                                                                                                                                                                                                                                                                                                                                                                                                              |                                                                                                                                  |     |   |      |      |
| <div>■ Oracle</div> <div>1. 계정 확인(SQL*Plus)<br/>SQL&gt; select username from dba_users order by username;(사용하지 않거나 모르는 계정 확인)</div> <div>2. 공통으로 사용하는 계정 삭제<br/>SQL&gt; DROP USER '삭제할 계정'</div> <div>3. 사용자별, 응용프로그램별 계정 생성<br/>SQL&gt; Create user username identified by passwd</div> <div>4. 권한 부여<br/>SQL&gt; grant connect, resource to username</div>                                                                        |                                                                                                                                  |     |   |      |      |
| <div>■ MSSQL</div> <div>1. 불필요한 계정 삭제<br/>Exec sp_droplogin '삭제할 계정'</div> <div>2. 사용자별, 응용프로그램별 계정 생성<br/>CREATE login '생성 계정' WITH password = '패스워드'<br/>CREATE user '생성 계정' FOR login '생성 계정' WITH default_schema ='생성 계정' ;<br/>ALTER USER '생성 계정' WITH DEFAULT_SCHEMA = '생성 계정'<br/>EXEC sp_adduser '생성 계정', '생성 계정', 'db_owner'<br/>EXEC sp_adduser '생성 계정', '생성 계정', '생성 계정'<br/>EXEC sp_grantdbaccess '생성 계정','생성 계정'</div> |                                                                                                                                  |     |   |      |      |
| <div>■ MySQL</div> <div>1. 불필요한 계정 삭제<br/>mysql&gt; Delete from user where user='삭제할 계정'</div> <div>2. 사용자별, 응용프로그램별 계정 생성, 권한 설정<br/>mysql&gt; insert into user('localhost','user', 'password') values('localhost', '생성 계정', 'password('패스워드'));<br/>mysql&gt; insert into mysql.db values('%','DB name', 'username', 'Y', 'Y', 'Y', 'Y', 'Y', 'Y', 'Y', 'Y', 'Y', 'Y', 'Y', 'Y', 'Y');</div>                                      |                                                                                                                                  |     |   |      |      |

**DBMS**

'Y', 'Y', 'Y', 'Y', 'Y', 'Y', 'Y')

mysql> flush privileges

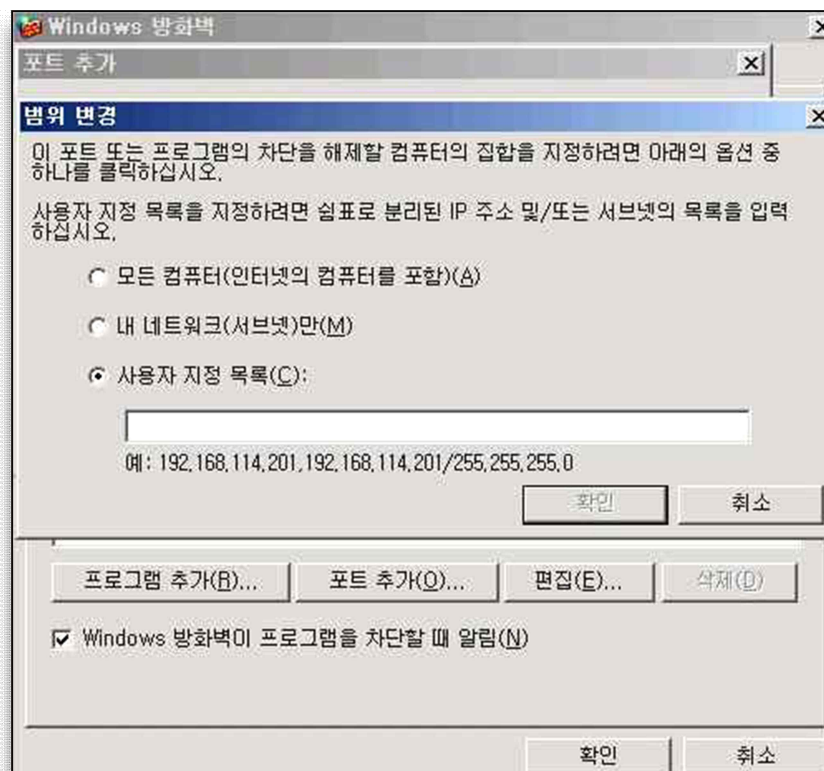
**조치 시 영향**

일반적으로 영향 없음

## 2. 접근관리

| 취약점 항목 | 2.1. 원격에서 DB 서버로의 접속 제한                                                                                                                            |     |   |      |      |
|--------|----------------------------------------------------------------------------------------------------------------------------------------------------|-----|---|------|------|
| 대상     | OS, MySQL                                                                                                                                          | 위험도 | 상 | Code | D-07 |
| 취약점 개요 | 허용되지 않은 IP에서 원격으로 DB에 접속이 허용되어 있는 경우 공격자에 의해 네트워크 서비스 스캐닝을 통한 DB 사용 여부가 확인되어 공격 대상이 될 수 있으며, DB 내의 데이터 유출이 가능함.                                    |     |   |      |      |
|        | ■ <b>Oracle</b> - REMOTE_OS_AUTHENT 값이 TRUE로 설정되어 있으면 안전하지 않은 연결을 통한 원격지의 OS의 인증을 허용함. 이는 원격지 OS의 사용자인 것처럼 속이는 공격자를 허용할 수 있으며, 패스워드 없이 DB 접근을 허용함. |     |   |      |      |
| 보안대책   |                                                                                                                                                    |     |   |      |      |
| 판단기준   | 양호: 허용된 IP 및 포트에 대한 접근 통제가 되어 있는 경우                                                                                                                |     |   |      |      |
|        | 취약: IP에 대해 접근 통제가 이루어지지 않는 경우                                                                                                                      |     |   |      |      |
| 조치방법   | 허용된 IP 및 포트에 대한 접근 통제 적용                                                                                                                           |     |   |      |      |
| 보안설정방법 |                                                                                                                                                    |     |   |      |      |

## ■ OS





특정 IP에서만 접속 가능하도록 방화벽 등이 설정되어 있는지 확인

시작> 제어판> 보안 센터> windows 방화벽 설정

- 예외 tab -> 포트추가 -> 1433 -> TCP 추가 -> 범위 변경
- 예외 tab -> 포트추가 -> 135 -> TCP 추가 -> 범위 변경
- 예외 tab -> 포트추가 -> 1434 -> UDP 추가 -> 범위 변경

#### ■ Oracle

1. 원격 OS 인증 방식이 불필요한 경우, SYS 계정으로 접속하여 'REMOTE\_OS\_AUTHENT=FALSE'로 설정

- spfile 사용하는 경우 아래와 같이 설정

```
SQL> ALTER SYSTEM SET REMOTE_OS_AUTHENT=FALSE SCOPE=spfile
```

- pfile 사용하는 경우 init<SID>.ora 파일 안에 아래와 같이 설정

```
SQL> ALTER SYSTEM SET REMOTE_OS_AUTHENT=FALSE
```

2. 원격 OS 인증 방식이 필요한 경우

- 방화벽을 통한 원격 접근 IP 제한
- NAT(Network Address Translation)를 사용하여 비공인 IP 부여 후 외부 접근 제한

#### ■ MySQL

1. mysql.user 테이블과 mysql.db 테이블을 조회하여 host가 "%"인 필드 삭제하고 접속 IP를 지정하여 등록

```
mysql> delete from user where host='%';
```

```
mysql> delete from db where host='%';
```

#### 조치 시 영향

허용되지 않은 IP에서 접속 제한

## DBMS

| 취약점 항목                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         | 2.2. DBA이외의 인가되지 않은 사용자 시스템 테이블 접근 제한 설정                                        |     |   |      |      |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------|-----|---|------|------|
| 대상                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             | Oracle, MSSQL, MySQL                                                            | 위험도 | 상 | Code | D-08 |
| 취약점 개요                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         | DBA만 접근 가능해야 할 테이블을 잘못 설정할 경우 비인가 사용자가 시스템의 주요 정보를 획득하거나, 주요 데이터베이스 설정 변경이 가능함. |     |   |      |      |
| 보안대책                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |                                                                                 |     |   |      |      |
| 판단기준                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           | 양호: DBA만 접근 가능한 테이블에 일반 사용자 접근이 불가능 할 경우                                        |     |   |      |      |
|                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                | 취약: DBA만 접근 가능한 테이블에 일반 사용자 접근이 가능한 경우                                          |     |   |      |      |
| 조치방법                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           | DBA만 접근 가능한 테이블(System Table)의 접근 권한 변경                                         |     |   |      |      |
| 보안설정방법                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |                                                                                 |     |   |      |      |
| ■ Oracle                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |                                                                                 |     |   |      |      |
| 1. DBA만 접근 가능한 테이블의 권한 확인(SQL*Plus)                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |                                                                                 |     |   |      |      |
| SQL> select grantee, privilege, owner, table_name from dba_tab_privs where (owner='SYS' or table_name like 'DBA_%') and privilege <> 'EXECUTE' and grantee not in ('PUBLIC', 'AQ_ADMINISTRATOR_ROLE', 'AQ_USER_ROLE', 'AURORA\$JIS\$UTILITY\$', 'OSE\$HTTP\$ADMIN', 'TRACESVR', 'CTXSYS', 'DBA', 'DELETE_CATALOG_ROLE', 'EXECUTE_CATALOG_ROLE', 'EXP_FULL_DATABASE', 'GATHER_SYSTEM_STATISTICS', 'HS_ADMIN_ROLE', 'IMP_FULL_DATABASE', 'LOGSTDBY_ADMINISTRATOR', 'MDSYS','ODM', 'OEM_MONITOR', 'OLAPSYS', 'ORDSYS', 'OUTLN', 'RECOVERY_CATALOG_OWNER', 'SELECT_CATALOG_ROLE', 'SNMPAGENT', 'SYSTEM', 'WKSYS', 'WKUSER', 'WMSYS', 'WM_ADMIN_ROLE', 'XDB', 'LBACSYS', 'PERFSTAT', 'XDBADMIN') and grantee not in (select grantee from dba_role_privs where granted_role='DBA') order by grantee; |                                                                                 |     |   |      |      |
| (어떤 계정이나 role이 나타나지 않으면 양호)                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |                                                                                 |     |   |      |      |
| 2. 불필요하게 테이블 접근 권한이 사용자 계정에 할당된 경우(SQL*Plus)                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |                                                                                 |     |   |      |      |
| SQL> REVOKE 권한 on 객체 FROM User                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |                                                                                 |     |   |      |      |
| ■ MSSQL                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |                                                                                 |     |   |      |      |
| 1. System tables 접근 권한이 Public, Guest 또는 비 인가된 사용자에게 부여된 경우 접근 권한을 Public, Guest, 비인가된 사용자로부터 권한 제거                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |                                                                                 |     |   |      |      |
| Use database name                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |                                                                                 |     |   |      |      |
| Revoke <권한> on <object> from [user name][[public]][[guest]]                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |                                                                                 |     |   |      |      |
| 2. 시스템 테이블에 접근하기 위해서는 stored procedure 또는, information_schema views를 통해 접근해야 함                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |                                                                                 |     |   |      |      |
| 3. 시스템 테이블에 접근 가능한 stored procedure는 사용이 제한되어야 함                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |                                                                                 |     |   |      |      |

### ■ MySQL

1. 일반 사용자로부터 mysql.user 테이블 모든 접근 권한 제거

```
mysql> revoke all on mysql.user from '[user name]'@[hosts];
mysql> flush privileges
```

2. 일반 사용자로부터 mysql.user 테이블 접근 권한 제거

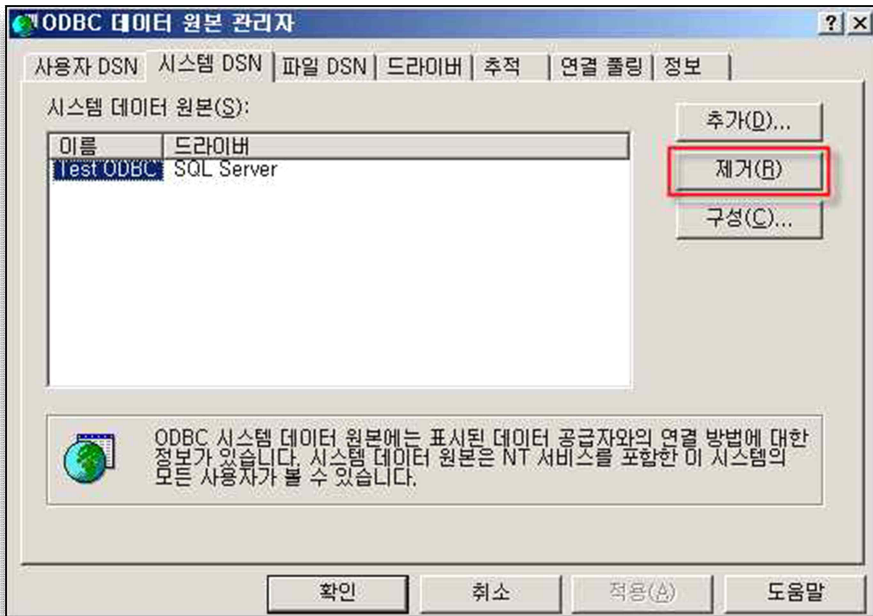
```
mysql> revoke [권한] on mysql.user from [user name];
mysql> flush privileges
```

|                |                        |
|----------------|------------------------|
| <b>조치 시 영향</b> | 사용자 계정으로 시스템 테이블 접근 불가 |
|----------------|------------------------|

## DBMS

| 취약점 항목                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              | 2.3. 오라클 데이터베이스의 경우 리스너 패스워드 설정                                                                                                                                                         |     |   |      |      |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----|---|------|------|
| 대상                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  | Oracle                                                                                                                                                                                  | 위험도 | 상 | Code | D-09 |
| 취약점 개요                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              | Listener의 패스워드가 설정되어 있지 않은 경우, Listener의 Owner라면 DBA가 아니라도 Listener를 Shutdown 시키거나 DB 서버에 임의의 파일을 생성할 수 있으며, 원격에서 LSNRCTL 유틸리티를 사용하여 listener.ora 파일에 대한 변경이 가능하므로 이를 수정하지 못하도록 설정해야 함. |     |   |      |      |
| 보안대책                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |                                                                                                                                                                                         |     |   |      |      |
| 판단기준                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                | 양호: Listener의 패스워드가 설정되어 있는 경우                                                                                                                                                          |     |   |      |      |
|                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     | 취약: Listener의 패스워드가 설정되어 있지 않은 경우                                                                                                                                                       |     |   |      |      |
| 조치방법                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                | Listener 패스워드 설정                                                                                                                                                                        |     |   |      |      |
| 보안설정방법                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |                                                                                                                                                                                         |     |   |      |      |
| <div>■ Oracle</div> <p>Listener에 패스워드가 설정되지 않은 경우 DoS, 정보 획득, Listener 프로세서를 다운 시킬 수 있는 위험이 있으므로 반드시 Listener 패스워드 설정 필요</p> <div>1. Listener 패스워드 설정</div> <pre>LSNRCTL&gt; change_password Old password:&lt;Old Password&gt; Not displayed New password:&lt;New password&gt; Not displayed Reenter new password:&lt;New password&gt; Not displayed Connecting (DESCRIPTION=(ADDRESS=(PROTOCOL=TCP)(HOST=prolin1)(PORT=1521)(IP=FIRST))) Password change for LISTENER The command completed successfully LSNRCTL&gt; set password LSNRCTL&gt; save_config</pre> <div>2. Listener 매개변수 설정</div> <p>(1) \$TNS_ADMIN/listener.ora 파일 안에 아래 Option 추가</p> <pre>PASSWORDS_&lt;listener name&gt;=&lt;Encrypted Password&gt; ADMIN_RESTRICTIONS_&lt;listener name&gt;=ON</pre> <p>(2) LSNRCTL&gt; reload Listener 재시작</p> |                                                                                                                                                                                         |     |   |      |      |
| 조치 시 영향                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             | 일반적으로 영향 없음                                                                                                                                                                             |     |   |      |      |

## DBMS

| 취약점 항목                                                                                                                                                                                                                                                                                                                                                  | 2.4. 불필요한 ODBC/OLE-DB 데이터 소스와 드라이브 제거                                                                                             |     |   |      |      |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------|-----|---|------|------|
| 대상                                                                                                                                                                                                                                                                                                                                                      | Windows OS                                                                                                                        | 위험도 | 중 | Code | D-10 |
| 취약점 개요                                                                                                                                                                                                                                                                                                                                                  | 애플리케이션에 따라 샘플 데이터베이스를 위해서 ODBC 데이터 소스를 설치하거나 불필요한 ODBC/OLE-DB 데이터베이스 드라이브를 설치하여 사용하는 경우 임의의 명령어 실행, 임의의 파일 수정, 시스템 관리자 권한 획득이 가능함 |     |   |      |      |
| 보안대책                                                                                                                                                                                                                                                                                                                                                    |                                                                                                                                   |     |   |      |      |
| 판단기준                                                                                                                                                                                                                                                                                                                                                    | 양호: 불필요한 ODBC/OLE-DB가 설치되지 않은 경우                                                                                                  |     |   |      |      |
|                                                                                                                                                                                                                                                                                                                                                         | 취약: 불필요한 ODBC/OLE-DB가 설치된 경우                                                                                                      |     |   |      |      |
| 조치방법                                                                                                                                                                                                                                                                                                                                                    | 불필요한 ODBC/OLE-DB 제거                                                                                                               |     |   |      |      |
| 보안설정방법                                                                                                                                                                                                                                                                                                                                                  |                                                                                                                                   |     |   |      |      |
| <div>■ Windows NT</div> <div>1. 사용하지 않는 불필요한 ODBC 데이터 소스 제거</div> <div>시작&gt; 설정&gt; 제어판&gt; 데이터 원본(ODBC)&gt; 시스템 DSN</div> <div>2. 사용하지 않는 데이터 소스 제거</div> <div>■ Windows 2000, 2003</div> <div>1. 사용하지 않는 불필요한 ODBC 데이터 소스 제거</div> <div>시작&gt; 설정&gt; 제어판&gt; 관리도구&gt; 데이터 원본 (ODBC)&gt; 시스템DSN&gt; 해당 드라이브 클릭</div> <div>2. 사용하지 않는 데이터 소스 제거</div> |                                                                                                                                   |     |   |      |      |
| <div></div>                                                                                                                                                                                                                                                         |                                                                                                                                   |     |   |      |      |
| 조치 시 영향                                                                                                                                                                                                                                                                                                                                                 | 일반적으로 영향 없음                                                                                                                       |     |   |      |      |

## DBMS

| 취약점 항목                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             | 2.5. 일정 횟수의 로그인 실패 시 잠금 정책 설정                                                    |     |   |      |      |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------|-----|---|------|------|
| 대상                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 | Oracle                                                                           | 위험도 | 중 | Code | D-11 |
| 취약점 개요                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             | 일정한 횟수의 로그인 실패 횟수 발생 시 이를 제한하지 않으면 무작위 추측 공격 (Brute force)을 통하여 데이터베이스에 접근이 가능함. |     |   |      |      |
| 보안대책                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |                                                                                  |     |   |      |      |
| 판단기준                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               | 양호: 로그인 시도 횟수를 제한하는 값을 설정한 경우                                                    |     |   |      |      |
|                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    | 취약: 로그인 시도 횟수가 UNLIMITED로 설정된 경우                                                 |     |   |      |      |
| 조치방법                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               | 로그인 시도 횟수 제한 값 설정                                                                |     |   |      |      |
| 보안설정방법                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |                                                                                  |     |   |      |      |
| <div>■ Oracle</div> <div>1. 접근 횟수 제한을 위해 파라미터 설정</div> <div>Failed_login_attempts 프로파일 파라미터 수정</div> <div>SQL&gt; ALTER PROFILE LIMIT FAILED_LOGIN_ATTEMPTS XXX</div> <div>XXX회 이하로 설정</div> <div>2. 프로파일 적용</div> <div>SQL&gt; connect / as sysdba</div> <div>SQL&gt; @\$Ora_Home/rdbms/admin/utlpwdmg.sql</div> <div>또는, default profile에 unlimited로 설정하고 이 default 값을 적용하고자 하는 profile에 적용</div> <div>SQL&gt; Alter profile default limit password_lock_time unlimited;</div> <div>SQL&gt; Alter profile [profile name] limit password_lock_time default;</div> |                                                                                  |     |   |      |      |
| 조치 시 영향                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            | 일반적으로 영향 없음                                                                      |     |   |      |      |

## DBMS

|                                                                                                                                       |                                                                                                                                    |     |   |      |      |
|---------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------|-----|---|------|------|
| 취약점 항목                                                                                                                                | 2.6. 데이터베이스의 주요 파일 보호 등을 위해 DB 계정의 umask를 022 이상으로 설정                                                                              |     |   |      |      |
| 대상                                                                                                                                    | Unix OS                                                                                                                            | 위험도 | 하 | Code | D-12 |
| 취약점 개요                                                                                                                                | Oracle 소프트웨어의 주요 파일에 대한 보호 등을 위해 Oracle 계정의 umask는 022 이상으로 설정되어야 하며, 설정되어있지 않은 경우 인가되지 않은 사용자가 이를 이용하여 관련 소프트웨어를 실행할 수 있는 위험이 있음. |     |   |      |      |
| 보안대책                                                                                                                                  |                                                                                                                                    |     |   |      |      |
| 판단기준                                                                                                                                  | 양호: 계정의 umask가 022 이상으로 설정되어있는 경우                                                                                                  |     |   |      |      |
|                                                                                                                                       | 취약: 계정의 umask가 022 이하로 설정되어있는 경우                                                                                                   |     |   |      |      |
| 조치방법                                                                                                                                  | 계정의 umask를 022 이상으로 설정 변경                                                                                                          |     |   |      |      |
| 보안설정방법                                                                                                                                |                                                                                                                                    |     |   |      |      |
| ■ Unix OS                                                                                                                             |                                                                                                                                    |     |   |      |      |
| 일시적 설정으로 umask 명령을 이용하여 umask 022 이상 설정> 시스템 재부팅> 설정 내역 유지를 위해 .bashrc, .cshrc, .login,.profile 등의 환경 변수 지정 파일에 umask 022(이상 설정)를 추가함 |                                                                                                                                    |     |   |      |      |
| 조치 시 영향                                                                                                                               | 일반적으로 영향 없음                                                                                                                        |     |   |      |      |

## DBMS

| 취약점 항목                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          | 2.7. 데이터베이스의 주요 설정파일, 패스워드 파일 등 주요 파일들의 접근 권한 설정                                                                                                            |     |   |      |      |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------|-----|---|------|------|
| 대상                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              | Unix OS, Windows OS                                                                                                                                         | 위험도 | 중 | Code | D-13 |
| 취약점 개요                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          | 비인가자가 redo 파일, 데이터베이스 설정 파일, 데이터 파일, 네트워크 설정 파일, Oracle 패스워드 관련 파일인 orapw.ora, listener.ora,init<SID>.ora 등의 주요 파일에 접근하여 수정·삭제하면 Oracle 데이터베이스 운영에 오류가 발생함. |     |   |      |      |
| 보안대책                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |                                                                                                                                                             |     |   |      |      |
| 판단기준                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            | 양호: 주요 설정 파일 및 디렉터리의 퍼미션 설정이 되어있는 경우                                                                                                                        |     |   |      |      |
|                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 | 취약: 주요 설정 파일 및 디렉터리의 퍼미션 설정이 되어있지 않은 경우                                                                                                                     |     |   |      |      |
| 조치방법                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            | 주요 설정 파일 및 디렉터리의 퍼미션 설정 변경                                                                                                                                  |     |   |      |      |
| 보안설정방법                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |                                                                                                                                                             |     |   |      |      |
| <div>■ Oracle</div> <div>■ Unix OS</div> <div>1. 디렉터리 또는 파일의 퍼미션 점검</div> <div>\$ORACLE_HOME/bin/oracle (퍼미션 755)</div> <div>\$ORACLE_HOME/bin/ 아래 (퍼미션 755)</div> <div>.sqlplus, sqlldr, sqlload, proc, oraenv, oerr, exp, imp,tkprof,tnsping, wrap</div> <div>\$ORACLE_HOME/bin 아래 (퍼미션 750)</div> <div>.svrmgrl, lsnrctl, dbsnmp</div> <div>\$ORACLE_HOME/nework (퍼미션 755)</div> <div>\$ORACLE_HOME/network/admin (퍼미션 755)</div> <div>.listener.ora, sqlnet.ora 등</div> <div>\$ORACLE_HOME/lib (퍼미션 755)</div> <div>\$ORACLE_HOME/network/admin 아래 환경파일 (퍼미션 644)</div> <div>.tnsnames.ora, protocol.ora, sqlpnet.ora</div> <div>\$ORACLE_HOME/dbs/init.ora (퍼미션 640)</div> <div>\$ORACLE_HOME/dbs/init&lt;SID&gt;.ora (퍼미션 640)</div> <div>- Find \$ORACLE_HOME -name init*.ora -print</div> <div>2. redo 파일, 데이터베이스 설정 파일, 데이터 파일 위치 확인(SQL*Plus)</div> <div>SQL&gt; Select value from v\$parameter where name='spfile';</div> <div>SQL&gt; Select 'Control Files: '  value from v\$parameter where name='control_files';</div> <div>SQL&gt; select 'Control Files: '  value from v\$parameter where name='spfile';</div> <div>SQL&gt; select 'Logfile: '  member from v\$logfile;</div> <div>SQL&gt; select 'Datafile: '  name from v\$datafile;</div> <div>- 파일 및 디렉터리의 퍼미션 설정 변경</div> |                                                                                                                                                             |     |   |      |      |



## DBMS

## ■ Windows OS

1. 패스워드 파일(orapw<SID>) 접근 권한은 administrators, system group, owner group, oracle service account, DBAs에게 모든 권한 또는, 그 이하로 설정하고 다른 그룹은 제거함

## ■ MySQL

## ■ Unix OS

초기화 파일(my.cnf, my.ini)의 접근 권한을 초기화 파일에 대한 보호를 위하여 600 또는, 640으로 설정  
my.cnf 파일 디폴트 위치: /etc/my.cnf, <각 홈디렉터리>/my.cnf

```
chmod 600 ./my.cnf
```

## ■ Windows OS

초기화 파일의 접근 권한은 Administrators, SYSTEM, Owner에게 모든 권한 또는, 그 이하로 설정하고 다른 그룹은 제거함

## 조치 시 영향

일반적으로 영향 없음

## DBMS

| 취약점 항목                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           | 2.8. 관리자 이외의 사용자가 오라클 리스너의 접속을 통해 리스너 로그 및 trace 파일에 대한 변경 권한 제한                                                          |     |   |      |      |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------|-----|---|------|------|
| 대상                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               | Oracle                                                                                                                    | 위험도 | 하 | Code | D-14 |
| 취약점 개요                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           | Oracle의 LSNRCTL 도구를 이용하여 리스너에 직접 접근 시 set 명령어를 이용하여 리스너의 모든 파라미터를 변경할 수 있음. 파라미터 변경이 가능한 경우, trace파일 및 리스너 로그 파일 변경이 가능함. |     |   |      |      |
| 보안대책                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |                                                                                                                           |     |   |      |      |
| 판단기준                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             | 양호: 주요 설정 파일 및 로그 파일에 대한 퍼미션을 관리자로 설정한 경우                                                                                 |     |   |      |      |
|                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  | 취약: 주요 설정 파일 및 로그 파일에 대한 퍼미션이 일반 사용자로 설정되어있는 경우                                                                           |     |   |      |      |
| 조치방법                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             | 주요 파일 및 로그 파일에 대한 퍼미션을 관리자로 제한                                                                                            |     |   |      |      |
| 보안설정방법                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |                                                                                                                           |     |   |      |      |
| <div>■ Oracle</div> <div>1. 파일 퍼미션 확인</div> <div>\$ORACLE_HOME/network/admin 디렉터리의 퍼미션을 ls-al(Unix 계열 시스템) 또는, 파일 속성(Windows 계열)을 통해 확인</div> <div>LSNRCTL&gt; status ListenerName</div> <div>LISTENER.ORA 파일 확인</div> <div>ADMIN_RESTRICTIONS_ListenerName=ON</div> <div>2. listener.ora 파일에 ADMIN_RESTRICTIONS_LISTENER=ON 라인 추가</div> <div>listener를 재실행하거나 lsnrctl reload 명령어를 실행하여 listener 재로딩함</div> <div>#vi /Oracle_HomeDirectory/network/admin/listener.ora</div> <div>- ADMIN_RESTRICTIONS_LISTENER=ON 추가</div> <div>※ ListenerName은 DBA가 제공한 리스너 이름</div> <div>#cd /Oracle_Homedirectory/bin/에서</div> <div>#LSNRCTL&gt; reload</div> |                                                                                                                           |     |   |      |      |
| 조치 시 영향                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          | 일반적으로 영향 없음                                                                                                               |     |   |      |      |

## 3. 옵션관리

| 취약점 항목                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       | 3.1. 응용프로그램 또는 DBA 계정의 Role이 Public으로 설정되지 않도록 조정                                              |     |   |      |      |
|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------|-----|---|------|------|
| 대상                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           | Oracle, MSSQL                                                                                  | 위험도 | 상 | Code | D-15 |
| 취약점 개요                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       | 응용 프로그램 계정의 Role 또는 DBA 계정의 Role이 Public으로 설정되어 있으면, 일반 계정에서도 응용 프로그램 테이블 또는 DBA 테이블로의 접근이 가능함 |     |   |      |      |
| 보안대책                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |                                                                                                |     |   |      |      |
| 판단기준                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         | 양호: DBA 계정의 Role이 Public으로 설정되어있지 않은 경우                                                        |     |   |      |      |
|                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              | 취약: DBA 계정의 Role이 Public으로 설정되어있는 경우                                                           |     |   |      |      |
| 조치방법                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         | DBA 계정의 Role 설정에서 Public 그룹 권한 취소                                                              |     |   |      |      |
| 보안설정방법                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |                                                                                                |     |   |      |      |
| <div>■ Oracle</div> <div>1. DBA Role 설정 확인(SQL*Plus)</div> <div>SQL&gt; Select granted_role from dba_role_privs where grantee='PUBLIC';</div> <div>위와 같이 롤(role)이 설정되어 있는 경우 취약</div> <div>2. public 그룹의 권한 취소(SQL*Plus)</div> <div>SQL&gt; Revoke role from public;</div> <div>■ MSSQL</div> <div>1. 각 Object의 사용 권한이 불필요하게 Public, Guest에 부여된 경우 권한 제거</div> <div>Use database name</div> <div>(1) 권한 제거</div> <div>REVOKE &lt;권한&gt; on &lt;object&gt; FROM public guest;</div> <div>(2) 권한 부여</div> <div>GRANT &lt;권한&gt; on &lt;object&gt; TO public guest;</div> <div>(예) syscolumns 테이블에 대한 SELECT 권한 제거</div> <div>USE master</div> <div>REVOKE select on sys.syscolumns FROM public;</div> <div>※ Object 사용 권한이 Public에 부여된 경우, 사용 권한이 없는 모든 계정이 Object에 접근 가능하여 Object의 정보를 획득할 수 있으므로 Object 사용 권한을 Public에 부여하는 것을 제한하여야 함</div> |                                                                                                |     |   |      |      |
| 조치 시 영향                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      | 일반적으로 영향 없음                                                                                    |     |   |      |      |

## DBMS

| 취약점 항목                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  | 3.2. OS_ROLES, REMOTE_OS_AUTHENTICATION, REMOTE_OS_ROLES를 FALSE로 설정                                                                                                                                                             |     |   |      |      |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----|---|------|------|
| 대상                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      | Oracle                                                                                                                                                                                                                          | 위험도 | 상 | Code | D-16 |
| 취약점 개요                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  | OS_ROLES 설정 파라미터는 데이터베이스 접근 제어로 컨트롤되지 않는 OS 그룹에 의해 grant된 퍼미션이 허락되며, REMOTE_OS_ROLES가 TRUE로 설정되어 있는 경우, 원격 사용자가 OS의 다른 사용자로 속여 데이터베이스에 접근할 수 있음.<br>REMOTE_OS_AUTHENT가 TRUE로 설정되어있는 경우 신뢰하는 원격 호스트에서 인증 절차 없이 데이터베이스에 접속할 수 있음. |     |   |      |      |
| 보안대책                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |                                                                                                                                                                                                                                 |     |   |      |      |
| 판단기준                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    | 양호: OS_ROLES, REMOTE_OS_AUTHENTICATION, REMOTE_OS_ROLES설정이 FALSE로 되어있는 경우                                                                                                                                                       |     |   |      |      |
|                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         | 취약: OS_ROLES, REMOTE_OS_AUTHENTICATION, REMOTE_OS_ROLES설정이 TRUE로 되어있는 경우                                                                                                                                                        |     |   |      |      |
| 조치방법                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    | OS_ROLES, REMOTE_OS_AUTHENTICATION, REMOTE_OS_ROLES 설정을 FALSE로 설정                                                                                                                                                               |     |   |      |      |
| 보안설정방법                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |                                                                                                                                                                                                                                 |     |   |      |      |
| <div>■ Oracle</div> <div>1. 설정 확인(SQL*Plus)</div> <div>• OS_ROLES</div> <div>(1) SQL&gt; Show parameter os_roles;</div> <div>(2) SQL&gt; select value from v\$parameter where name='os_roles';</div> <div>(3) OS_ROLES 파라미터를 FALSE로 설정</div> <div>#vi /Oracle_HomeDirectory/admin/pfile/init.ora에서 OS_Role=False 추가</div> <div>• REMOTE_OS_AUTHENTICATION</div> <div>(1) SQL&gt; Show parameter remote_os_authent;</div> <div>(2) SQL&gt; Select value from v\$parameter where name='remote_os_authent';</div> <div>(3) init.ora 파일에서 remote_os_authent=FALSE 추가</div> <div>pfile='\$full_path/init.ora'</div> <div>버전 9i 이후 버전은 SPFILE을 재생성해야 하므로, DBMS를 Shutdown 시키면 spfile이 재생성 됨</div> <div>• REMOTE_OS_ROLES</div> <div>(1) SQL&gt; Show parameter remote_os_roles;</div> <div>(2) SQL&gt; Select value from v\$parameter where name='remote_os_roles';</div> <div>(3) init.ora 파일에 remote_os_roles=FALSE 추가</div> |                                                                                                                                                                                                                                 |     |   |      |      |
| 조치 시 영향                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 | 일반적으로 영향 없음                                                                                                                                                                                                                     |     |   |      |      |

## DBMS

| 취약점 항목                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               | 3.3. 패스워드 확인함수가 설정되어 적용되는가?                                                                                                                                                |     |   |      |      |              |  |                       |                    |                    |                    |                     |                        |                    |                         |                          |                        |                    |                                         |                     |                                                                                         |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----|---|------|------|--------------|--|-----------------------|--------------------|--------------------|--------------------|---------------------|------------------------|--------------------|-------------------------|--------------------------|------------------------|--------------------|-----------------------------------------|---------------------|-----------------------------------------------------------------------------------------|
| 대상                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   | Oracle                                                                                                                                                                     | 위험도 | 중 | Code | D-17 |              |  |                       |                    |                    |                    |                     |                        |                    |                         |                          |                        |                    |                                         |                     |                                                                                         |
| 취약점 개요                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               | PASSWORD_VERIFY_FUNCTION 값은 이 프로파일에 명시된 사용자가 데이터베이스에 로그인 할 때 패스워드 확인을 위해 PL/SQL 함수가 사용되도록 명시하는 프로파일임. PASSWORD_VERIFY_FUNCTION 값이 명시되지 않은 경우 기본적인 패스워드 정책이 적용되지 않는 경우 존재함. |     |   |      |      |              |  |                       |                    |                    |                    |                     |                        |                    |                         |                          |                        |                    |                                         |                     |                                                                                         |
| 보안대책                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |                                                                                                                                                                            |     |   |      |      |              |  |                       |                    |                    |                    |                     |                        |                    |                         |                          |                        |                    |                                         |                     |                                                                                         |
| 판단기준                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 | 양호: 패스워드 검증 함수로 검증이 진행되는 경우                                                                                                                                                |     |   |      |      |              |  |                       |                    |                    |                    |                     |                        |                    |                         |                          |                        |                    |                                         |                     |                                                                                         |
|                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      | 취약: 패스워드 검증 함수가 설정되지 않은 경우                                                                                                                                                 |     |   |      |      |              |  |                       |                    |                    |                    |                     |                        |                    |                         |                          |                        |                    |                                         |                     |                                                                                         |
| 조치방법                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 | 패스워드 검증 함수(PASSWORD_VERIFY_FUNCTION) 사용 설정                                                                                                                                 |     |   |      |      |              |  |                       |                    |                    |                    |                     |                        |                    |                         |                          |                        |                    |                                         |                     |                                                                                         |
| 보안설정방법                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |                                                                                                                                                                            |     |   |      |      |              |  |                       |                    |                    |                    |                     |                        |                    |                         |                          |                        |                    |                                         |                     |                                                                                         |
| <div>■ Oracle</div> <div>1. 설정 확인(SQL*Plus)</div> <div>SQL&gt; SELECT profile, limit FROM dba_profiles, (SELECT limit AS def_pwd_verify_func FROM dba_profiles WHERE resource_name = 'PASSWORD_VERIFY_FUNCTION' AND profile = 'DEFAULT') WHERE resource_name='PASSWORD_VERIFY_FUNCTION' AND REPLACE(limit,'DEFAULT',def_pwd_verify_func) in ('UNLIMITED','NULL');</div> <div>(반환 레코드가 존재하는 경우 취약)</div> <div>2. 패스워드 복잡도를 강제하는 패스워드 검증 함수를 생성, 사용하여야 함</div> <div>패스워드 확인 함수 적용 예시</div> <div>SQL&gt; Alter profile default limit</div> <div>SQL&gt; Password_verify_function verify_password_dod;</div>                             |                                                                                                                                                                            |     |   |      |      |              |  |                       |                    |                    |                    |                     |                        |                    |                         |                          |                        |                    |                                         |                     |                                                                                         |
| <table><tr><th colspan="2">PARAMETER 설명</th></tr><tr><td>FAILED_LOGIN_ATTEMPTS</td><td>log on 시도 반복 허용 횟수</td></tr><tr><td>PASSWORD_LIFE_TIME</td><td>password의 수명 날짜 기간</td></tr><tr><td>PASSWORD_REUSE_TIME</td><td>password의 재사용 금지 날짜 기간</td></tr><tr><td>PASSWORD_REUSE_MAX</td><td>password의 재사용 가능한 최대 횟수</td></tr><tr><td>PASSWORD_VERIFY_FUNCTION</td><td>password의 검증 함수로 검증 진행</td></tr><tr><td>PASSWORD_LOCK_TIME</td><td>password의 log on 허용 횟수 실패 후 계정 잠금 날짜 기간</td></tr><tr><td>PASSWORD_GRACE_TIME</td><td>password가 만료된 후 password_life_time이 경과되어 비밀번호를 변경해야 할 경우, password를 변경할 수 있는 기간을 날수로 지정</td></tr></table> |                                                                                                                                                                            |     |   |      |      | PARAMETER 설명 |  | FAILED_LOGIN_ATTEMPTS | log on 시도 반복 허용 횟수 | PASSWORD_LIFE_TIME | password의 수명 날짜 기간 | PASSWORD_REUSE_TIME | password의 재사용 금지 날짜 기간 | PASSWORD_REUSE_MAX | password의 재사용 가능한 최대 횟수 | PASSWORD_VERIFY_FUNCTION | password의 검증 함수로 검증 진행 | PASSWORD_LOCK_TIME | password의 log on 허용 횟수 실패 후 계정 잠금 날짜 기간 | PASSWORD_GRACE_TIME | password가 만료된 후 password_life_time이 경과되어 비밀번호를 변경해야 할 경우, password를 변경할 수 있는 기간을 날수로 지정 |
| PARAMETER 설명                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |                                                                                                                                                                            |     |   |      |      |              |  |                       |                    |                    |                    |                     |                        |                    |                         |                          |                        |                    |                                         |                     |                                                                                         |
| FAILED_LOGIN_ATTEMPTS                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                | log on 시도 반복 허용 횟수                                                                                                                                                         |     |   |      |      |              |  |                       |                    |                    |                    |                     |                        |                    |                         |                          |                        |                    |                                         |                     |                                                                                         |
| PASSWORD_LIFE_TIME                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   | password의 수명 날짜 기간                                                                                                                                                         |     |   |      |      |              |  |                       |                    |                    |                    |                     |                        |                    |                         |                          |                        |                    |                                         |                     |                                                                                         |
| PASSWORD_REUSE_TIME                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  | password의 재사용 금지 날짜 기간                                                                                                                                                     |     |   |      |      |              |  |                       |                    |                    |                    |                     |                        |                    |                         |                          |                        |                    |                                         |                     |                                                                                         |
| PASSWORD_REUSE_MAX                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   | password의 재사용 가능한 최대 횟수                                                                                                                                                    |     |   |      |      |              |  |                       |                    |                    |                    |                     |                        |                    |                         |                          |                        |                    |                                         |                     |                                                                                         |
| PASSWORD_VERIFY_FUNCTION                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             | password의 검증 함수로 검증 진행                                                                                                                                                     |     |   |      |      |              |  |                       |                    |                    |                    |                     |                        |                    |                         |                          |                        |                    |                                         |                     |                                                                                         |
| PASSWORD_LOCK_TIME                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   | password의 log on 허용 횟수 실패 후 계정 잠금 날짜 기간                                                                                                                                    |     |   |      |      |              |  |                       |                    |                    |                    |                     |                        |                    |                         |                          |                        |                    |                                         |                     |                                                                                         |
| PASSWORD_GRACE_TIME                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  | password가 만료된 후 password_life_time이 경과되어 비밀번호를 변경해야 할 경우, password를 변경할 수 있는 기간을 날수로 지정                                                                                    |     |   |      |      |              |  |                       |                    |                    |                    |                     |                        |                    |                         |                          |                        |                    |                                         |                     |                                                                                         |
| 조치 시 영향                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              | 일반적으로 영향 없음                                                                                                                                                                |     |   |      |      |              |  |                       |                    |                    |                    |                     |                        |                    |                         |                          |                        |                    |                                         |                     |                                                                                         |

DBMS

| 취약점 항목                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              | 3.4. 인가되지 않은 Object Owner가 존재하지 않는가?                                                                                     |     |   |      |      |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------|-----|---|------|------|
| 대상                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  | Oracle                                                                                                                   | 위험도 | 하 | Code | D-18 |
| 취약점 개요                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              | Object Owner는 SYS, SYSTEM과 같은 데이터베이스 관리자 계정과 응용 프로그램의 관리자 계정에만 존재하여야 하며, 일반 계정이 존재할 경우 공격자가 이를 이용하여 Object의 수정, 삭제가 가능함. |     |   |      |      |
| 보안대책                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |                                                                                                                          |     |   |      |      |
| 판단기준                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                | 양호: Object Owner 의 권한이 SYS, SYSTEM, 관리자 계정 등으로 제한된 경우                                                                    |     |   |      |      |
|                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     | 취약: Object Owner 의 권한이 일반 사용자에게도 부여되어있는 경우                                                                               |     |   |      |      |
| 조치방법                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                | Object Owner의 권한을 SYS, SYSTEM, 관리자 계정으로 제한 설정                                                                            |     |   |      |      |
| 보안설정방법                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |                                                                                                                          |     |   |      |      |
| <div>■ Oracle</div> <div>1. 설정 확인(SQL*Plus)</div> <div>SQL&gt; Select distinct owner from dba_objects where owner not in ('SYS','SYSTEM','MDSYS','CTXSYS','ORDSYS', 'ORDPLUGINS', 'AURORA\$JIS\$UTILITY\$','HR','ODM','ODM_MTR','OE','OLAPDBA','OLA PSYS', 'OSE\$HTTP\$ADMIN', 'OUTLN', 'LBACSYS', 'MTSYS', 'PM', 'PUBLIC', 'QS', 'QS_ADM', 'QS_CB', 'QS_CBADM', 'DBSNMP', 'QS_CS', 'QS_ES','QS_OS', 'QS_WS','RMAN', 'SH', 'WKSYS', 'WMSYS','XDB') and owner not in (select grantee from dba_role_privs where granted_role='DBA');</div> <div>2. 권한 취소(SQL*Plus)</div> <div>SQL&gt; REVOKE 권한 on 객체 FROM User</div> |                                                                                                                          |     |   |      |      |
| 조치 시 영향                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             | 일반적으로 영향 없음                                                                                                              |     |   |      |      |

## DBMS

| 취약점 항목                                                                                                                                                                                                                                                                                                                                                                                                                                                       | 3.5. grant option이 role에 의해 부여되도록 설정                                                                                 |     |   |      |      |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------|-----|---|------|------|
| 대상                                                                                                                                                                                                                                                                                                                                                                                                                                                           | Oracle                                                                                                               | 위험도 | 중 | Code | D-19 |
| 취약점 개요                                                                                                                                                                                                                                                                                                                                                                                                                                                       | 일반 사용자에게 GRANT OPTION이 설정되어있는 경우 일반 사용자가 객체 소유자인 것과 같이 다른 일반 사용자에게 권한을 부여할 수 있어 WITH_GRANT_OPTION은 role에 의하여 설정되어야 함 |     |   |      |      |
| 보안대책                                                                                                                                                                                                                                                                                                                                                                                                                                                         |                                                                                                                      |     |   |      |      |
| 판단기준                                                                                                                                                                                                                                                                                                                                                                                                                                                         | 양호: WITH_GRANT_OPTION이 ROLE에 의하여 설정되어있는 경우                                                                           |     |   |      |      |
|                                                                                                                                                                                                                                                                                                                                                                                                                                                              | 취약: WITH_GRANT_OPTION이 ROLE에 의하여 설정되어있지 않은 경우                                                                        |     |   |      |      |
| 조치방법                                                                                                                                                                                                                                                                                                                                                                                                                                                         | WITH_GRANT_OPTION이 ROLE에 의하여 설정되도록 변경                                                                                |     |   |      |      |
| 보안설정방법                                                                                                                                                                                                                                                                                                                                                                                                                                                       |                                                                                                                      |     |   |      |      |
| <div>■ Oracle</div> <div>1. 설정 확인(SQL*Plus)</div> <div>SQL&gt; Select grantee  ':'  owner  '.'  table_name from dba_tab_privs where grantable='YES' and owner not in ('SYS','MDSYS','ORDPLUGINS','ORDSYS','SYSTEM', 'WMSYS','SDB','LBACSYS') and grantee not in (select grantee from dba_role_privs where granted_role='DBA') order by grantee;</div> <div>(계정이 나오는 경우 취약)</div> <div>2. 권한 취소, 재부여(SQL*Plus)</div> <div>SQL&gt; REVOKE Role FROM User</div> |                                                                                                                      |     |   |      |      |
| 조치 시 영향                                                                                                                                                                                                                                                                                                                                                                                                                                                      | 일반적으로 영향 없음                                                                                                          |     |   |      |      |

DBMS

| 취약점 항목                                                                                                                                                                                                                     | 3.6. 데이터베이스의 자원 제한 기능을 TRUE로 설정                                                                                                          |     |   |      |      |
|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------|-----|---|------|------|
| 대상                                                                                                                                                                                                                         | Oracle                                                                                                                                   | 위험도 | 하 | Code | D-20 |
| 취약점 개요                                                                                                                                                                                                                     | 설정 옵션 RESOURCE_LIMIT에 의해서 모든 프로파일 limit 설정 값을 무시할 수 있음.<br>기본적으로 설정 옵션 RESOURCE_LIMIT 값이 TRUE로 설정되어있지 않으면 모든 프로파일 limit 설정 값들은 무시될 수 있음. |     |   |      |      |
| 보안대책                                                                                                                                                                                                                       |                                                                                                                                          |     |   |      |      |
| 판단기준                                                                                                                                                                                                                       | 양호: RESOURCE_LIMIT 설정이 TRUE로 되어있는 경우                                                                                                     |     |   |      |      |
|                                                                                                                                                                                                                            | 취약: RESOURCE_LIMIT 설정이 FALSE로 되어있는 경우                                                                                                    |     |   |      |      |
| 조치방법                                                                                                                                                                                                                       | RESOURCE_LIMIT 설정을 TRUE로 설정 변경                                                                                                           |     |   |      |      |
| 보안설정방법                                                                                                                                                                                                                     |                                                                                                                                          |     |   |      |      |
| <div>■ Oracle</div> <div>1. init.ora 설정 파일에 RESOURCE_LIMIT = TRUE' 라인 추가</div> <div>#vi /Oracle_HomeDirectory/admin/pfile/init.ora</div> <div>2. SQL*Plus에서</div> <div>SQL&gt; Alter System Set Resource_Limit=TRUE;</div> |                                                                                                                                          |     |   |      |      |
| 조치 시 영향                                                                                                                                                                                                                    | 일반적으로 영향 없음                                                                                                                              |     |   |      |      |



## 4. 패치관리

| 취약점 항목                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             | 4.1. 데이터베이스에 대해 최신 보안패치와 밴더 권고사항을 모두 적용                           |     |   |      |      |
|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------|-----|---|------|------|
| 대상                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 | Oracle, MSSQL, MySQL                                              | 위험도 | 상 | Code | D-21 |
| 취약점 개요                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             | 데이터베이스의 주요 보안 패치 등을 설치하지 않은 경우 공격자가 알려진 취약점을 이용하여 데이터베이스에 접근 가능함. |     |   |      |      |
| 보안대책                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |                                                                   |     |   |      |      |
| 판단기준                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               | 양호: 버전별 최신 패치를 적용한 경우                                             |     |   |      |      |
|                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    | 취약: 버전별 최신 패치를 적용하지 않은 경우                                         |     |   |      |      |
| 조치방법                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               | 데이터베이스에 대한 버전을 확인 후 업그레이드 및 패치 적용                                 |     |   |      |      |
| 보안설정방법                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |                                                                   |     |   |      |      |
| <div>■ Oracle</div> <p>ORACLE_HOME에 설치된 Oracle 제품 컴포넌트를 조회하거나, 적용된 임시 패치를 조회할 때는 lsinventory 명령어를 사용함</p> <ul style="list-style-type: none"><li>Oracle 제공 패치 명령을 이용하여 확인함</li></ul> <pre>\$opatchlsinventory[ -all ] [ -detail ] [ -invPtrLoc ] [ -jre ] [ -oh ]</pre> <p>all : ORACLE_BASE 밑에 설치된 모든ORACLE_HOME 정보를 표시<br/>detail : 설치된 패치 내에 포함된 라이브러리 파일까지 표시하므로<br/>패치 적용 시 충돌되는 객체 파일을 확인 가능함</p> <div>■ Unix 시스템</div> <pre>\$ORACLE_HOME/OPatch/opatchlsinventory -detail</pre> <div>■ Windows 시스템</div> <pre>%ORACLE_HOME%\WOPatch\wopatchlsinventory -detail</pre> <p>http://metalink.oracle.com에서 최신 패치 버전 확인 후 opatch 명령을 통해 도출된 결과를 비교함</p> <ul style="list-style-type: none"><li>- 버전이 9.2.0, 10.2.0, or 10.1.0이 아니면 아주 취약함</li><li>- Oracle 10g Release 2의 patchset level이 10.2.0.1이나 이후 버전이 아니면 취약함</li><li>- Oracle 10g Release 1의 patchset level이 10.1.0.4이나 이후 버전이 아니면 취약함</li><li>- Oracle 9i Release 2의 patchset level이 9.2.0.6이나 이후 버전이 아니면 취약함</li><li>- Oracle 9.0이 Oracle 9iAS 또는 Oracle AS10g를 지원하기 위해 사용되면 취약함</li></ul> |                                                                   |     |   |      |      |

## DBMS

| 데이터베이스 명             | 적용 패치                          |
|----------------------|--------------------------------|
| Oracle 10g Release 2 | 10.2.0.5 Windows 64bit itanium |
| Oracle 10g Release 2 | 10.2.0.4 Windows, MAC OS X     |
| Oracle 10g Release 2 | 10.2.0.1 All OS                |
| Oracle 10g Release 1 | 10.1.0.5                       |
| Oracle 9i Release 2  | 9.2.0.8                        |
| Oracle 9i Release 1  | 9.0.1.4                        |
| Oracle 8i Release 3  | 8.1.7.4                        |
| Oracle 8i            | 8.0.6.3                        |

※ 참고 사이트

<http://www.oracle.com/technetwork/database/enterprise-edition/downloads/index.html>

### ■ MSSQL

| Release                         | Sqlserver.exe |
|---------------------------------|---------------|
| SQL Server 2000 SP 4            | 8.00.2283     |
| SQL Server 2000 SP 3            | 8.00.1007     |
| SQL Server 2000 SP 2            | 8.00.534      |
| SQL Server 2000 SP 1            | 8.00.384      |
| SQL Server 2000 RTM             | 8.00.194      |
| SQL Server 2005 SP4 CU#3        | 9.00.5266     |
| SQL Server 2005 SP3 CU#15       | 9.00.4325     |
| SQL Server 2005 SP2 CU#17       | 9.00.3356     |
| SQL Server 2005 SP1             | 9.00.2047     |
| SQL Server 2005 RTM             | 9.00.1399     |
| SQL Server 2008 R2 SP2 CU #3    | 10.50.4266.00 |
| SQL Server 2008 R2 SP1 CU #9    | 10.50.2866.00 |
| SQL Server 2008 R2 RTM CU #13   | 10.50.1815.00 |
| SQL Server 2008 SP3 CU #8       | 10.00.5785.00 |
| SQL Server 2008 SP2 CU #11      | 10.00.4333.00 |
| SQL Server 2008 SP1 CU #16      | 10.00.2850.00 |
| SQL Server 2008 RTM CU #10      | 10.00.1835.00 |
| SQL Server 2012 SP1 + KB2765331 | 11.00.3321.00 |

※ 참고 사이트

<http://support.microsoft.com/kb/321185/en-us>

<http://www.sqlsecurity.com/FAQs/SQLServerVersionDatabase/tabid/63/Default.aspx>

## ■ MySQL

<Enterprise Release>

| Version | Last Version |
|---------|--------------|
| 6.0     | 6.0.11       |
| 5.6     | 5.6.9        |
| 5.5     | 5.5.6        |
| 5.4     | 5.4.2        |
| 5.1     | 5.1.40       |
| 5.0     | 5.0.88       |
| 4.1     | 4.1.22       |

※ 참고 사이트

버그 패치된 릴리즈 사이트 <http://downloads.mysql.com/archives.php>

버그 현황 사이트 <http://bugs.mysql.com/bugstats.php>

**조치 시 영향** 적용 시 개발자 및 운영자와 협의 후 적용

## DBMS

| 취약점 항목 | 4.2. 데이터베이스의 접근, 변경, 삭제 등의 감사기록이 기관의 감사기록 정책에 적합하도록 설정                                                                                          |     |   |      |      |
|--------|-------------------------------------------------------------------------------------------------------------------------------------------------|-----|---|------|------|
| 대상     | Oracle, MSSQL                                                                                                                                   | 위험도 | 상 | Code | D-22 |
| 취약점 개요 | 데이터베이스의 감사 기록이 기관에서 정의한 감사 기록 정책에 적합하도록 기록해야 함. 데이터베이스는 데이터, 로그와 응용프로그램에 대한 백업 정책을 수립해야 하며, 지속적으로 준수하지 않을 경우 데이터베이스에 문제 발생 시 이를 효과적으로 대처할 수 없음. |     |   |      |      |
| 보안대책   |                                                                                                                                                 |     |   |      |      |
| 판단기준   | 양호: DBMS의 감사 로그 저장 정책이 수립되어 있으며, 정책이 적용되어있는 경우                                                                                                  |     |   |      |      |
|        | 취약: DBMS에 대한 감사 로그 저장을 하지 않거나, 정책이 수립되어있지 않은 경우                                                                                                 |     |   |      |      |
| 조치방법   | DBMS에 대한 감사 로그 저장 정책 수립, 적용                                                                                                                     |     |   |      |      |
| 보안설정방법 |                                                                                                                                                 |     |   |      |      |

## ■ Oracle

데이터베이스 감사 기록 정책 및 백업 정책 수립

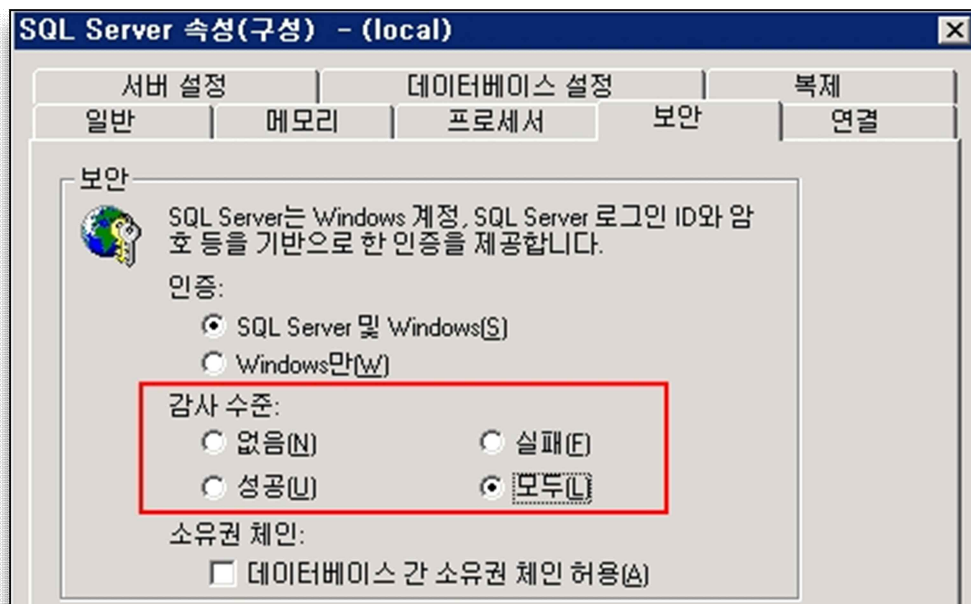
## ■ MSSQL

데이터베이스 감사 기록 정책 및 백업 정책 수립

## ■ MSSQL 2000

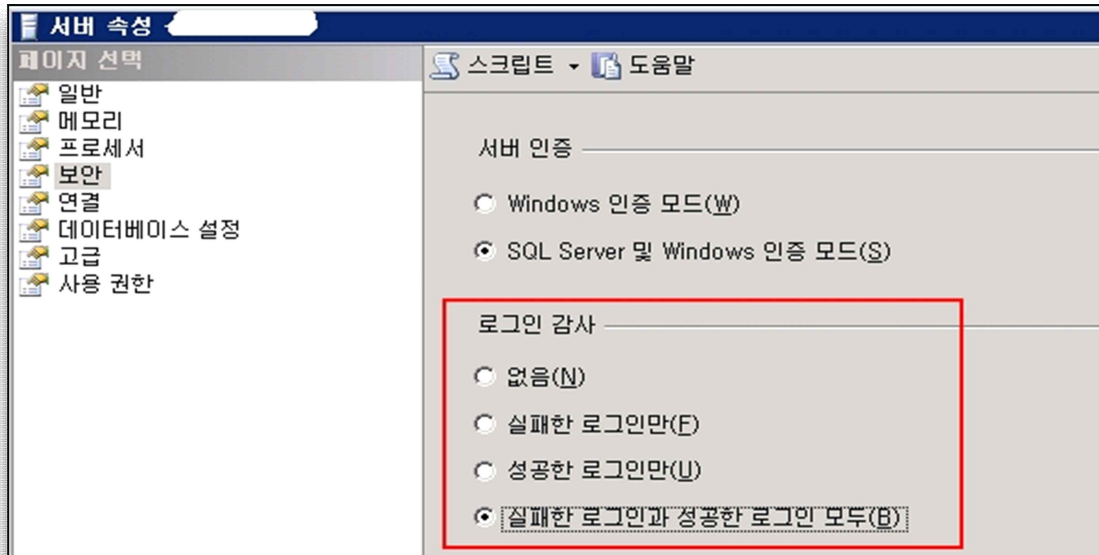
DB 접근에 대한 보안 감사를 할 수 있도록 보안 감사 설정

[SQL SERVER]> [등록정보]> [보안]탭> [감사수준]에서 '모두' 선택



## ■ MSSQL 2005

[MSSQL2005]> [오른쪽 마우스 클릭]> [속성]> [보안탭]> [로그인 감사] 옵션>  
 '실패한 로그인과 성공한 로그인 모두' 선택



## ■ MSSQL 2008 / 2012

[시스템 이름]> [오른쪽 마우스 클릭]> [속성]> [보안탭]> [로그인 감사] 옵션>  
 '실패한 로그인과 성공한 로그인 모두' 선택

|         |             |
|---------|-------------|
| 조치 시 영향 | 일반적으로 영향 없음 |
|---------|-------------|

DBMS

| 취약점 항목                                                                                                                                                                                   | 4.3. 보안에 취약하지 않은 버전의 데이터베이스를 사용하고 있는가?                                |     |   |      |      |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------|-----|---|------|------|
| 대상                                                                                                                                                                                       | Oracle                                                                | 위험도 | 중 | Code | D-23 |
| 취약점 개요                                                                                                                                                                                   | 벤더에서 보안 패치 등을 지원하지 않는 버전을 사용할 경우 공격자가 시스템 권한 획득 등을 수행할 수 있는 취약점이 존재함. |     |   |      |      |
| 보안대책                                                                                                                                                                                     |                                                                       |     |   |      |      |
| 판단기준                                                                                                                                                                                     | 양호: Oracle 보안 패치가 지원되는 버전을 사용하는 경우                                    |     |   |      |      |
|                                                                                                                                                                                          | 취약: Oracle 보안 패치가 지원되지 않는 버전을 사용하는 경우                                 |     |   |      |      |
| 조치방법                                                                                                                                                                                     | Oracle 보안패치가 지원되는 버전으로 업데이트                                           |     |   |      |      |
| 보안설정방법                                                                                                                                                                                   |                                                                       |     |   |      |      |
| <div>■ Oracle</div> <div>1. 9.2 버전 또는 이전 버전에 대한 업그레이드 계획이 없으면 취약점이 존재함</div> <div>2. 버전 확인(SQL*Plus)</div> <div>SQL&gt; select banner from v\$version where banner like 'Oracle%';</div> |                                                                       |     |   |      |      |
| 조치 시 영향                                                                                                                                                                                  | 일반적으로 영향 없음                                                           |     |   |      |      |

## 5. 로그관리

| 취약점 항목                                                                                                                                                                                                                                | 5.1. Audit Table은 데이터베이스 관리자 계정에 속해 있도록 설정                                                                   |     |   |      |      |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------|-----|---|------|------|
| 대상                                                                                                                                                                                                                                    | Oracle                                                                                                       | 위험도 | 하 | Code | D-24 |
| 취약점 개요                                                                                                                                                                                                                                | Audit Table은 반드시 SYS, SYSTEM과 같은 데이터베이스 관리자 계정에 속해 있어야 하며, 그렇지 않은 경우 인가되지 않은 사용자가 감사 데이터의 수정, 삭제 등의 수행이 가능함. |     |   |      |      |
| 보안대책                                                                                                                                                                                                                                  |                                                                                                              |     |   |      |      |
| 판단기준                                                                                                                                                                                                                                  | 양호: Audit Table 접근 권한이 관리자 계정으로 설정한 경우                                                                       |     |   |      |      |
|                                                                                                                                                                                                                                       | 취약: Audit Table 접근 권한이 일반 계정으로 설정한 경우                                                                        |     |   |      |      |
| 조치방법                                                                                                                                                                                                                                  | Audit Table 접근 권한 관리자 계정으로 설정                                                                                |     |   |      |      |
| 보안설정방법                                                                                                                                                                                                                                |                                                                                                              |     |   |      |      |
| <div>■ Oralce</div> <div>1. 설정 확인(SQL*Plus)</div> <div>SQL&gt; Select owner from dba_tables where table_name='AUD\$';</div> <div>SYS 또는 SYSTEM이 아닌 계정이 나올 경우 확인 후 권한 삭제</div> <div>2. Audit table에 접근할 권한이 없는 계정이 확인 될 경우 권한 삭제</div> |                                                                                                              |     |   |      |      |
| 조치 시 영향                                                                                                                                                                                                                               | 일반적으로 영향 없음                                                                                                  |     |   |      |      |

# Web(웹) 보안가이드라인

2014. 01



안전행정부 *희망의 새시대*



## Web 취약점 분석·평가 항목

| 분류                   | 항목 중요도 | 항목코드 |
|----------------------|--------|------|
| 버퍼 오버플로우             | 상      | BO   |
| 포맷스트링                | 상      | FS   |
| LDAP 인젝션             | 상      | LI   |
| 운영체제 명령 실행           | 상      | OC   |
| SQL 인젝션              | 상      | SI   |
| SSI 인젝션              | 상      | SS   |
| XPath 인젝션            | 상      | XI   |
| 디렉터리 인덱싱             | 상      | DI   |
| 정보 누출                | 상      | IL   |
| 악성 콘텐츠               | 상      | CS   |
| 크로스사이트 스크립팅          | 상      | XS   |
| 약한 문자열 강도            | 상      | BF   |
| 불충분한 인증              | 상      | IA   |
| 취약한 패스워드 복구          | 상      | PR   |
| 크로스사이트 리퀘스트 변조(CSRF) | 상      | CF   |
| 세션 예측                | 상      | SE   |
| 불충분한 인가              | 상      | IN   |
| 불충분한 세션 만료           | 상      | SC   |
| 세션 고정                | 상      | SF   |
| 자동화 공격               | 상      | AU   |
| 프로세스 검증 누락           | 상      | PV   |
| 파일 업로드               | 상      | FU   |
| 파일 다운로드              | 상      | FD   |
| 관리자 페이지 노출           | 상      | AE   |
| 경로 추적                | 상      | PT   |
| 위치 공개                | 상      | PL   |
| 데이터 평문 전송            | 상      | SN   |
| 쿠키 변조                | 상      | CC   |

## 웹(Web)

| 취약점 항목                                                                                                                                                                                                                                                                           | 1.1. 버퍼 오버플로우                                                                                                                        |     |   |      |    |
|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------|-----|---|------|----|
| 대상                                                                                                                                                                                                                                                                               | 소스코드                                                                                                                                 | 위험도 | 상 | Code | BO |
| 취약점 개요                                                                                                                                                                                                                                                                           | 애플리케이션 입력값의 크기에 대한 적절성이 검증되지 않을 경우 개발 시에 할당된 저장 공간보다 더 큰 값의 입력이 가능하고 이로 인한 오류 발생으로 의도되지 않은 정보 노출, 프로그램에 대한 비인가된 접근 및 사용 등이 발생할 수 있음. |     |   |      |    |
| 보안대책                                                                                                                                                                                                                                                                             |                                                                                                                                      |     |   |      |    |
| 판단기준                                                                                                                                                                                                                                                                             | 양호: 파라미터 입력값에 대한 검증이 이루어지는 경우                                                                                                        |     |   |      |    |
|                                                                                                                                                                                                                                                                                  | 취약: 파라미터 입력값에 대한 검증이 이루어지지 않고 에러가 발생하는 경우                                                                                            |     |   |      |    |
| 조치방법                                                                                                                                                                                                                                                                             | 외부 입력값을 동적으로 할당하여 사용하는 경우 변수의 값 범위를 검사                                                                                               |     |   |      |    |
| 보안설정방법                                                                                                                                                                                                                                                                           |                                                                                                                                      |     |   |      |    |
| <div>■ 점검방법</div> <div>1. 웹 애플리케이션에 많은 인수 값 전달 시 오류가 나타나는지 점검</div> <div>2. 게시물 작성 시 허용된 문자보다 많은 문자열 입력</div> <div>3. 사이트 검색란에 많은 문자열 전달</div> <div>(예) http://hostname.com/login.asp?id=xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx</div>                                          |                                                                                                                                      |     |   |      |    |
| <div>■ 보안설정방법</div> <div>1. 웹 서버의 제품 버전을 안전한 버전으로 유지하며, 보안 패치를 항상 최신으로 유지</div> <div>2. 웹 애플리케이션에 전달되는 인수 값을 필요한 크기만큼만 받을 수 있도록 변경</div> <div>3. 버퍼 오버플로우를 점검하는 웹 스캐닝 툴을 이용하여 주기적으로 점검</div> <div>4. 동적 메모리 할당을 위해 크기를 사용하는 경우 그 값이 음수가 아닌지 검사하여 버퍼오버플로우를 예방하는 형태로 소스코드 변경</div> |                                                                                                                                      |     |   |      |    |
| 조치 시 영향                                                                                                                                                                                                                                                                          | 일반적으로 영향 없음                                                                                                                          |     |   |      |    |

## 웹(Web)

| 취약점 항목                                                                                                                                                                                                                                                                |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           | 1.2. 포맷스트링 |   |      |    |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------|---|------|----|
| 대상                                                                                                                                                                                                                                                                    | 소스코드                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      | 위험도        | 상 | Code | FS |
| 취약점 개요                                                                                                                                                                                                                                                                | <p>C언어로 만드는 프로그램 중 변수의 값을 출력하거나 입력받을 때가 있는데 이때 입력받은 값을 조작하여 프로그램의 메모리 위치를 반환받아 메모리 주소를 변조하여 시스템의 관리자 권한을 획득할 수 있음. 입력값 검증 로직을 구현함으로써 이와 같은 위험으로부터 예방할 수 있음.</p> <p>※ printf 등의 함수에서 문자열 입력 포맷을 잘못된 형태로 입력하는 경우 나타나는 취약점으로 루트 권한을 획득하는 것도 가능함.</p> <p>포맷 스트링의 종류에는 여러 가지가 있는데 그중 C언어에서 일반적으로 Data(변수)를 입·출력문에서 일정한 형태로 받아들이거나 출력하기 위하여 사용하는 기호로는 다음과 같은 것들이 있음. (예) %d, %f, %c, %s, %x, %p ...</p> <p>%d : 정수형 10진수 상수</p> <p>%f : 실수형 상수</p> <p>%lf : 실수형 상수</p> <p>%c : 문자값</p> <p>%s : 문자 스트링</p> <p>%u : 양의 정수(10진수)</p> <p>%o : 양의정수 (8진수)</p> <p>%x : 양의 정수 (16진수)</p> <p>%n : 쓰인 총 바이트수</p> <p>%n 은 이전까지 입력되었던 문자열의 길이(Byte)수 만큼 해당 변수에 저장시키기 때문에 메모리의 내용도 변조 가능하므로 Format String 취약점에서 핵심이기도 함.</p> <p>문자열의 길이를 변조 시키고 싶은 값의 길이만큼 만든 후 %n을 써주게 되면 메모리상에 공격자가 원하는 값을 넣을 수 있게 됨.</p> |            |   |      |    |
|                                                                                                                                                                                                                                                                       | 보안대책                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |            |   |      |    |
| 판단기준                                                                                                                                                                                                                                                                  | <p><b>양호:</b> 임의의 문자열 입력에 대한 검증이 이루어지는 경우</p> <p><b>취약:</b> 임의의 문자열 입력에 대한 검증이 이루어지지 않으며, 오류가 발생하는 경우</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |            |   |      |    |
| 조치방법                                                                                                                                                                                                                                                                  | 임의의 문자열 입력에 대한 검증 로직 구현                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |            |   |      |    |
| 보안설정방법                                                                                                                                                                                                                                                                |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |            |   |      |    |
| ■ 보안설정방법                                                                                                                                                                                                                                                              |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |            |   |      |    |
| <p>컴파일러에서는 문자열 입력 포맷에 대한 자체적인 검사를 내장하고 있음</p> <p>(예) GCC에서는 문자열 입력 포맷과 실제 입력이 맞지 않는 경우에 대해 경고 옵션 존재</p> <p>하지만, 이 방식은 컴파일 시간에 문제를 발견할 수 있는 경우에 한해 검증 가능함</p> <p>런타임 상황에서는 퍼지 테스트를 이용하여 프로그램의 입력값으로 임의의 값을 넣어서 프로그램을 예외 상황으로 빠뜨리는 경우가 있으므로 이러한 경우에 버그가 없는지 확인이 필요함</p> |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |            |   |      |    |
| 조치 시 영향                                                                                                                                                                                                                                                               | 일반적으로 영향 없음                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |            |   |      |    |

## 웹(Web)

| 취약점 항목                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |                                                                                                                                                                                                                                                                                        | 1.3. LDAP 인젝션 |            |             |            |   |   |    |   |   |   |   |    |    |   |   |   |             |                    |  |            |             |            |       |        |        |      |        |     |    |    |      |           |      |       |         |        |            |     |             |   |   |   |   |  |  |  |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------|------------|-------------|------------|---|---|----|---|---|---|---|----|----|---|---|---|-------------|--------------------|--|------------|-------------|------------|-------|--------|--------|------|--------|-----|----|----|------|-----------|------|-------|---------|--------|------------|-----|-------------|---|---|---|---|--|--|--|
| 대상                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 | 소스코드                                                                                                                                                                                                                                                                                   | 위험도           | 상          | Code        | LI         |   |   |    |   |   |   |   |    |    |   |   |   |             |                    |  |            |             |            |       |        |        |      |        |     |    |    |      |           |      |       |         |        |            |     |             |   |   |   |   |  |  |  |
| 취약점 개요                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             | LDAP인젝션은 사용자 입력을 기반으로 LDAP(Lightweight Directory Access Protocol) 구문을 구축하여 웹 기반 응용 프로그램을 악용하는 데 사용되는 공격임.<br>응용 프로그램이 사용자 입력값에 대한 적절한 필터링 및 유효성 검증을 하지 않아 공격자는 로컬 프록시를 사용함으로 LDAP 문을 수정 가능함. 공격 성공 시 승인되지 않은 쿼리에 권한을 부여하고, LDAP 트리 내의 내용 수정이나 임의의 명령 실행을 가능하게 하므로 적절한 필터링 로직을 구현하여야 함. |               |            |             |            |   |   |    |   |   |   |   |    |    |   |   |   |             |                    |  |            |             |            |       |        |        |      |        |     |    |    |      |           |      |       |         |        |            |     |             |   |   |   |   |  |  |  |
|                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    | 보안대책                                                                                                                                                                                                                                                                                   |               |            |             |            |   |   |    |   |   |   |   |    |    |   |   |   |             |                    |  |            |             |            |       |        |        |      |        |     |    |    |      |           |      |       |         |        |            |     |             |   |   |   |   |  |  |  |
| 판단기준                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               | 양호: 임의의 문자열 입력에 대한 검증이 이루어지는 경우                                                                                                                                                                                                                                                        |               |            |             |            |   |   |    |   |   |   |   |    |    |   |   |   |             |                    |  |            |             |            |       |        |        |      |        |     |    |    |      |           |      |       |         |        |            |     |             |   |   |   |   |  |  |  |
|                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    | 취약: 임의의 문자열 입력에 대한 검증이 이루어지지 않은 경우                                                                                                                                                                                                                                                     |               |            |             |            |   |   |    |   |   |   |   |    |    |   |   |   |             |                    |  |            |             |            |       |        |        |      |        |     |    |    |      |           |      |       |         |        |            |     |             |   |   |   |   |  |  |  |
| 조치방법                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               | 지정된 문자열만 입력 허용, 임의의 문자열 입력에 대한 검증 로직 구현                                                                                                                                                                                                                                                |               |            |             |            |   |   |    |   |   |   |   |    |    |   |   |   |             |                    |  |            |             |            |       |        |        |      |        |     |    |    |      |           |      |       |         |        |            |     |             |   |   |   |   |  |  |  |
| 보안설정방법                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |                                                                                                                                                                                                                                                                                        |               |            |             |            |   |   |    |   |   |   |   |    |    |   |   |   |             |                    |  |            |             |            |       |        |        |      |        |     |    |    |      |           |      |       |         |        |            |     |             |   |   |   |   |  |  |  |
| <div>■ 보안설정방법</div> <div>1. 사용자 입력값을 White List로 지정하여 영문(a-z, A-Z)과 숫자(0-9)만을 허용</div> <div>2. DN과 필터에 사용되는 사용자 입력값에는 특수문자가 포함되지 않도록 특수문자 제거</div> <div>3. 특수문자를 사용해야 하는 경우 특수문자(DN에 사용되는 특수문자는 'w', 필터에 사용되는 특수문자는 =, +, &lt;, &gt;, #, ;, w 등)에 대해서는 실행 명령이 아닌 일반문자로 인식되도록 처리</div>                                                                                                                                                                                                                                                                                                                                                                              |                                                                                                                                                                                                                                                                                        |               |            |             |            |   |   |    |   |   |   |   |    |    |   |   |   |             |                    |  |            |             |            |       |        |        |      |        |     |    |    |      |           |      |       |         |        |            |     |             |   |   |   |   |  |  |  |
| ※ 참고: 필터링 대상                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |                                                                                                                                                                                                                                                                                        |               |            |             |            |   |   |    |   |   |   |   |    |    |   |   |   |             |                    |  |            |             |            |       |        |        |      |        |     |    |    |      |           |      |       |         |        |            |     |             |   |   |   |   |  |  |  |
| <table><tr><td>'</td><td>"</td><td>--</td><td>#</td><td>(</td><td>)</td></tr><tr><td>=</td><td>*/</td><td>/*</td><td>+</td><td>&lt;</td><td>&gt;</td></tr><tr><td>user_tables</td><td colspan="2">user_table_columns</td><td>table_name</td><td>column_name</td><td>Syscolumns</td></tr><tr><td>union</td><td>select</td><td>insert</td><td>drop</td><td>update</td><td>and</td></tr><tr><td>or</td><td>If</td><td>join</td><td>substring</td><td>from</td><td>where</td></tr><tr><td>declare</td><td>substr</td><td>openrowset</td><td>xp_</td><td>'sysobjects</td><td>%</td></tr><tr><td>*</td><td>;</td><td>&amp;</td><td> </td><td></td><td></td></tr></table> |                                                                                                                                                                                                                                                                                        |               |            |             |            | ' | " | -- | # | ( | ) | = | */ | /* | + | < | > | user_tables | user_table_columns |  | table_name | column_name | Syscolumns | union | select | insert | drop | update | and | or | If | join | substring | from | where | declare | substr | openrowset | xp_ | 'sysobjects | % | * | ; | & |  |  |  |
| '                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  | "                                                                                                                                                                                                                                                                                      | --            | #          | (           | )          |   |   |    |   |   |   |   |    |    |   |   |   |             |                    |  |            |             |            |       |        |        |      |        |     |    |    |      |           |      |       |         |        |            |     |             |   |   |   |   |  |  |  |
| =                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  | */                                                                                                                                                                                                                                                                                     | /*            | +          | <           | >          |   |   |    |   |   |   |   |    |    |   |   |   |             |                    |  |            |             |            |       |        |        |      |        |     |    |    |      |           |      |       |         |        |            |     |             |   |   |   |   |  |  |  |
| user_tables                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        | user_table_columns                                                                                                                                                                                                                                                                     |               | table_name | column_name | Syscolumns |   |   |    |   |   |   |   |    |    |   |   |   |             |                    |  |            |             |            |       |        |        |      |        |     |    |    |      |           |      |       |         |        |            |     |             |   |   |   |   |  |  |  |
| union                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              | select                                                                                                                                                                                                                                                                                 | insert        | drop       | update      | and        |   |   |    |   |   |   |   |    |    |   |   |   |             |                    |  |            |             |            |       |        |        |      |        |     |    |    |      |           |      |       |         |        |            |     |             |   |   |   |   |  |  |  |
| or                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 | If                                                                                                                                                                                                                                                                                     | join          | substring  | from        | where      |   |   |    |   |   |   |   |    |    |   |   |   |             |                    |  |            |             |            |       |        |        |      |        |     |    |    |      |           |      |       |         |        |            |     |             |   |   |   |   |  |  |  |
| declare                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            | substr                                                                                                                                                                                                                                                                                 | openrowset    | xp_        | 'sysobjects | %          |   |   |    |   |   |   |   |    |    |   |   |   |             |                    |  |            |             |            |       |        |        |      |        |     |    |    |      |           |      |       |         |        |            |     |             |   |   |   |   |  |  |  |
| *                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  | ;                                                                                                                                                                                                                                                                                      | &             |            |             |            |   |   |    |   |   |   |   |    |    |   |   |   |             |                    |  |            |             |            |       |        |        |      |        |     |    |    |      |           |      |       |         |        |            |     |             |   |   |   |   |  |  |  |
| 조치 시 영향                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            | 일반적으로 영향 없음                                                                                                                                                                                                                                                                            |               |            |             |            |   |   |    |   |   |   |   |    |    |   |   |   |             |                    |  |            |             |            |       |        |        |      |        |     |    |    |      |           |      |       |         |        |            |     |             |   |   |   |   |  |  |  |

## 웹(Web)

| 취약점 항목                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            | 1.4. 운영체제 명령 실행                                                                                                                                                                                 |     |   |      |    |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----|---|------|----|
| 대상                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                | 소스코드                                                                                                                                                                                            | 위험도 | 상 | Code | OC |
| 취약점 개요                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            | 웹 사이트의 인터페이스를 통해 웹 서버를 운영하는 운영체제 명령어를 입력할 경우 적절한 검증절차를 거치지 않은 사용자 입력값에 의해 의도하지 않은 시스템 명령어가 실행될 수 있음. 그 결과 부적절하게 권한이 변경되거나 시스템 동작 및 운영에 악영향을 줄 가능성이 있으므로 " ", "&", ";", "\"" 문자에 대한 필터링 구현이 필요함. |     |   |      |    |
| 보안대책                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |                                                                                                                                                                                                 |     |   |      |    |
| 판단기준                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              | 양호: 임의의 명령어 입력에 대한 검증이 이루어지는 경우                                                                                                                                                                 |     |   |      |    |
|                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   | 취약: 임의의 명령어 입력에 대해 명령이 실행되는 경우                                                                                                                                                                  |     |   |      |    |
| 조치방법                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              | 애플리케이션은 운영체제로부터 명령어를 직접적으로 호출하지 않도록 구현                                                                                                                                                          |     |   |      |    |
| 보안설정방법                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |                                                                                                                                                                                                 |     |   |      |    |
| <div>■ 보안설정방법</div> <div>1. 애플리케이션은 운영체제로부터 명령어를 직접적으로 호출하지 않도록 구현</div> <div>2. 명령어를 직접 호출하는 것이 필요한 경우에는, 데이터가 OS 의 명령어 해석기에 전달되기 전에 입력값 검증/확인 하도록 구현</div> <div>3. 입력값에 대한 파라미터 데이터의 "&amp;", " ", ";", "\"" 문자에 대한 필터링 처리</div> <div>※ 참고: "&amp;", " ", "\"" 문자 설명</div> <div><div>• &amp; : 윈도우 명령어 해석기에서 첫 번째 명령이 성공했을 경우만 두 번째 명령어를 실행</div><div>•   : 첫 번째 명령어가 성공하는지에 상관없이 두 번째 명령어를 실행</div><div>• ` : 쉘 해석기가 명령어를 해석하다 역 작은따옴표(‘) 내에 포함된 명령어를 만나면 기존 명령어를 계속 실행하기 전에 역 작은따옴표로 둘러싸인 명령어를 먼저 실행 (예) `ls -al`</div></div> |                                                                                                                                                                                                 |     |   |      |    |
| 조치 시 영향                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           | 일반적으로 영향 없음                                                                                                                                                                                     |     |   |      |    |

## 웹(Web)

| 취약점 항목                                                                                                                                                                                                                 |                                                                                                                                                                                                                       | 1.5. SQL 인젝션 |   |      |    |    |    |   |             |   |          |       |               |       |                  |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------|---|------|----|----|----|---|-------------|---|----------|-------|---------------|-------|------------------|
| 대상                                                                                                                                                                                                                     | 소스코드                                                                                                                                                                                                                  | 위험도          | 상 | Code | SI |    |    |   |             |   |          |       |               |       |                  |
| 취약점 개요                                                                                                                                                                                                                 | 대화형 웹 사이트는 사용자의 입력값을 이용하여 데이터베이스 접근을 위한 SQL 쿼리를 만들어 구현됨. SQL인젝션은 사용자의 입력값으로 웹 사이트 SQL 쿼리가 완성되는 약점을 이용하며, 입력값을 변조하여 비정상적인 SQL 쿼리를 조합하거나 실행함. 비정상적인 SQL 쿼리로 DBMS 및 데이터(Data)를 열람하거나 조작 가능하므로 사용자의 입력값에 대한 필터링을 구현하여야 함. |              |   |      |    |    |    |   |             |   |          |       |               |       |                  |
| 보안대책                                                                                                                                                                                                                   |                                                                                                                                                                                                                       |              |   |      |    |    |    |   |             |   |          |       |               |       |                  |
| 판단기준                                                                                                                                                                                                                   | 양호: 임의의 SQL Query 입력에 대한 검증이 이루어지는 경우                                                                                                                                                                                 |              |   |      |    |    |    |   |             |   |          |       |               |       |                  |
|                                                                                                                                                                                                                        | 취약: 임의의 SQL Query 입력에 대한 검증이 이루어지지 않는 경우                                                                                                                                                                              |              |   |      |    |    |    |   |             |   |          |       |               |       |                  |
| 조치방법                                                                                                                                                                                                                   | 임의의 SQL Query 입력에 대한 검증 로직 구현                                                                                                                                                                                         |              |   |      |    |    |    |   |             |   |          |       |               |       |                  |
| 보안설정방법                                                                                                                                                                                                                 |                                                                                                                                                                                                                       |              |   |      |    |    |    |   |             |   |          |       |               |       |                  |
| ■ 보안설정방법                                                                                                                                                                                                               |                                                                                                                                                                                                                       |              |   |      |    |    |    |   |             |   |          |       |               |       |                  |
| 1. 문자열 유효성 검증 로직 구현                                                                                                                                                                                                    |                                                                                                                                                                                                                       |              |   |      |    |    |    |   |             |   |          |       |               |       |                  |
| SQL Query에 사용되는 문자열에 대해 유효성 검사를 실시하는 프로세스 구현                                                                                                                                                                           |                                                                                                                                                                                                                       |              |   |      |    |    |    |   |             |   |          |       |               |       |                  |
| 아래와 같은 특수문자를 사용자 입력값으로 지정 금지                                                                                                                                                                                           |                                                                                                                                                                                                                       |              |   |      |    |    |    |   |             |   |          |       |               |       |                  |
| (아래 문자들은 해당 데이터베이스에 따라 달라질 수 있음)                                                                                                                                                                                       |                                                                                                                                                                                                                       |              |   |      |    |    |    |   |             |   |          |       |               |       |                  |
| <table><tr><th>문자</th><th>설명</th></tr><tr><td>'</td><td>문자 데이터 구분기호</td></tr><tr><td>;</td><td>쿼리 구분 기호</td></tr><tr><td>--, #</td><td>해당라인 주석 구분 기호</td></tr><tr><td>/* */</td><td>/* 와 */ 사이 구문 주석</td></tr></table> |                                                                                                                                                                                                                       |              |   |      |    | 문자 | 설명 | ' | 문자 데이터 구분기호 | ; | 쿼리 구분 기호 | --, # | 해당라인 주석 구분 기호 | /* */ | /* 와 */ 사이 구문 주석 |
| 문자                                                                                                                                                                                                                     | 설명                                                                                                                                                                                                                    |              |   |      |    |    |    |   |             |   |          |       |               |       |                  |
| '                                                                                                                                                                                                                      | 문자 데이터 구분기호                                                                                                                                                                                                           |              |   |      |    |    |    |   |             |   |          |       |               |       |                  |
| ;                                                                                                                                                                                                                      | 쿼리 구분 기호                                                                                                                                                                                                              |              |   |      |    |    |    |   |             |   |          |       |               |       |                  |
| --, #                                                                                                                                                                                                                  | 해당라인 주석 구분 기호                                                                                                                                                                                                         |              |   |      |    |    |    |   |             |   |          |       |               |       |                  |
| /* */                                                                                                                                                                                                                  | /* 와 */ 사이 구문 주석                                                                                                                                                                                                      |              |   |      |    |    |    |   |             |   |          |       |               |       |                  |
| 2. Dynamic SQL 구문 사용 금지                                                                                                                                                                                                |                                                                                                                                                                                                                       |              |   |      |    |    |    |   |             |   |          |       |               |       |                  |
| Dynamic SQL 구문 사용을 지양하며 파라미터에 문자열 검사 필수적용                                                                                                                                                                              |                                                                                                                                                                                                                       |              |   |      |    |    |    |   |             |   |          |       |               |       |                  |
| 3. 오류에 대한 예외처리                                                                                                                                                                                                         |                                                                                                                                                                                                                       |              |   |      |    |    |    |   |             |   |          |       |               |       |                  |
| 에러 메시지는 공격자에게 많은 정보를 제공하므로. 오류처리로 정보 노출을 최소화                                                                                                                                                                           |                                                                                                                                                                                                                       |              |   |      |    |    |    |   |             |   |          |       |               |       |                  |
| 시스템에서 제공하는 에러메시지 및 DBMS에서 제공하는 에러코드가 노출되지 않도록 예외처리                                                                                                                                                                     |                                                                                                                                                                                                                       |              |   |      |    |    |    |   |             |   |          |       |               |       |                  |
| 4. Stored Procedure 사용                                                                                                                                                                                                 |                                                                                                                                                                                                                       |              |   |      |    |    |    |   |             |   |          |       |               |       |                  |
| 데이터 접근의 추상화 제공을 위해 Stored Procedure 사용                                                                                                                                                                                 |                                                                                                                                                                                                                       |              |   |      |    |    |    |   |             |   |          |       |               |       |                  |
| 5. 필터링 등 입력값 검증 프로세스는 Client side script가 아닌, Server 페이지로 구현                                                                                                                                                           |                                                                                                                                                                                                                       |              |   |      |    |    |    |   |             |   |          |       |               |       |                  |
| ■ ASP                                                                                                                                                                                                                  |                                                                                                                                                                                                                       |              |   |      |    |    |    |   |             |   |          |       |               |       |                  |
| 1. 문자열 유효성 검증 로직 구현                                                                                                                                                                                                    |                                                                                                                                                                                                                       |              |   |      |    |    |    |   |             |   |          |       |               |       |                  |
| (예) 특정 문자열 필터링 적용 (※ 예로 제시한 것으로, 구현 시 다를 수 있음)                                                                                                                                                                         |                                                                                                                                                                                                                       |              |   |      |    |    |    |   |             |   |          |       |               |       |                  |

## 웹(Web)

```

function SQL_Injection(get_String)
 get_String = REPLACE(get_String, "'", "''")
 get_String = REPLACE(get_String, ";", "")
 get_String = REPLACE(get_String, "--", "")
 get_String = REPLACE(get_String, "select", "", 1, -1, 1)
 get_String = REPLACE(get_String, "insert", "", 1, -1, 1)
 get_String = REPLACE(get_String, "update", "", 1, -1, 1)
 get_String = REPLACE(get_String, "delete", "", 1, -1, 1)
 get_String = REPLACE(get_String, "drop", "", 1, -1, 1)
 get_String = REPLACE(get_String, "union", "", 1, -1, 1)
 get_String = REPLACE(get_String, "and", "", 1, -1, 1)
 get_String = REPLACE(get_String, "or", "", 1, -1, 1)
 get_String = REPLACE(get_String, "1=1", "", 1, -1, 1)
 get_String = REPLACE(get_String, "sp_", "", 1, -1, 1)
 get_String = REPLACE(get_String, "xp_", "", 1, -1, 1)
 get_String = REPLACE(get_String, "@variable", "", 1, -1, 1)
 get_String = REPLACE(get_String, "@@variable", "", 1, -1, 1)
 get_String = REPLACE(get_String, "exec", "", 1, -1, 1)
 get_String = REPLACE(get_String, "sysobject", "", 1, -1, 1)
 SQL_Injection = get_String
end function
.....

```

## ■ ASP.net

### 1. 문자열 유효성 검증 로직 구현

(예) 특정 문자열 필터링 적용 (※ 예로 제시한 것으로, 구현 시 다를 수 있음)  
 request로 입력값을 가져올 경우 입력값에서 특수문자를 제거하여 바인딩 하는 소스 삽입  
 replaceAll() 메소드를 사용하여 구현

```

private string SafeSqlLiteral(string inputSQL)
{
 Str = inputSQL.Replace("'", "''");
 Str = str. Replace(";","");
 Str = str. Replace("--","");
 Str = str. Replace("|","");
 Str = str. Replace(":","");
 Str = str. Replace("+","");
 Str = str. Replace("W","");
}

```

## 웹(Web)

```
Str = str. Replace("/", "");
```

```
.....
```

```
return str;
```

```
}
```

## 2. Dynamic SQL

```
Private void cmdLogin_Click(object sender, System.EventArgs e) {
 string strCnx = ConfigurationSettings.AppSettings["cnxNWindBad"];
 Using (SqlConnection cnx = new SqlConnection(strCnx))
 {
 SqlParameter prm;
 Cnx.Open();
 string strQry =
"SELECT Count(*) FROM Users WHERE UserName = @username " +
"AND Password = @password";
Int intRecs;
 SqlCommand cmd = new SqlCommand(strQry, cnx);
 cmd.CommandType = CommandType.Text;

 prm = new SqlParameter("@username", SqlDbType.VarChar, 50);
 prm.Direction = ParameterDirection.Input;
 prm.Value = txtUser.Text;
 cmd.Parameters.Add(prm);

 prm = new SqlParameter("@password", SqlDbType.VarChar, 50);
 prm.Direction = ParameterDirection.Input;
 prm.Value = txtPassword.Text;
 cmd.Parameters.Add(prm);

 intRecs = (int) cmd.ExecuteScalar();

 if(intRecs > 0) {
 FormsAuthentication.RedirectFromLoginPage(txtUser.Text, false);
 }
 else {
 lblMsg.Text = "Login attempt failed.";
 }
 }
}
```



## 웹(Web)

## ■ JSP

## 1. 문자열 유효성 검증 로직 구현

(예) 특정 문자열 필터링 적용 (※ 예로 제시한 것으로, 구현 시 다를 수 있음)

request로 입력값을 가져올 경우 입력값에서 특수문자를 제거하여 바인딩 하는 소스 삽입  
replaceAll() 메소드를 사용하여 구현

```
public static String makeQuery(String str) {
 String result = "";
 if(str != null) {
 result = chkNull(replace(str, "", ""));
 result = chkNull(replace(str, ";", ""));
 result = chkNull(replace(str, "--", ""));
 result = chkNull(replace(str, "|", ""));
 result = chkNull(replace(str, ":", ""));
 result = chkNull(replace(str, "+", ""));
 result = chkNull(replace(str, "W", ""));
 result = chkNull(replace(str, "/", ""));
 result = chkNull(replace(str.toLowerCase(), "select", ""));
 result = chkNull(replace(str.toLowerCase(), "update", ""));
 result = chkNull(replace(str.toLowerCase(), "delete", ""));
 result = chkNull(replace(str.toLowerCase(), "insert", ""));
 result = chkNull(replace(str.toLowerCase(), "where", ""));
 result = chkNull(replace(str.toLowerCase(), "from", ""));
 result = ""+result+"";
 }

 return result;
}

public static String chkNull(String str) {
 if (str == null)
 return "";
 else
 return str;
}
```

## 2. Dynamic SQL 구문 사용 금지

(예1) PreparedStatement 객체 사용 (※ 예로 제시한 것으로, 구현 시 다를 수 있음)

```
try{
 String tableName = props.getProperty("jdbc.tableName");
 String name = props.getProperty("jdbc.name")
 String qry = "SELECT * FROM ? WHERE Name = ?";
}
```

## 웹(Web)

```

 stmt = con.prepareStatement(query);
 stmt.setString(1, tableName);
 stmt.setString(2, name);
 rs = stmt.executeQuery();

}
catch (SQLException sqle){ }
finally { }

```

(예2) JDO API 사용 시 외부 입력값이 위치하는 부분을 "?"로 설정하여 실행 시 해당 파라미터가 실행되도록 수정 (※ 예로 제시한 것으로, 구현 시 다를 수 있음)

```

try{
 Properties props = new Properties();
 String filename = "contacts.txt";
 FileInputStream in = new FileInputStream(filename);
 Props.load(in);
 name = props.getProperty("name");
 if (name == null || "".equals(name)) return null;
 query += " where name = ?";
}
catch (IOException e)
{
 Javax.jdo.Query q = pm.newQuery(query);
 return (List<Contact>) q.execute(name);
}

```

(예3) J2EE Persistence API 사용 시 파라미터를 받는 쿼리를 생성하고 파라미터를 설정하여 실행 (※ 예로 제시한 것으로, 구현 시 다를 수 있음)

```

try{
 Properties props = new Properties();
 String filename = "contacts.txt";
 FileInputStream in = new FileInputStream(filename);
 Props.load(in);
 String id = props.getProperty("id");
 If (id == null || "".equals(id)) id = "itemid";
 Query query = em.createNativeQuery("Select OBJECT(i) from Item I where
i.itemID > :id");
 Query.setParameter("id", id);
 }

```

## 웹(Web)

(예4) mybatis Data Map 사용 시 쿼리에 삽입되는 Name 파라미터를 #name# 형태로 받아 실행  
(※ 예로 제시한 것으로, 구현 시 다를 수 있음)

```
<?xml version="1.0" encoding="UTF-8"?>
.....
<!-- static SQL 사용 -->
<delete id="delStudent" parameterClass="Student">
DELETE STUDENTS
WHERE NUM = #num# AND Name = '#name#'
</delete>
```

## ■ PHP

### 1. 문자열 유효성 검증 로직 구현

(예1) addslashes 함수를 이용한 특정 문자열 필터링 적용 (※ 예로 제시한 것으로, 구현 시 다를 수 있음)

```
$query = sprintf("SELECT id,password,username FROM user_table WHERE_
id='%s';",addslashes($id));
// id 변수를 문자형으로 받고, id 변수의 특수문자를 일반문자로 변환
// @로 php 에러 메시지를 막음
$result = @OCIParse($conn, $query);
if (!@OCIExecute($result))
error("SQL 구문 에러");
exit;
@OCIFetchInto($result,&$rows);
... 중략 ...
```

(예2) eregi\_replace 함수를 이용한 특정 문자열 필터링 적용 (※ 예로 제시한 것으로, 구현 시 다를 수 있음)

```
function SQL_Injection($get_Str) {
return eregi_replace("
(select| union| insert| update| delete| drop|w"|w"|#|w/w*|w*w/|www|w);", "",
$get_Str;
}
```

(예3) php.ini 설정 중 magic\_quotes\_gpc 옵션을 이용하여 특정 문자열 필터링 적용

# GPC(Get, Post, Cookie)를 통해 넘어오는 문자열 중 ', ", \, NULL 값의 앞에 자동으로 백슬래시 문자를 붙여주는 기능을 함 (PHP 6.0 이후 버전 사용 불능)

```
magic_quotes_gpc = on
```

## 웹(Web)

## 2. Dynamic SQL 구문 사용 금지

(예1) Static SQL 구문 사용 (※ 예로 제시한 것으로, 구현 시 다를 수 있음)

```
$sql = 'SELECT ID, PASSWORD, USER_NAME FORM DB WHERE VALUES = ? ';
$stmt = $mysqli->prepare($sql);
$stmt->bind_param('s', '1');
$stmt->execute();
$stmt->bind_result($ID, $PASSWORD, $USER_NAME); // 칼럼수만큼 변수로 지정
while($stmt->fetch()) {
 printf("%s %s\n", $ID, $PASSWORD, $USER_NAME);
}
$stmt->close();
$mysqli->close();
```

(예2) mybatis Data Map 사용 시 쿼리에 삽입되는 Name 파라미터를 #name# 형태로 받아 실행  
(※ 예로 제시한 것으로, 구현 시 다를 수 있음)

```
<?xml version="1.0" encoding="UTF-8"?>
.....
<!-- static SQL 사용 -->
<delete id="delStudent" parameterClass="Student">
DELETE STUDENTS
WHERE NUM = #num# AND Name = '#name#'
</delete>
```

<b>조치 시 영향</b>	일반적으로 영향 없음
----------------	-------------

## 웹(Web)

취약점 항목		1.6. SSI 인젝션					
대상	소스코드	위험도	상	Code	SS		
취약점 개요	SSI(Server-Side Includes) 인젝션은 HTML 문서 내 입력받은 변수값을 서버 측에서 처리할 때 부적절한 명령문이 포함 및 실행되어 서버의 데이터가 유출되는 취약점임. SSI는 CGI 프로그램을 작성하거나 혹은 서버사이드 스크립트를 사용하는 언어로, 웹 서버가 사용자에게 페이지를 제공하기 전에 구문을 해석하도록 지시하는 역할을 함. 공통 SSI 구현은 외부의 파일을 Include 할 수 있는 명령어를 제공하며, 웹 서버의 CGI 환경 변수를 설정하고 출력할 수 있고, 외부의 CGI 스크립트나 시스템 명령어들을 실행할 수 있으므로 사용자 입력값에 대한 검증 로직을 추가로 구현하여야 함.						
보안대책							
판단기준	양호: 사용자 입력값에 대한 검증이 이루어지는 경우						
	취약: 사용자 입력값에 대한 검증이 이루어지지 않는 경우						
조치방법	사용자 입력값에 대한 검증 로직 추가 구현						
보안설정방법							
■ 점검방법							
1. 변수값에 <!--echo var="DOCUMENT_ROOT" -->를 삽입하여 표시 페이지에 사이트의 홈 디렉터리가 표시되는지 확인함							
2. 변수 값에 <!--exec cmd="ls -al" -->를 삽입하여 표시 페이지에 디렉터리의 파일 리스트가 표시되는지 확인함							
■ 보안설정방법							
1. 사용자 입력으로 사용 가능한 문자들을 정해놓음							
2. 정해진 문자들을 제외한 나머지 모든 문자들을 필터링 함							
3. 필터링 해야 하는 대상은 GET 질의 문자열, POST 데이터, 쿠키, URL, 그리고 일반적으로 브라우저와 웹 서버가 주고받는 모든 데이터를 포함하며, 아래는 특수문자에 대한 Entity 형태를 표시한 것임.							
변경 전	<	>	"	(	)	#	&
변경 후	&lt;	&gt;	&quot;	&#40	&#41	&#35	&amp
조치 시 영향	일반적으로 영향 없음						

## 웹(Web)

취약점 항목	1.7. XPath 인젝션					
대상	소스코드		위험도	상	Code	XI
취약점 개요	프로그래머가 의도하지 않았던 문자열을 전달하여 쿼리문의 의미를 왜곡시키거나 그 구조를 변경하고 임의의 쿼리를 실행하여 인가되지 않은 데이터를 열람할 수 있는 취약점으로 적절한 필터링 로직 구현이 필요함.					
보안대책						
판단기준	양호: 쿼리 입력값에 대해 검증이 이루어지는 경우					
	취약: 쿼리 입력값에 대해 검증이 이루어지지 않는 경우					
조치방법	쿼리 입력값에 대해 검증 로직 추가 구현					
보안설정방법						
■ 점검방법   1. ['and'a='a, 'and'a='b], [ and 1=1, and 1=2]의 셋트의 값을 각각 삽입하여 정상 변수 값을 보낸 화면과 [동일화면, 다른화면]의 반응이 있는지 확인   2. 다음 값을 입력해서 에러가 발생하지 않는지 확인   ' or count(parent::*[position()=1])=0 or 'a'='b   ' or count(parent::*[position()=1])&gt;0 or 'a'='b   1 or count(parent::*[position()=1])=0   1 or count(parent::*[position()=1])&gt;0						
■ 보안설정방법   XPath 쿼리에 입력값이 입력되는 경우, 엄격한 입력값 검증을 통해 필요 문자만을 받아들이게 함 ( ) = ' [ ] : , * / 등 XPath 쿼리를 파괴하는 특수문자는 입력하지 못하게 하여야 하며, 특정 특수문자만을 필터링하는 것이 아닌 허용된 문자 이외의 모든 입력을 허용하지 않아야 함						
조치 시 영향	일반적으로 영향 없음					

## 웹(Web)

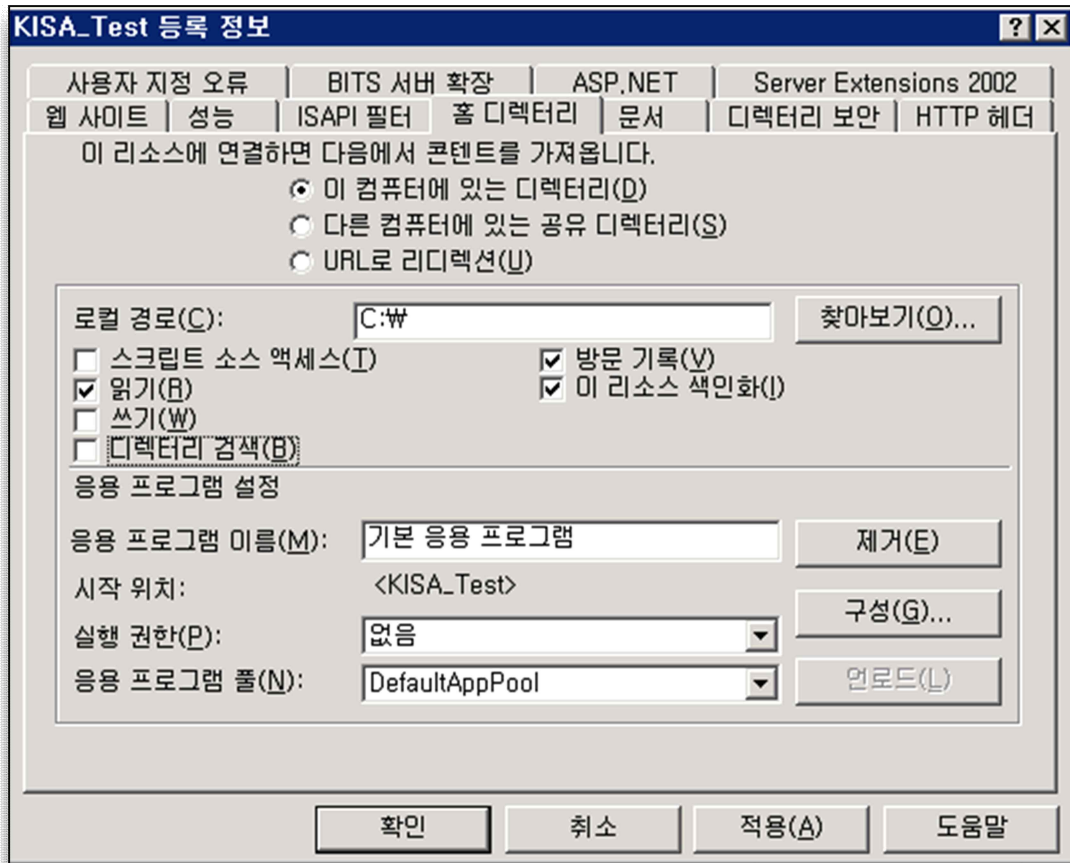
취약점 항목	1.8. 디렉터리 인덱싱				
대상	Web Server	위험도	상	Code	DI
취약점 개요	본 페이지(index.html, home.html, default.asp 등)의 파일이 존재하지 않을 때 자동으로 디렉터리 리스트를 출력하는 취약점으로, 웹 서버 운영 시 특정 디렉터리에 초기화 파일이 없을 경우(index.html, default.html 등...) 해당 디렉터리의 파일 리스트를 브라우저에 보여주게 되며 이는 공격자에게 웹 응용시스템의 구조를 파악할 수 있도록 함. 민감한 정보가 포함된 설정 파일이 노출되면 보안상 심각한 위험을 초래할 수 있으므로 반드시 해당 기능을 중지시켜야 함.				
보안대책					
판단기준	양호: 디렉터리 파일 리스트가 노출되지 않는 경우				
	취약: 디렉터리 파일 리스트가 노출되는 경우				
조치방법	웹 서버 설정을 변경하여 디렉터리 파일 리스트가 노출 되지 않도록 설정				
보안설정방법					
■ 점검방법   1. URL 경로 중 확인 하고자 하는 디렉터리까지만 주소 창에 입력하여 인덱싱 여부를 확인   2. 디렉터리 끝에 %3f.jsp 문자열을 붙여 디렉터리 인덱싱이 되는지 확인   ■ 보안설정방법   웹 서버 환경설정에서 디렉터리 인덱싱 기능 제거   ■ Apache    Httpd.conf 파일 내 DocumentRoot 항목의 Options에서 Indexes 제거  Indexes가 해당 디렉터리의 파일 목록을 보여주는 지시자임  설정 전  &lt;Directory "/var/www/html"&gt;  Options Indexes  &lt;/Directory&gt;  설정 후  &lt;Directory "/var/www/html"&gt;  Options  &lt;/Directory&gt;					

## 웹(Web)

## ■ IIS 7.0

설정> 제어판> 관리도구> “인터넷 서비스 관리자” 선택 후

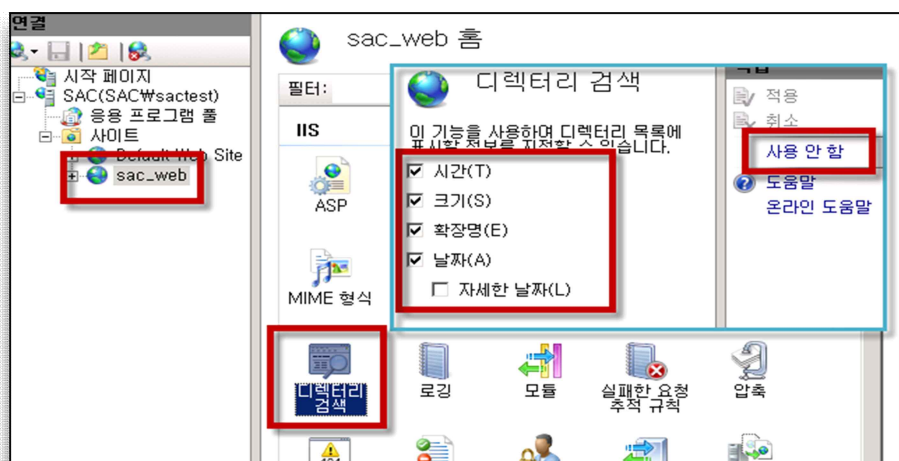
해당 웹 사이트에서 우클릭 후 등록 정보> [홈 디렉터리] 탭> [디렉터리 검색] 체크 해제



## ■ IIS 7.5/8.0

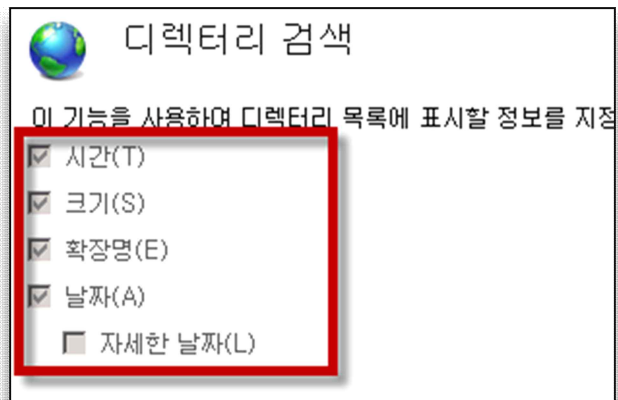
IIS(인터넷 정보 서비스) 관리자> [해당 웹 사이트]> [IIS]> [디렉터리 검색] 선택

우측의 [사용 안 함] 버튼을 눌러 비활성화





## 웹(Web)



## ■ WebtoB 설정

1. \${WEBTOBDIR}/config/http.m 파일 Options 항목에서 index 옵션 삭제 또는, -index 옵션으로 설정 ( default: -index )
2. \${WEBTOBDIR}/config/http.m에서 확인

```
${WEBTOBDIR}/config/http.m

*NODE

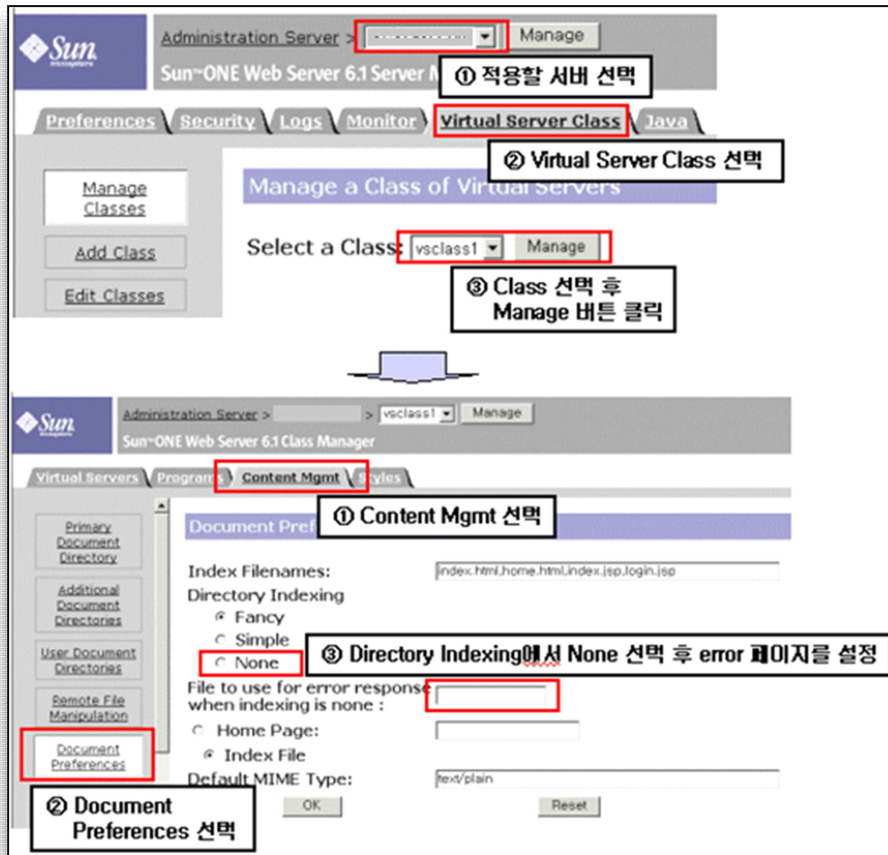
GuideSample WEBTOBDIR="/home/user/webtob",
 SHMKEY = 54000,
 DOCROOT="/home/user/webtob/docs",
 PORT = "8080",
 HTH = 1,
 LOGGING = "log1",
 ERRORLOG = "log2",
 Options = "-index"
```

3. 후 설정파일 컴파일 및 재구동
  - # wscfl -i http.m (http.m 파일 컴파일)
  - # wsdown
  - # wsboot (재구동)

## ■ iPlanet

1. 관리자 콘솔에서 설정 (※ 1 또는, 2번 방법 중 선택 적용)
  - 관리자 콘솔> Server Name> Virtual Server Class> Class Manage> Content Mgmt> Document Preferences> Directory Indexing 항목 "None" 설정

## 웹(Web)



## 2. 설정 파일에서 설정

/[iPlanet Dir]/https-[Server\_name]/config/obj.c

```
<Object name="default">
AuthTrans fn="match-browser" browser="*MSIE*" ssl-unclean-shutdown="true"
NameTrans fn="ntrans-j2ee" name="j2ee"
NameTrans fn="pfx2dir" from="/mc-icons" dir="C:/Sun/WebServer6.1/ns-icons" name="es-internal"
NameTrans fn="document-root" root="$docroot"
PathCheck fn="nt-uri-clean"
PathCheck fn="check-acl" acl="default"
PathCheck fn="find-pathinfo"
PathCheck fn="find-index" index-names="index.html,home.html,index.jsp"
ObjectType fn="type-by-extension"
ObjectType fn="force-type" type="text/plain"
Service method="(GET|HEAD)" type="magnus-internal/imagemap" fn="imagemap"
Service method="(GET|HEAD)" type="magnus-internal/directory" fn="send-error"
path="C:/Sun/WebServer6.1/docs/error/error1.html"
Service method="(GET|HEAD)" type="magnus-internal/directory" fn="send-error"
Service method="TRACE" fn="send-error"
Error fn="error-j2ee"
Error fn="send-error" reason="Unauthorized" path="C:/Sun/WebServer6.1/docs/error/error1.html"
Error fn="send-error" reason="Forbidden" path="C:/Sun/WebServer6.1/docs/error/error1.html"
Error fn="send-error" reason="Not Found" path="C:/Sun/WebServer6.1/docs/error/error1.html"
Error fn="send-error" reason="Server Error" path="C:/Sun/WebServer6.1/docs/error/error1.html"
AddLog fn="flex-log" name="access"
</Object>
```

문구 없거나, send-error로 설정되어 있지 않을 경우 취약  
error page path가 설정되어 있어야 함.

## 웹(Web)

## ■ %3f.jsp 취약점 제거

웹 서버를 Apache로 사용한다면 아래와 같이 설정하여 %3f.jsp 문자를 필터링 해야 하며, Resin 이나 Tomcat 을 사용한다면 최신 버전으로 업그레이드 함

```
<LocationMatch "/(%3f|W?)W.jsp">
AllowOverride None
Deny from all
</LocationMatch>
```

Resin 2.1.x 에서는 최신 버전으로 업그레이드 하거나 아래와 같이 설정 할 수 있음

1. Resin 환경 설정 파일 (resin.conf)에서 가상 디렉터리 설정 부분인 "web-app id"를 찾음
2. 아래 내용 추가

```
<directory-servlet>none</directory-servlet>
```

※ 주의할 점: 모든 가상 디렉터리에 적용 필요

<b>조치 시 영향</b>	일반적으로 영향 없음
----------------	-------------

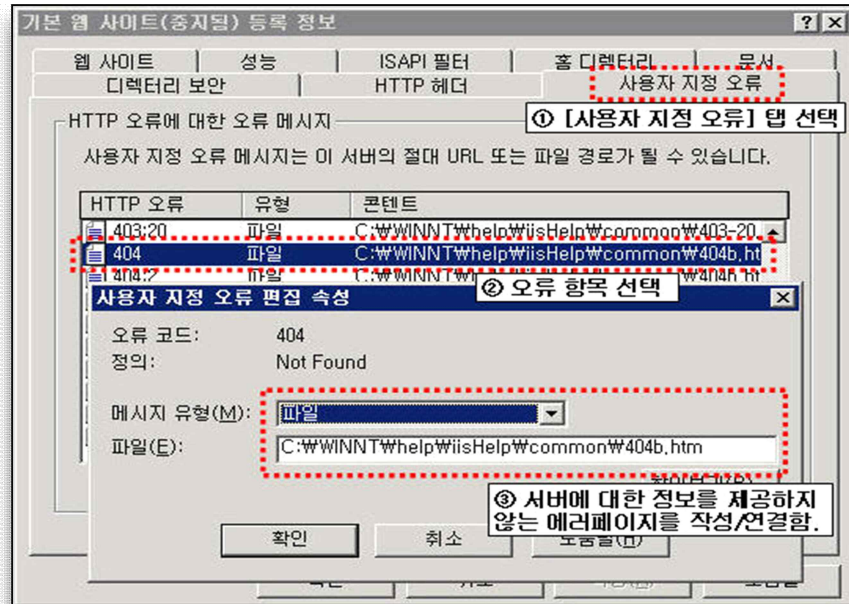
## 웹(Web)

취약점 항목	1.9. 정보 누출				
대상	Web Server	위험도	상	Code	IL
취약점 개요	웹 사이트 데이터가 노출되는 것으로 개발 과정의 코멘트나 오류 메시지 등에서 중요한 정보가 노출되어 공격자에게 2차 공격을 하기 위한 중요한 정보를 제공할 수 있음.				
보안대책					
판단기준	양호: 웹 서비스 에러 페이지가 별도로 지정되어 있는 경우				
	취약: 웹 서비스 에러 페이지가 별도로 지정되지 않아 에러 발생 시 중요 정보가 노출되는 경우				
조치방법	발생 가능한 각 에러에 대한 별도의 웹 서비스 에러 페이지를 지정함				
보안설정방법					
■ 점검방법   1. html 소스 내에 개인정보(화면엔 마스킹처리 되지만 소스에는 그대로 표시), 인증정보, DB접속 정보 등의 중요 정보가 노출되고 있는지 확인   2. 에러 메시지에서 중요 정보(시스템 정보, 절대경로 정보, 컴파일 소스 정보 등)가 노출되는지 확인   ■ 보안설정방법   html 소스 단에 기록되는 정보는 사용자가 웹 브라우저의 소스보기 기능만을 사용해도 간단히 내용을 볼 수 있으므로, html 소스 레벨에서 중요 정보를 코멘트 처리하거나 hidden 등의 값으로 기록하지 말아야 함   일반적으로 웹에서 발생하는 에러 메시지는 400,500번대 의 에러코드를 리턴하게 되는데 이러한 에러 코드에 대해 별도의 에러 페이지로 Redirect하거나 적절한 에러 처리 루틴을 설정하여 처리 되도록 함   ■ Apache    ErrorDocument 500 "Error Message"  ErrorDocument 404 "/your web root/error.html"  ErrorDocument 404 "/your web root/error.html"  ErrorDocument 402 http://xxx.com/error.html    위와 같이 특정 에러코드에 대해 에러 메시지를 출력할 수도 있고 특정 웹 페이지로 Redirect 시킬 수 있으며, 이 설정은 httpd.conf 의 전역 설정에 추가 하거나 원하는 가상 호스트의 &lt;VirtualHost&gt; &lt;/VirtualHost&gt; 사이에 추가하면 됨					

## 웹(Web)

## ■ IIS 5.0, 6.0

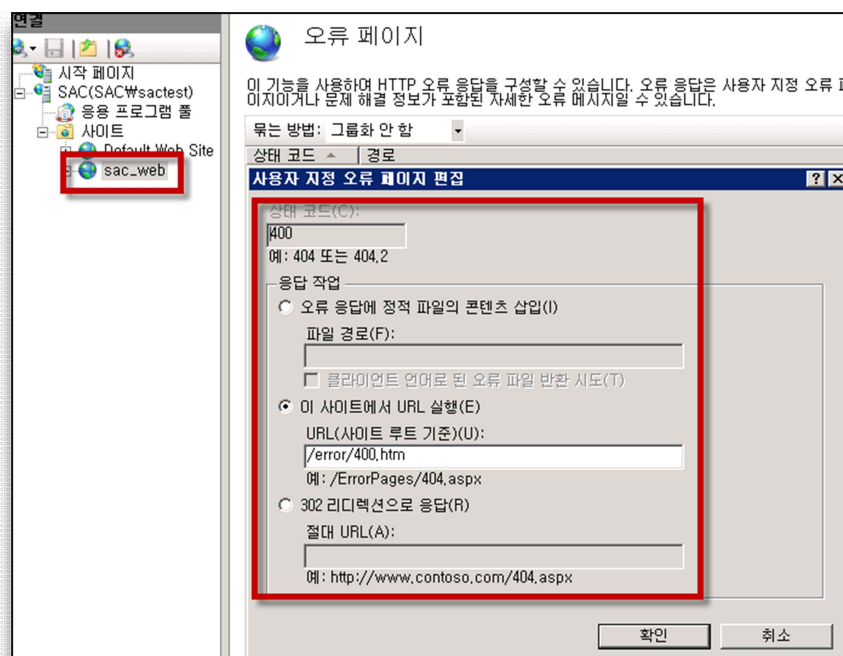
인터넷 정보 서비스(IIS) 관리> 속성> [사용자 지정 오류] 탭에서 400, 401, 403, 404, 500 등 웹 서비스 에러에 대해 별도 페이지 지정



## ■ IIS 7.0 설정

## 1. 에러 메시지 설정

인터넷 정보 서비스(IIS) 관리자> 해당 웹 사이트> [오류 페이지]에서 400, 401, 403, 404, 500 등 웹 서비스 에러에 대해 별도 페이지 지정



## 웹(Web)

## 2. 오류 페이지 설정 편집

인터넷 정보 서비스(IIS) 관리자> 해당 웹 사이트> 오류 페이지> [기능 설정 편집]에서  
 “서버오류 발생 시 다음 반환” 항목을 “사용자 지정 오류 페이지”로 설정

<b>조치 시 영향</b>	일반적으로 영향 없음
----------------	-------------

## 웹(Web)

취약점 항목	1.10. 악성 콘텐츠				
대상	소스코드	위험도	상	Code	CS
취약점 개요	웹 애플리케이션에 정상적인 콘텐츠 대신에 악성콘텐츠를 주입하여 사용자에게 악의적인 영향을 미치는 취약점을 말함.				
보안대책					
판단기준	양호: 악의적 콘텐츠가 실행되지 않는 경우				
	취약: 악의적 콘텐츠가 입력되며, 실행되는 경우				
조치방법	사용자 입력값에 대한 검증 로직 추가 및 실행 제한 설정				
보안설정방법					
■ 점검방법   게시판 등의 페이지에서 강제적으로 이뤄지는 악의적인 프로그램 다운로드나 악의적인 사이트로의 이동이 발생하는지 확인   ■ 보안설정방법   악성콘텐츠가 삽입되어 있는 페이지에 대하여 증적(화면, 소스 등)을 남기고, 삽입된 악성콘텐츠를 삭제하거나 페이지의 삭제 등을 실시함   취득한 증적을 가지고 악성콘텐츠의 삽입 원인에 대하여 분석하여 원인을 제거할 것을 권고함					
조치 시 영향	일반적으로 영향 없음				

## 웹(Web)

취약점 항목	1.11. 크로스사이트 스크립팅								
대상	소스코드	위험도	상	Code	XS				
취약점 개요	사용자가 입력한 내용을 기반으로 페이지를 동적으로 생성하는 웹 애플리케이션 (검색, 게시물 등록 등)을 악용하면, 해당 페이지를 보는 사용자의 웹 브라우저에서 임의의 코드 실행이 가능하게 됨. 로그인 *Session hijacking, 악성 프로그램 설치 등의 Client hacking의 위험성이 존재하므로 사용자 입력값에 대한 검증 로직을 구현하고, 입력문자 필터링이 가능하도록 설정하여야 함.  *Session Hijacking: 이미 인증을 받아 생성된 세션의 연결을 여러 가지 방법으로 가로채는 공격								
보안대책									
판단기준	양호: 사용자 입력값에 대한 검증 및 필터링이 이루어지는 경우 취약: 사용자 입력값에 대한 검증 및 필터링이 이루어지지 않으며, HTML 코드가 입력·실행되는 경우								
조치방법	사용자로부터 입력받는 값에 대해 검증 로직을 추가하고, 게시판에서 HTML을 사용하는 경우 HTML 코드 중 필요한 코드에 대해서만 입력 가능하도록 설정								
보안설정방법									
XSS에 취약한 페이지 유형	1. HTML을 지원하는 게시판 2. Search Page 3. Join Form Page 4. Referrer를 이용하는 Page 5. 그 외 사용자로부터 입력받아 화면에 출력하는 모든 페이지에서 발생 가능								
XSS를 유발할 수 있는 스크립트	<pre>&lt;script&gt; ... &lt;/script&gt; &lt;img src="javascript:....."&gt; &lt;div style="background-image:url(javascript...)"&gt; &lt;/div&gt; &lt;embed&gt;...&lt;/embed&gt; &lt;iframe&gt; &lt;/iframe&gt;</pre>  ※ Filtering을 우회하기 위해 다양한 표현 가능  <table><tr><td>◆ %3Cscript%3E.....%3Cscript%3E</td><td>◆ Jav&amp;#97;script;</td></tr><tr><td>◆ Java&amp;#13;script</td><td>◆ Java&amp;#0013;script</td></tr></table>					◆ %3Cscript%3E.....%3Cscript%3E	◆ Jav&#97;script;	◆ Java&#13;script	◆ Java&#0013;script
◆ %3Cscript%3E.....%3Cscript%3E	◆ Jav&#97;script;								
◆ Java&#13;script	◆ Java&#0013;script								

■ 보안설정방법

1. 게시물에 HTML이나 자바 스크립트에 해당되는 태그 사용을 사전에 제한하고, 사용자가 입력한 값에 대한 필터링 작업 필요

2. 게시물의 본문뿐만 아니라 제목, 댓글, 검색어 입력 창, 그 외 사용자 측에서 넘어오는 값을 신뢰하는 모든 form과 파라미터 값에 대해서 필터링을 수행함



## 웹(Web)

3. 입력값에 대한 필터링 로직 구현 시 공백 문자를 제거하는 trim, replace 함수를 사용하여 반드시 서버 측에서 구현되어야 함

※ 필터링 조치 대상 입력값

- 스크립트 정의어 : <SCRIPT>, <OBJECT>, <APPLET>, <EMBED>, <FORM>, <IFRAME> 등
- 특수문자 : <, >, ", ', &, %, %00(null) 등

#### ■ ASP

```
<%
... 중략 ...
If use_HTML Then
 content = Server.HTMLEncode(content)
... 중략 ...

Sub ReplaceStr(content, byref str)
 content = replace(content, "'", " ")
 content = replace(content, "&", "&")
 content = replace(content, " ", """)
 content = replace(content, "<", "<")
 content = replace(content, ">", ">")

 str = content
End Sub

... 중략 ...
%>
```

#### ■ PHP

```
... 중략 ...
if($use_html == 1) // HTML tag를 사용하게 할 경우 부분 허용
 $memo = str_replace("<", "<", $memo); // HTML TAG 모두 제거
 $tag = explode(",", $use_tag);

 for($i=0; $i<count($tag); $i++) { // 허용할 TAG만 사용 가능하게 변경
 $memo = eregi_replace("<".$tag[$i].", "<".$tag[$i].", ", $memo);
 $memo = eregi_replace("<".$tag[$i].">", "<".$tag[$i].">", $memo);
 $memo = eregi_replace("</".$tag[$i], "</".$tag[$i], $memo); }
 else // HTML tag를 사용하지 못하게 할 경우
 $memo = str_replace("<", "<", $memo);
```

## 웹(Web)

```
$memo = str_replace(">", ">", $memo);
... 중략 ...
```

## ■ JSP

```
<%
... 중략 ...
tring subject = request.getParameter("subject_BOX");
 subject = subject.replaceAll("<", "<");
 subject = subject.replaceAll(">", ">");
 ... 중략 ...
%>
```

## ※ 참고: 필터링 대상

<	>	&lt;	&gt;	innerHTML
javascript	eval	onmousewheel	onactive	onfocusout
expression	charset	ondataavailable	oncut	onkeyup
applet	document	onafteripupdate	onclick	onkeypress
meta	string	onmousedown	onchange	onload
xml	create	onbeforeactivate	onbeforecut	onbounce
blink	append	onbeforecopy	ondbclick	onmouseenter
link	binding	onbeforedeactivate	ondeactivate	onmouseout
style	alert	ondatasetchaged	ondrag	onmouseover
script	msgbox	cnbeforeprint	ondragend	onsubmit
embed	refresh	cnbeforepaste	ondragenter	onmouseend
object	void	onbeforeeditfocus	ondragleave	onresizestart
iframe	cookie	onbeforeunload	ondragover	onunload
frame	Href	onbeforeupdate	ondragstart	onselectstart
frameset	onpaste	onpropertychange	ondrop	onreset
ilayer	onresize	ondatasetcomplete	onerror	onmove
layer	onselect	oncellchange	onfinish	onstop
bgsound	base	onlayoutcomplete	onfocus	onrowexit
title	onblur	onselectionchange	vbscript	onerrorupdate
onbefore	onstart	onrowsinserted	onkeydown	onfilterchage
onmouseup	onfocusin	oncontrolselected	onrowsdelete	onlosecapture
onrowenter	onhelp	onreadystatechange	onmouseleave	onmousemove
oncontextmenu				

조치 시 영향      일반적으로 영향 없음

## 웹(Web)

취약점 항목		1.12. 약한 문자열 강도			
대상	소스코드	위험도	상	Code	BF
취약점 개요	계정이나 패스워드, 암호화 키 등을 유추하기 위해 반복적으로 값을 입력하여 해당 값을 발견해 내는 취약점으로, 유추가 용이한 계정 및 패스워드의 사용을 방지하기 위해 해당 값의 적절성 및 복잡성을 검증하는 체크 로직을 구현하여야 함.				
보안대책					
판단기준	양호: 관리자 계정이 유추하기 어려운 계정으로 설정되어 있는 경우				
	취약: 관리자 계정이 유추하기 쉽게 설정되어 있는 경우				
조치방법	계정 및 비밀번호의 체크 로직 추가 구현				
보안설정방법					
■ 점검방법   1. 인증값에 단순 조합의 값을 삽입하여 정상적인 인증을 취득하는지 확인   • 취약한 계정: admin, administrator, manager, guest, test, scott, tomcat, root, user, operator, anonymous 등   • 취약한 패스워드: Abcd, aaaa, 1234, 1111, test, password, public, blank 패스워드, ID와 동일한 패스워드 등   ■ 보안설정방법   취약한 계정 및 패스워드를 삭제하고, 사용자가 취약한 계정이나 패스워드를 등록하지 못하도록 패스워드 규정이 반영된 체크 로직을 구현하여야 함    1. 다음 각 목의 문자 종류 중 2종류 이상을 조합하여 최소 10자리 이상 또는 3종류 이상을 조합하여 최소 8자리 이상의 길이로 구성  (1) 영문 대문자(26개)  (2) 영문 소문자(26개)  (3) 숫자(10개)  (4) 특수문자(32개)  2. 연속적인 숫자나 생일, 전화번호 등 추측하기 쉬운 개인정보 및 아이디와 비슷한 비밀번호는 사용하지 않는 것을 권고  3. 비밀번호에 유효기간을 설정하여 반기별 1회 이상 변경					
조치 시 영향	일반적으로 영향 없음				

## 웹(Web)

취약점 항목	1.13. 불충분한 인증				
대상	소스코드	위험도	상	Code	IA
취약점 개요	민감한 데이터에 접근 가능한 경로에 대한 인증 절차가 불충분할 경우 발생하는 취약점으로 사용자가 권한 외의 페이지에 접근하여 정보를 유출하거나 변조할 수 있으므로 추가적인 인증 절차를 구현하여야 함.				
보안대책					
판단기준	양호: 중요 정보 페이지 접근 시 추가 인증을 하는 경우				
	취약: 중요 정보 페이지 접근에 대한 추가 인증을 하지 않는 경우				
조치방법	중요 정보 페이지에 대한 추가 인증 로직 추가 구현				
보안설정방법					
■ 점검방법   1. 개인정보 수정 및 패스워드 수정 기능 페이지 접근 전에 본인인증에 대한 재인증 여부 확인   2. 인증 후 페이지에 아이디만을 인증값으로 하여 변수로 관리 되고 있는지 확인   ■ 보안설정방법   1. 개인정보 및 패스워드 수정 페이지와 같은 중요 정보를 표시하는 페이지에서는 본인 인증을 재확인하는 로직을 구현하고, 인증 후 사용자가 이용 가능 페이지에 접근할 때마다 승인을 얻은 사용자인지 페이지마다 검증하여야 함   2. 접근 통제 정책을 구현하고 있는 코드는 구조화, 모듈화가 되어 있어야 함   3. 접근제어가 필요한 모든 페이지에 통제수단(로그인 체크 및 권한 체크)을 구현해야 하며 특히, 하나의 프로세스가 여러 개의 페이지 또는 모듈로 이루어져 있을 때 권한 체크가 누락되는 경우를 방지하기 위해서 공통 모듈을 사용하는 것을 권장함   4. 인증 과정을 처리하는 부분에 Client Side Script(Javascript, VBScript 등)를 사용하면 사용자가 임의로 수정할 수 있으므로 Server Side Script(PHP, ASP, JSP 등)를 통하여 인증 및 필터링 과정을 수행함					
조치 시 영향	일반적으로 영향 없음				

## 웹(Web)

취약점 항목	1.14. 취약한 비밀번호 복구				
대상	소스코드	위험도	상	Code	PR
취약점 개요	취약한 비밀번호 복구 로직(비밀번호 찾기 등)으로 인하여 공격자가 불법적으로 다른 사용자의 비밀번호를 획득, 변경할 수 있는 취약점으로 비밀번호 복구 로직은 유추하기 어렵게 구현되어야 함.				
보안대책					
판단기준	양호: 비밀번호 재발행 시 난수를 이용하여 재발행 되는 경우				
	취약: 비밀번호 재발행 시 일정 패턴으로 재발행 되는 경우				
조치방법	비밀번호 복구 로직 변경				
보안설정방법					
■ 점검방법   1. 재발행 되는 비밀번호 몇 개를 획득함   2. 비밀번호 재발행 기능에서 사용자의 연락처, 주소, 메일 주소, 일정 패턴을 비밀번호로 이용하고 있는지 확인함					
■ 보안설정방법   사용자의 개인정보(연락처, 주소, 메일 주소 등)로 비밀번호를 생성하지 말아야 하며, 난수를 이용한 불규칙적이고 최소 길이(6자 이상 권고) 이상의 패턴이 없는 비밀번호를 발급하여야 함					
조치 시 영향	일반적으로 영향 없음				

## 웹(Web)

취약점 항목		1.15. 크로스사이트 리퀘스트 변조(CSRF)			
대상	소스코드	위험도	상	Code	CF
취약점 개요	CSRF(Cross Site Request Forgery) 공격은 세션 쿠키, SSL 인증서, 윈도우 도메인 인증과 같이 자동으로 입력된 신뢰(인증) 정보를 기반으로 하는 웹 애플리케이션에서 발생하는 취약점임. 사용자의 신뢰(인증) 정보 내에서 사용자의 요청(Request)을 변조함으로써 해당 사용자의 권한으로 악의적인 공격을 수행할 수 있는 취약점으로 XSS 취약점과 마찬가지로 사용자 입력값에 대한 적절한 필터링 및 인증에 대한 유효성 검증을 통해 방지가 가능함.				
보안대책					
판단기준	양호: 사용자 입력값에 대한 검증 및 필터링이 이루어지는 경우				
	취약: 사용자 입력값에 대한 필터링이 이루어지지 않으며, HTML 코드를 입력하여 실행되는 경우				
조치방법	사용자 입력값에 대해 검증 로직 및 필터링 추가 적용				
보안설정방법					
■ 점검방법					
1. 등록 및 변경 등의 데이터 수정 기능의 페이지가 있는지 조사함					
2. 데이터 수정 페이지에서 전송되는 요청(Request)을 취득 후에 재송하여 정상적인 데이터 수정 기능이 재수행 되는지 점검함					
■ 보안설정방법					
1. 사용자가 입력하는 값에 대한 검증 로직 구현					
2. 정상적인 리퀘스트와 비정상적인 리퀘스트를 구분할 수 있도록 Form/URL 에서 임의의 토큰을 추가하고 이 토큰을 검증하도록 설계					
3. HTML 이나 자바스크립트에 해당되는 태그 사용을 사전에 제한하고, 서버 단에서 사용자 입력값에 대한 필터링 구현					
4. HTML Editor 사용으로 인한 상기사항 조치 불가 시, 서버 사이드/서블릿/DAO(Data Access Object) 영역에서 조치하도록 설계					
5. XSS 조치 방안 참조					
조치 시 영향	일반적으로 영향 없음				

## 웹(Web)

취약점 항목		1.16. 세션 예측			
대상	소스코드	위험도	상	Code	SE
취약점 개요	단순한 방법(연속된 숫자 할당 등)으로 생성되는 세션의 ID를 예측하여 세션을 가로채는 취약점으로, 사용자에게 전달하는 세션 ID가 일정한 패턴을 가지고 있는 경우 공격자는 세션 ID를 추측하여 불법적인 연결을 생성할 수 있음. 또한 추측 과정의 자동화를 통하여 비교적 짧은 시간 안에 유효한 세션 ID를 얻는 것이 가능하므로 세션 ID를 추측 불가능하도록 난수로 생성하여야 함.				
보안대책					
판단기준	양호: 추측 불가능한 세션 ID가 발급되는 경우				
	취약: 세션 ID가 일정한 패턴으로 발급되는 경우				
조치방법	추측 불가능한 세션 ID가 발급되도록 로직 구현				
보안설정방법					
■ 점검방법   1. 각기 다른 IP 주소와 다른 사용자명, 시간적 차이로 세션 ID를 발급받음   2. 발급받은 세션 ID에 일정한 패턴이 있는지 조사   3. 일정한 패턴이 확인되고, 패턴의 의해 사용 가능한 세션 ID의 예측이 가능한지 확인   ■ 보안설정방법   아무리 길이가 길고 복잡한 항목으로 세션 ID가 만들어져도 공격자가 충분한 시간과 자원이 있다면 뚫는 것은 불가능하지 않으므로 강력한 세션 ID를 생성하여야 함   주된 목적은 수많은 대역폭과 처리 자원을 가지고 있는 공격자가 하나의 유효한 세션 ID를 추측하는데 최대한 오랜 시간이 걸리게 하여 쉽게 추측하지 못하게 하는 것에 있음   단순 조합 보다는 상용 웹 서버나 웹 애플리케이션 플랫폼에서 제공하는 세션 ID를 사용하고, 가능하다면 맞춤형 세션 관리 매커니즘을 권고함   세션 ID는 로그인 시마다 추측할 수 없는 새로운 세션 ID로 발급하여야 함					
조치 시 영향	일반적으로 영향 없음				

## 웹(Web)

취약점 항목	1.17. 불충분한 인가				
대상	소스코드	위험도	상	Code	IN
취약점 개요	민감한 데이터 또는, 기능에 대한 접근 또는 사용 제한이 없는 경우 발생하는 취약점으로 접근 권한에 대한 검증 로직이 구현되지 않아 다른 사용자의 민감한 정보나 인증이 필요한 페이지에 임의로 접근할 수 있게 됨. 따라서 중요 정보 페이지 접근, 수정에 대한 추가 인증 절차가 필요함.				
보안대책					
판단기준	양호: 중요 정보 페이지 접근 시 추가 인증을 하는 경우				
	취약: 중요 정보 페이지의 파라미터 변경으로 타인의 정보를 열람, 수정이 가능한 경우				
조치방법	중요 정보 페이지의 추가 인증 로직 구현				
보안설정방법					
■ 점검방법   1. 개인정보 수정 및 패스워드 수정 기능의 페이지에서 다른 사용자와의 구분을 ID, 일련번호 등의 단순한 값을 사용하는지 조사   2. 다른 사용자와 구분하는 값을 변경하는 것만으로 다른 사용자의 개인정보, 패스워드에 접근이 가능한지 확인   ■ 보안설정방법   1. 민감한 중요 데이터에 대한 접근 페이지에서 인증을 위한 로직이 구현되지 않았다면, 세션을 통한 인증 및 사용자에게 확인을 위한 인증값 입력을 통한 인증 절차의 로직을 구현하여야 함   2. 페이지별 권한 매트릭스를 작성하여, 페이지에 부여된 권한의 타당성을 체크 후에 권한 매트릭스를 기준으로 하여 전 페이지에서 권한 체크가 이뤄지도록 구현하여야 함					
조치 시 영향	일반적으로 영향 없음				



## 웹(Web)

취약점 항목		1.18. 불충분한 세션 만료			
대상	소스코드, Web Server	위험도	상	Code	SC
취약점 개요	세션의 만료 기간을 정하지 않거나, 만료기한을 너무 길게 설정하여 공격자가 만료되지 않은 세션을 활용할 수 있게 되는 취약점으로, 세션 만료는 사용자 인증 후 웹 사이트 내에서 이벤트 없이 일정 시간이 경과하면, 임의로 세션을 종료시켜 서비스 접근을 제한하는 기능으로, 특히 공개된 장소에서 사용자가 오랜 시간 자리를 비우는 경우 타 사용자에게 의한 침해를 방지하기 위해서 필요함.				
보안대책					
판단기준	양호: 세션 종료 시간이 설정되어 있는 경우				
	취약: 세션 종료 시간이 설정되어 있지 않아 세션 재사용이 가능한 경우				
조치방법	세션 종료 시간 설정 또는 자동 로그아웃 기능 구현				
보안설정방법					
■ 점검방법   1. 인증 후 정상적으로 세션이 발행된 페이지의 리퀘스트를 취득하여 일정 시간(10분 이상)이 지난 후에 재전송 시 정상 처리가 되는지 확인   ■ 보안설정방법   1. 세션 타임아웃 기능이 구현되어 있지 않을 경우 장시간 부재중인 사용자에게 대한 보호 장치가 없는 것이며, 세션 타임아웃 구현 시 타임아웃 시간은 10분으로 설정할 것을 권고함   ■ ASP   접속자 별로 세션을 생성하여 사용자 정보를 각각 저장할 수 있는 *세션 오브젝트를 사용하여 타임아웃 기능을 구현함   *세션 오브젝트: 페이지 접근을 허가하거나 금지할 때 또는, 사용자 별로 정보를 저장할 때 많이 사용하며 접속자의 브라우저에서 쿠키 기능을 지원해야 세션 오브젝트 사용이 가능함   다음과 같은 설정이 적용될 경우 사용자가 로그아웃할 경우 세션은 바로 삭제되며 로그아웃하지 않고 10분 동안 웹 서버로의 요청이 없을 경우 세션은 없어지게 됨    ... 중략 ...  // Session의 유지 시간 Setting  Session.timeout = 10  ... 중략 ...					

## 웹(Web)

구분		설 명
Property	SessionID	사용자마다 갖게 되는 고유한 세션값
	Timeout	세션이 유지되는 기간
Method	Abandon	강제로 세션을 소멸시키는 함수
Event	Onstart	각각의 사용자가 처음 방문할 때 발생
	Onend	사용자의 세션이 끝나는 시점에 발생

## ■ JSP

세션 타임아웃 기능을 구현하는 방법은 session.getLastAccessedTime()를 이용하여 세션의 마지막 접근 시간으로부터 일정 시간 이내에 다시 세션에 접근하지 않은 경우 자동으로 세션을 종료하도록 함

세션의 타임아웃은 두 가지 방법으로 설정할 수 있음

1. web.xml 파일에서 <session-config> 태그를 사용하여 타임아웃을 지정하는 방법  
web.xml, Weblogic.xml 중 한 곳에만 설정  
(만약, 두 곳 모두 설정 시 우선순위에 의해 web.xml의 설정이 적용됨)

Web.xml : "분" 단위

```
<session-config>
 <session-timeout>10</session-timeout>
</session-config>
```

Weblogic.xml: "초" 단위

```
<session-descriptor>
 <timeout-secs>600</timeout-secs>
</session-descriptor>
또는,
<session-param>
 <param-name>TimeoutSecs</param-name>
 <param-value>600</param-value>
</session-param>
```

## 웹(Web)

## 2. 세션 기본 객체가 제공하는 setMaxInactiveInterval() 메소드 사용

※ 주의할 점: web.xml에서는 타임아웃 시간단위가 분이지만 메소드에서는 초단위임

```

... 중략 ...
// Session의 유지 시간을 Setting
String strTime = Param.getPropertyFromXML("SessionPersistenceTime");
if (strTime == null) {
 session.setMaxInactiveInterval(600);
} else {
 session.setMaxInactiveInterval((new Integer(strTime)).intValue());
}
... 중략 ...

```

## 조치 시 영향

일반적으로 영향 없음

## 웹(Web)

취약점 항목	1.19. 세션 고정				
대상	소스코드	위험도	상	Code	SE
취약점 개요	사용자 로그인 시 항상 일정하게 고정된 세션 ID 값을 사용하는 취약점으로 로그인 시 세션마다 새로운 세션 ID가 발행되지 않는다면 세션 ID를 도용한 비인가자의 접근 및 권한 우회가 가능하므로 세션 ID의 타임아웃 기능을 설정하고 세션 ID의 고정 사용을 방지하도록 설정함.				
보안대책					
판단기준	양호: 로그인별 세션 ID가 발행되는 경우				
	취약: 로그인 세션 ID가 고정 사용되는 경우				
조치방법	로그인별 세션 ID 생성 로직 구현				
보안설정방법					
■ 점검방법   1. 로그인 기능에서 세션 ID가 발행되는지 확인   2. 로그인 전에 URL 및 파라미터에 세션 ID와 값을 삽입하여 세션으로 사용되는지 확인   ■ 보안설정방법   인증 기능에서 사용자가 인증을 받은 후에 새로운 세션 ID를 할당 받도록 발행함					
조치 시 영향	일반적으로 영향 없음				

## 웹(Web)

취약점 항목		1.20. 자동화 공격			
대상	소스코드	위험도	상	Code	AU
취약점 개요	웹 애플리케이션에 자동화된 공격을 수행하여 많은 수의 프로세스를 실행 시키는 취약점으로, 자동화 공격을 방지하면, 자동 로봇 또는 공격자가 반복적으로 웹 사이트 기능을 사용해서 시스템을 악용할 수 있음. 데이터 등록 또는, 메일 발송 기능 등 웹 애플리케이션에 구현된 기능의 적절성에 대한 검증 로직이 필요함.				
보안대책					
판단기준	양호: 웹 애플리케이션의 데이터 등록 등의 기능 사용 시 대량 사용에 대한 통제가 이루어지는 경우				
	취약: 웹 애플리케이션의 데이터 등록 등 기능 사용 시 통제가 이루어지지 않는 경우				
조치방법	데이터 등록, 메일 발송 등 웹 애플리케이션 기능에 대한 대량 사용 통제 로직 구현				
보안설정방법					
■ 점검방법   1. 데이터 등록 및 메일 발송의 기능에서 반복적인 기능을 이용하여 대량의 데이터 등록이나 메일 발송이 가능한지 확인   ■ 보안설정방법   1. 데이터 등록 및 메일 발송의 기능에서 사용자의 등록이 일회성이 될 수 있도록, 이미지를 이용하여 확인값을 표시하고 사용자가 값을 등록하여 인증하는 등 일회성 확인 로직을 구현하여야 함   2. 자동화 공격을 시도하면 짧은 시간에 다량의 패킷(양)이 전송되므로 이를 공격으로 감지하고 방어할 수 있는 IDS/IPS의 시스템을 구축하여야 함   3. 서버에 요청되는 패킷(양)을 모니터링 할 수 있는 시스템 구축이 없이는 적시 적절한 방어가 어려움					
조치 시 영향	일반적으로 영향 없음				

## 웹(Web)

취약점 항목		1.21. 프로세스 검증 누락			
대상	소스코드	위험도	상	Code	PV
취약점 개요	접근 제어가 미흡할 경우 URL 강제입력, 스크립트 조작 등의 방법으로 페이지에 대한 접근이 가능하므로, 인증이 필요한 모든 페이지에 대해 유효 세션임을 확인하는 프로세스 및 주요 정보 페이지에 접근 요청자의 권한 검증 로직을 적용하여야 함. 유효 세션의 검증 및 페이지에 대한 접근 권한은 스트립트에 의존하지 말아야 하며 Server Side Script로 구현된 프로세스를 사용해야 함.				
보안대책					
판단기준	양호: URL강제 입력으로 비인가 페이지 접근이 불가능 한 경우				
	취약: URL강제 입력으로 비인가 페이지 접근이 가능한 경우				
조치방법	페이지별 권한 체크 로직 구현				
보안설정방법					
■ 점검방법					
1. 업무프로세스 파악					
2. 권한의 종류 및 범위 파악					
3. 페이지의 모든 기능을 수집하여 프로세스 상에 통제된 페이지에 접근이 가능한지 확인					
■ 보안설정방법					
1. 우회될 수 있는 플로우를 차단하여야 하며, 페이지별 권한 매트릭스를 작성하여 페이지에 부여된 권한의 타당성을 체크한 후에 권한 매트릭스를 기준으로 전 페이지에서 권한 체크가 이뤄지도록 구현하여야 함					
2. 인증이 필요한 모든 페이지에 대해 유효 세션임을 확인하는 프로세스 및 주요 정보 페이지에 접근 요청자의 권한 검증 로직을 적용함					
3. 유효 세션의 검증 및 페이지에 대한 접근 권한은 스트립트에 의존하지 말아야 하며, Server Side Script로 구현된 프로세스를 사용					
■ ASP					
(예시) 인증이 필요한 페이지 소스 코드					
<pre>&lt;% - 인증 성공 시 세션값 세팅 Session("sessionChk") = True Session("UserID") = userID Session("UserGrp") = userGrp Session("UserIP") = Request.Servervariables("REMOTE_ADDR") ... 중략 ... - 사용자 그룹 리턴 함수 ... 중략 ... Function GetUserGroup(strUserID)</pre>					

## 웹(Web)

```

End function ... 중략 ...
- 페이지에 접근 가능한 UserGroup 설정값이 '100' 가정 시
ChkUserGrp = GetUserGroup(userID)
//세션 userID값을 통해 DB에 저장된 사용자 그룹 리턴 ... 중략 ...
If Session_Check and Session("UserGrp") = ChkUserGrp Then
 If Session("UserGrp") <> 100 Then
 Response.Write("권한이 없습니다.")
 Response.End
 End
Else
 Response.Redirect "Login.asp"
 Response.End
End if
... 중략 ... %>

```

## ■ JSP

(예시) 인증이 필요한 페이지 소스 코드

```

<%
... 중략 ...
PortalSessionManager sessionMgr = (PortalSessionManager)
session.getAttribute("sessionMgr");
if (sessionMgr == null || sessionMgr.getUserId() == null) {
 (new FailToAuthenticateCmd()).execute(request,response);
}
... 중략 ...
String usrGrp = session.getAttribute("Usrgrp") == null ?
"" : (String)session.getAttribute("Usrgrp");
if (!usrGrp.equals("") || !userGrp.equals(Code.getMarket())) {
 // 접근 권한을 인가할 수 없음.
 (new FailToPermissionCmd()).execute(request,response); }
중략 ...
%>

```

조치 시 영향

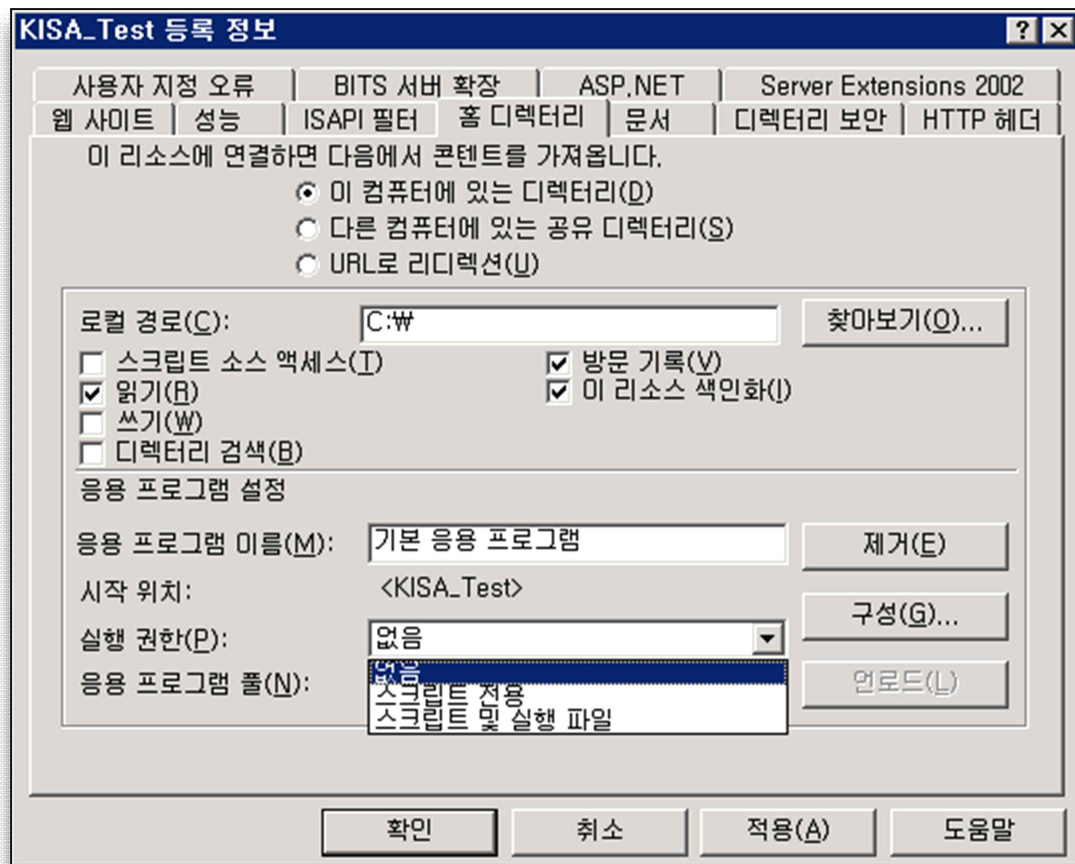
일반적으로 영향 없음

## 웹(Web)

취약점 항목		1.22. 파일 업로드			
대상	소스코드, Web Server	위험도	상	Code	FU
취약점 개요	파일 업로드 기능을 이용하여 시스템 명령어를 실행할 수 있는 웹 프로그램을 업로드 할 수 있는 취약점으로, 만일 업로드 되는 파일의 확장자에 대한 적절성 여부를 검증하는 로직이 존재하지 않는다면 공격자가 조작한 Server Side Script 파일을 업로드하고, 서버상에 저장된 경로를 유추하여 해당 Server Side Script 파일을 실행, 셸을 획득할 수 있음. 셸 권한 획득 후, 시스템 명령어를 홈페이지를 통해 실행하고 웹 브라우저를 통해 그 결과값을 보며 시스템 관리자 권한 획득 또는 인접 서버에 대한 침입을 시도 할 수 있으므로, 업로드 되는 파일에 대한 검증 및 업로드 폴더에 대한 접근 통제가 필요함.				
	보안대책				
판단기준	양호: 업로드 되는 파일에 대한 통제가 이루어지는 경우				
	취약: 업로드 되는 파일에 대한 통제가 이루어지지 않는 경우				
조치방법	업로드 되는 파일에 대한 통제 및 서버 설정 변경				
보안설정방법					
■ 점검방법					
1. 사용자 게시판에 파일 첨부 기능이 있는지 조사함					
2. 첨부 기능이 존재하는 경우, 확장자가 jsp, php, asp, cgi 등 Server Side Script 프로그램 업로드가 가능한지 조사함					
※ 클라이언트 프로그램에서 JavaScript, VBScript 등의 스크립트로 파일첨부를 차단하는 경우 차단 기능을 수정하여 파일을 첨부함					
3. 홈페이지에 있는 디렉터리 정보를 이용하여 첨부한 Server Side Script 프로그램의 위치를 조사한 후 브라우저 주소 창에서 해당 프로그램의 실행이 가능한지 확인					
■ 보안설정방법					
※ 사용자가 파일을 업로드 할 수 있는 모든 모듈에 적용 필요					
1. 업로드 파일을 위한 디렉터리에는 실행 설정을 제거함(웹 서버 보안 설정)					
2. 업로드 파일을 위한 전용 디렉터리를 별도로 생성하여 httpd.conf와 같은 웹 서버 데몬 설정파일에서 실행 설정을 제거함으로써, Server Side Script가 업로드 되더라도 웹 엔진이 실행하지 않는 환경을 설정함					
■ IIS					
설정> 제어판> 관리도구> 인터넷 서비스(IIS) 관리자 선택					
해당 업로드 폴더에서 우클릭> 등록 정보> 디렉터리> 실행 권한 "없음" 설정					



## 웹(Web)



## ■ Apache

Apache 설정 파일인 httpd.conf에 해당 디렉터리에 대한 문서 타입을 컨트롤하기 위해 Directory 섹션의 AllowOverride 지시자에서 FileInfo 또는, "All" 추가

```
<Directory "/usr/local/apache">AllowOverride FileInfo (또는, All)....
...
</Directory>
```

파일 업로드 디렉터리에 .htaccess 파일을 만들고 다음과 같이 AddType 지시자를 이용, 현재 서버에서 운영되는 Server Side Script 확장자를 text/html로 MIME Type을 재조정하여 업로드 된 Server Side Script가 실행되지 않도록 설정

또는, FileMatch 지시자를 이용하여 \*.ph, \*.inc, \*.lib 등의 Server Side Script 파일에 대해서 직접 URL 호출을 금지시킴

```
<.htaccess> <FilesMatch "%.ph|.inc|.lib">

Order allow, deny
```

## 웹(Web)

```
Deny from all
```

```
</FilesMatch>
```

```
AddType text/html .html .htm .php .php3 .php4 .phtml .phps .in .cgi .pl .shtml
.jsp
```

## ※ 주의할 점

- Apache 서버의 경우 AllowOverride 지시자 변경 시 Apache Restart 필요
  - 파일 업로드 되는 디렉터리 운영에 필요한 Server Side Script가 존재하는지 확인
  - 파일 다운로드 프로그램이 아닌 직접 URL 호출을 통해 파일을 다운받는 경우 FileMatch 지시자를 사용하면 차단 설정한 확장자의 파일 다운로드가 거부됨
1. 첨부 파일 확장자 필터링 처리로 사용자가 첨부 파일의 업로드 시도 시, 업로드 파일의 확장자를 검토하여 적절한 파일인지 검사하는 루틴을 삽입하여, 적합한 파일의 확장자 이외의 파일에 대해서 업로드가 불가능하도록 하며, 이런 필터링 규칙은 서버에서 구현하여야 함
  2. 시스템 보안설정 시 웹 서버 구동은 반드시 관리자 권한이 아닌 일반 사용자 권한으로 구동함
  3. 외부사용자가 첨부 파일을 이용하여 권한을 획득할지라도 최소한의 권한만을 사용할 수 있도록 함
  4. 업로드 된 디렉터리에서 실행 권한을 제거하는 방법은 임시적이기는 하지만 소스코드의 수정 없이 간단히 수행될 수 있음

## ■ ASP

1. 수용 가능한 파일의 확장자만 업로드 허용(Positive 방식)
  - 이미지 파일의 경우 (JPG, GIF, BMP 등)
  - 문서 파일의 경우 (XLS, PDF, PPT, DOC 등)

(예) doc, hwp, pdf, jpg 파일만 업로드 허용 (※ 예로 제시하는 것으로, 구현 시 다를 수 있음)  
확장자 검증 시 대소문자 구분 없이 문자열 비교

```
....
```

```
FunctionIsAllowExtension(originFilename,mAllowExtension)
Dim ReturnValue, eregObj, matches, PatternStr, FileNameExt
FileNameExt = Mid(originFilename, InStrRev(originFilename, ".") +1)
ReturnValue = False
```

## 웹(Web)

```

if IsNull(mAllowExtention) Then
 IsAllowExtension = True
 Exit Function
End if

PatternStr = "^(" & Replace(mAllowExtention, ",", "|") & ")$"
Set eregObj = New RegExp
With eregObj
 .IgnoreCase = True
 .Global = True
 .Pattern = PatternStr
 ReturnValue = .test(FileNameExt)
End with
Set eregObj = Nothing

IsAllowExtension = ReturnValue
End Function

.....
If Not IsAllowExtension("파일명.txt", "doc,hwp,pdf,jpg") Then
 response.write "허용되지 않은 확장자 입니다."
End if

```

## 2. MIME TYPE 확인을 통한 실행 파일 업로드 차단

(예) MIME TYPE을 통한 악성 파일 업로드 차단

```

if UploadForm("UPFILE").MimeType<> "image" then
 Response.write "Permit only Image files"
 Response.end
end if

```

## 3. 파일 확장자에 특수문자가 포함되지 않도록 검증하는 로직 구현

## 4. 파일 검증 시 대소문자 구분 없이 문자열 비교

## ■ ASP.net

## 1. 수용 가능한 파일의 확장자만 업로드 허용(Positive 방식)

- 이미지 파일의 경우 (JPG, GIF, BMP 등)
- 문서 파일의 경우 (XLS, PDF, PPT, DOC 등)

## 웹(Web)

(예) doc, hwp, pdf, jpg 파일만 업로드 허용 (※ 예로 제시하는 것으로, 구현 시 다를 수 있음)  
확장자 검증 시 대소문자 구분 없이 문자열 비교

```
string upload_Image(FileUpload fileupload, string ImageSavedPath)
{
 FileUpload fu = fileupload;
 string imagepath = "";
 if (fileupload.HasFile)
 {
 string filepath = Server.MapPath(ImageSavedPath);
 String fileExtension = System.IO.Path.GetExtension(fu.FileName).ToLower();
 String[] allowedExtensions = { ".doc", ".hwp", ".pdf", ".jpg" };
 for (int i = 0; i < allowedExtensions.Length; i++)
 {
 if (fileExtension == allowedExtensions[i])
 {
 try
 {
 string s_newfilename = DateTime.Now.Year.ToString()+
 DateTime.Now.Month.ToString() + DateTime.Now.Day.ToString()+
 DateTime.Now.Hour.ToString() + DateTime.Now.Minute.ToString()+
 DateTime.Now.Second.ToString() + fileExtension;
 fu.PostedFile.SaveAs(filepath + s_newfilename);
 imagepath = ImageSavedPath + s_newfilename;
 }
 catch (Exception ex)
 {
 Response.Write("File could not be uploaded.");
 }
 }
 }
 }
 return imagepath;
}
```

## 2. MIME TYPE 확인을 통한 실행 파일 업로드 차단

(예) MIME TYPE을 통한 악성 파일 업로드 차단

```
public void validateFileToUpload(FileUpload objFile)
{
```

## 웹(Web)

```

intMAX_FILE_SIZE=(4*1024*1024);
int fileSize = objFile.PostedFile.ContentLength;
if(fileSize>MAX_FILE_SIZE)
{
 returnMessage="FileUploadFailed";
 returnreturnMessage;
}
string chosenFileExtension = System.IO.Path.GetExtension(objFile.FileName);

string[]allowedExtensions={".doc",".xls",".ppt",".pptx",".txt"};
if(!allowedExtensions.Contains(chosenFileExtension))
{
 returnMessage="FileUploadFailed";
 returnreturnMessage;
}
string[] allowedMimeTypes = { "text/plain", "text/xml" };
stringchosenFileMiMeType=objFile.PostedFile.ContentType;
if(!allowedMimeTypes.Contains(chosenFileMiMeType))
{
 returnMessage="FileUploadFailed";
 returnreturnMessage;
}
}

```

## ■ JSP

## 1. 수용 가능한 파일의 확장자만 업로드 허용(Positive 방식)

- 이미지 파일의 경우 (JPG, GIF, BMP 등)
- 문서 파일의 경우 (XLS, PDF, PPT, DOC 등)

(예) doc, hwp, pdf, jpg 파일만 업로드 허용 (※ 예로 제시하는 것으로, 구현 시 다를 수 있음)  
확장자 검증 시 대소문자 구분 없이 문자열 비교

```

.....
publicvoidupload(HttpServletRequestrequest)throwsServletException
{
 MultipartHttpRequest multi = (MultipartHttpRequest) request;
 String next = (String) multi.getFileNames().next();
 MultipartFile file = multi.getFile(next);
 If (file == null) return;
}

```

## 웹(Web)

```
// 화이트리스트 방식으로 업로드 파일 확장자 체크
if (fileName != null)
{
 If (fileName.endsWith(".doc") || fileName.endsWith(".hwp") ||
 fileName.endsWith(".pdf") || fileName.endsWith(".jpg"))
 {
 //file 업로드 루틴: 저장 시 파일명을 외부 사용자가 추측할 수 없는 형태로 변경

 }
}
```

## 2. MIME TYPE 확인을 통한 실행 파일 업로드 차단

(예) MIME TYPE을 통한 악성 파일 업로드 차단

```
<%
String[] validExt = {"jpg","gif","png"}; // 파일 허용 확장자
String[] validType = {"application/octet-stream",
"application/x-msdownload",
"application/x-sh"}; // 파일 MIME 타입 제한

MultipartRequest mRequest = new MultipartRequest(request,
SITE_UPLOAD_DIR+strUploadDir, intUploadMaxSize,
"UTF-8", new DefaultFileRenamePolicy());

uploadFileSystemName1 = mRequest.getFileName("attach1");
//저장파일명
File strGetfile1= mRequest.getFile("attach1");

uploadFileExt1 =
uploadFileSystemName1.substring(uploadFileSystemName1.lastIndexOf('.')
+ 1); // 파일 확장자
uploadFileType1 = mRequest.getContentType("attach1"); //파일 MIME 타입

for(int i=0; i< validType.length; i++) {
if(uploadFileType1.equalsIgnoreCase(validType[i])) {
out.print("<script>alert('업로드 금지 파일')</script>");
commUtil.deleteFile(SITE_UPLOAD_DIR+strUploadDir+"/"+ uploadFileSystemName1);
return;
}
}
%>
```

## 웹(Web)

## ■ PHP

## 1. 수용 가능한 파일의 확장자만 업로드 허용(Positive 방식)

- 이미지 파일의 경우 (JPG, GIF, BMP 등)
- 문서 파일의 경우 (XLS, PDF, PPT, DOC 등)

(예) doc, hwp, pdf, jpg 파일만 업로드 허용 (※ 예로 제시하는 것으로, 구현 시 다를 수 있음)  
확장자 검증 시 대소문자 구분 없이 문자열 비교

```
.....
// 파일 이름에 특수문자가 있을 경우 업로드를 금지시킴
if (ereg("[^a-z0-9\W_W-]",$_FILES['userfile']['name']))
print "파일 이름의 특수문자 체크";
exit;

// 파일 확장자 중 업로드를 허용할 확장자를 정의함
$full_filename = explode(".", $_FILES['userfile']['name']);
$extension = $full_filename[sizeof($full_filename)-1];
$extension= strtolower($extension);

if (!(ereg($extension,"hwp") || ereg($extension,"pdf") || ereg($extension,"jpg"))))
print "업로드 금지 파일 입니다";
exit;
.....
```

## 2. MIME TYPE 확인을 통한 실행 파일 업로드 차단

(예) MIME TYPE을 통한 악성 파일 업로드 차단

```
<?
// 허용된 확장자를 가진 파일에 대해서 파일 업로드 성공
If (($FILES["file"]["type"] == "image/gif") || ($FILES["file"]["type"] == "image/jpeg") ||
($FILES["file"]["type"] == "image/JPG") || ($FILES["file"]["type"] == "text/plain"))
{
 echo "파일 업로드 성공"
}
else
{
 echo "파일 업로드 실패. 허용된 파일의 형식이 아닙니다."
}
?>
```

조치 시 영향	일반적으로 영향 없음
---------	-------------

## 웹(Web)

취약점 항목	1.23. 파일 다운로드				
대상	소스코드	위험도	상	Code	FD
취약점 개요	공격자가 파일 다운로드 스크립트를 이용하여 웹 사이트에 포함된 주요 파일을 다운로드 할 수 있는 취약점으로, 홈페이지 상에서 파일을 다운받는 cgi, jsp, php, php3 등의 프로그램에서 입력되는 경로를 체크하지 않는 경우 임의의 문자(..../. 등)나 주요 파일명의 입력을 통해 웹 서버의 홈 디렉터리를 벗어나서 임의의 위치에 있는 파일을 열람하거나 다운받는 것이 가능할 수 있음.				
보안대책					
판단기준	양호: 다운로드 파일이 저장된 디렉터리 이외에 접근이 불가능한 경우				
	취약: 다운로드 파일이 저장된 디렉터리 이외에 접근이 가능한 경우				
조치방법	다운로드 시 정해진 경로 이외의 디렉터리와 파일에 접근할 수 없도록 구현				
보안설정방법					
■ 점검방법					
1. 게시판 또는 공지사항, 자료실 등에서 cgi, jsp, php 등의 프로그램을 이용하여 파일을 다운받는 페이지가 있는지 조사					
2. 해당 홈페이지의 파일 다운받기 주소에서 다운받는 파일명을 시스템의 중요한 파일(winnt\win.ini, /etc/passwd 등)의 위치와 이름을 상대경로(..../)로 치환한 후 입력하여 중요 파일의 다운이 가능한지 확인					
..../..../..../..../..../..../etc/passwd ..../..../..../..../..../..../winnt/win.ini ..../..../..../..../..../..../boot.ini					
3. 아래의 인코딩을 적용하여 2에서 입력한 값을 전송하여 해당 파일의 내용이 표시되는지 확인					
URL인코딩-(%2e), /(2f), ₩(%5c) 16bit 유니코드인코딩-(%u002e), /(u2215), ₩(%u2216) 더블URL인코딩-(%252e), /(252f), ₩(%255c)					
4. 다음 문자열을 적용하여 2에서 입력한 값을 전송하여 해당 파일의 내용이 표시되는지 확인					
...//, ....₩₩, ....₩/, ..../₩					
5. 다음 문자열을 적용하여 2에서 입력한 값을 전송하여 해당 파일의 내용이 표시되는지 확인					
[파일명]%00.jpg, [파일명]%0a.jpg					



## 웹(Web)

## ■ 보안설정방법

1. 파일 다운로드의 취약성은 주로 파일의 이름을 조작하는 데서 비롯됨  
다운로드 파일 이름을 데이터베이스에 저장하고 다운로드 수행 시 요청 파일 이름과 비교하여 적절한지 확인하여 사용자가 조작할 수 있는 변수를 제거하는 것이 바람직하며 또한, 다운로드 위치는 지정된 데이터 저장소를 고정하여 사용하는 것이 바람직함
2. 프로그램 내에서 파일을 다운받을 수 있는 디렉터리를 특정 디렉터리로 한정하고 이 외의 다른 디렉터리에서는 파일을 다운받을 수 없도록 프로그램을 수정하며, ..\ 등의 하위 경로 탐색은 제한하도록 수정함
3. PHP를 사용하는 경우 php.ini 에서 magic\_quotes\_gpc를 On으로 설정하여 .\./ 와 같은 역슬래시 문자에 대해 대응이 가능함
4. 파일 다운로드의 절대경로 설정 및 DocBase의 상위경로 또는, 타 드라이브로 설정을 변경함
5. 다운로드 경로 정보를 자바스크립트나 js 파일에 설정을 제한하며, 서블릿 내부 또는, 별도의 설정 파일에서 관리가 필요함
6. 다운로드를 제공하는 페이지의 유효 세션 체크 로직은 필수로 적용해야 함

## ※ 참고: 필터링 문자

문자	설명
.	Path Traversal 가능성의 확인
/	특정 Path 의 접근 가능성을 확인
\	운영환경에 따른 Path 접근 확인
%	UTF 인코딩 파라미터

## ■ ASP

(예) 필터링 처리 (※ 예로 제시하는 것으로, 구현 시 다를 수 있음)

```
.....
file = Request.form("file")

Response.ContentType = "application/unknown"
Response.AddHeader "Content-Disposition", "attachment; filename=" & file
Set objStream = Server.CreateObject("ADODB.Stream")

strFile = Server.MapPath("./uploadfiles") & "\\" & file

strFname = Mid(Fname, InstrRev(file, "\") + 1)
```

## 웹(Web)

```
if strFile = strFPath Then
```

```
.....
```

### ■ ASP.net

(예) ASP.net 예외처리 (※ 예로 제시하는 것으로, 구현 시 다를 수 있음)

.NET 환경은 자체적으로 Path Traversal 을 막고 있으므로, 소스 자체적인 별다른 조치는 필요가 없으나 일부 .NET 버전에 해당 보안 매커니즘을 우회할 수 있는 취약점이 발견된 사례가 있으므로, 최신 패치를 설치할 것을 권고함

해당 패치가 설치되어 있지 않은 경우 Global.asax에 다음과 같은 내용을 추가하여야 함

```
<script language="C#" runat="server">
void Application_BeginRequest(object source, EventArgs e) {
if (Request.Path.IndexOf('\\\\') >= 0 ||
 System.IO.Path.GetFullPath(Request.PhysicalPath) != Request.PhysicalPath) {
 throw new HttpException(404, "not found");
}
}</script>
```

### ■ PHP

(예) 필터링 처리 (※ 예로 제시하는 것으로, 구현 시 다를 수 있음)

```
if (preg_match("/^[a-z0-9_]/I", $up_dir))
print "디렉터리의 특수 문자 체크";
exit;

if (preg_match("/^[\\xA1-\\xFEa-z0-9_]/I", urldecode($dn_file_name)))
print "파일 이름의 특수문자 체크";
exit;
```

### ■ JSP

(예) 필터링 처리 (※ 예로 제시하는 것으로, 구현 시 다를 수 있음)

```
String UPLOAD_PATH= "/var/www/upload/";
String filename= response.getParameter("filename");
String filepathname = UPLOAD_PATH + filename;

if(filename.equalsIgnoreCase(".") || filename.equalsIgnoreCase("/")||
filename.equalsIgnoreCase("\\"))
 // 파일명 체크
```

## 웹(Web)

```

return 0;

// 파일 전송 루틴
response.setContentType("application/unknown; charset=euc-kr");
response.setHeader("Content-Disposition","attachment;filename=" + filename + ".");
response.setHeader("Content-Transfer-Encoding:" , "base64");

try {
 BufferedInputStream in = new BufferedInputStream(new
 FileInputStream(filepathname));

} catch(Exception e) {
 // 에러 체크 [파일 존재 유무 등]
}

```

## 조치 시 영향

일반적으로 영향 없음

## 웹(Web)

취약점 항목		1.24. 관리자 페이지 노출			
대상	소스코드	위험도	상	Code	AE
취약점 개요	단순한 관리자 페이지 이름(admin, manager 등)이나 설정 프로그램 설계상의 오류로 인해 관리자 메뉴에 직접 접근할 수 있는 취약점으로, 관리자 페이지는 웹 서비스의 사용자나 데이터, 콘텐츠를 손쉽게 관리하기 위한 목적으로 홈페이지의 운영에서 매우 중요한 역할을 하고 있으므로 일반 사용자에게 대한 접근을 제어해야 함. 그러나 일반적으로 추측하기 쉬운 URL(ex: /admin, /manager)을 사용하고 ID/패스워드에 대한 크랙 또는 접근 허가 정책에 대해 요청하는 부분의 정보를 변경함으로써 접근이 가능한 경우가 많음. 웹 관리자의 권한이 노출될 경우 홈페이지의 변조뿐만 아니라 취약성 정도에 따라서 웹 서버의 권한까지도 노출될 수 있음.				
보안대책					
판단기준	양호: 유추하기 쉬운 URL로 관리자 페이지 접근이 불가능한 경우				
	취약: 유추하기 쉬운 URL로 관리자 페이지 접근이 가능한 경우				
조치방법	유추하기 어려운 이름으로 관리자 페이지 변경				
보안설정방법					
■ 점검방법					
1. /admin, /manager, /master, /system, /administrator 등의 명칭을 사용하는 폴더 및 파일 관리자 페이지 존재여부 확인					
2. 7001, 8080, 8443, 8888 포트의 접속으로 관리 페이지가 노출되는지 확인					
3. 관리자 페이지에 기본 관리자 계정 및 패스워드를 입력하여 패스워드 취약점 점검 (관리자 계정의 예) admin, administrator, manager 등					
4. 사용자 인증을 통과하여 접속한 페이지에 대하여 인증 과정 없이 중간 페이지에 접속하여 접속이 가능한지 점검 (예) /admin/main.asp, /admin/menu.html 등					
■ 보안설정방법					
1. 일반 사용자의 접근이 불필요한 관리자 로그인 페이지 주소를 유추하기 어려운 이름으로 변경함					
2. 중요한 정보를 가진 웹 서버의 특정 페이지들은 관리자 또는, 특정 사용자만 접근할 필요가 있으므로 이러한 주요 페이지들은 웹 서버에서 적절한 설정을 통하여 특정 사용자만 접근이 가능하도록 사용자 접근 제한이 필요함					
조치 시 영향	일반적으로 영향 없음				

## 웹(Web)

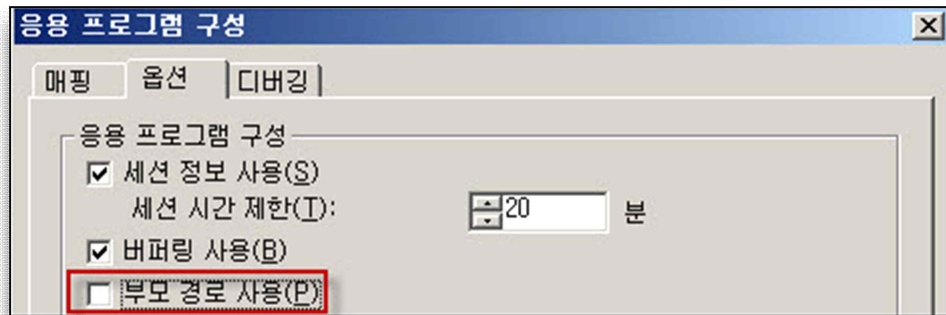
취약점 항목		1.25. 경로 추적			
대상	Web Server	위험도	상	Code	PT
취약점 개요	웹 서버 또는 웹 응용의 파일 또는, 디렉터리 접근이 통제되지 않아 서버 또는 웹 애플리케이션의 중요한 파일 또는 데이터에 접근을 허용하는 취약점으로 웹 루트 디렉터리에서 외부의 파일까지 접근하여 이를 실행할 수 있음. 공격자는 웹 서버에 존재하는 파일의 경로를 URL에 입력하여 해당 파일을 실행할 수 있음.				
보안대책					
판단기준	양호: 홈페이지 루트 디렉터리 상위 폴더 접근이 불가능한 경우				
	취약: 홈페이지 루트 디렉터리 상위 폴더로 접근이 가능한 경우				
조치방법	웹 사이트의 최상위 폴더를 웹 사이트 Root 폴더로 제한				
보안설정방법					
■ 점검방법					
1. 표시할 페이지의 파일을 지정하는 변수값에 다음 값을 입력하여 해당 파일의 내용이 표시되는 지 확인					
../..../etc/passwd					
../..../winnt/win.ini					
../..../boot.ini					
2. 다음 인코딩을 적용하여 1에서 입력한 값을 전송하여 해당 파일의 내용이 표시되는지 확인					
URL인코딩-.(%2e), /( %2f), ₩(%5c)					
16bit 유니코드인코딩-.(%u002e), /( %u2215), ₩(%u2216)					
더블URL인코딩-.(%252e), /( %252f), ₩(%255c)					
3. 다음 문자열을 적용하여 1에서 입력한 값을 전송하여 해당 파일의 내용이 표시되는지 확인					
...//, ....₩₩, ....₩/, ....₩					
4. 다음 문자열을 적용하여 1에서 입력한 값을 전송하여 해당 파일의 내용이 표시되는지 확인					
[파일명]%00.jpg, [파일명]%0a.jpg					
■ 보안설정방법					
1. 웹 사이트에서 접근하려는 파일이 있는 디렉터리에 *chroot 환경을 적용해서 경로 추적 공격을 최소화할 수 있음					
*chroot 환경: chroot 디렉터리는 해당 디렉터리가 루트처럼 다뤄짐. chroot 파일 시스템은 대부분의 유닉스를 기반으로 한 플랫폼에서 지원이 가능하고, 윈도우 플랫폼에서는 적절한 시작 디렉터리를 새로운 논리 드라이브로 만들어 웹 사이트에서 해당 드라이브를 통하여 접근하게 함.					

## 웹(Web)

## 2. 웹 사이트의 최상위 폴더를 웹 사이트 Root 폴더로 제한

## ■ IIS

인터넷 정보서비스(IIS) 관리> [해당 웹 사이트]> [속성]> [홈 디렉터리]탭> [구성] 버튼 선택> [옵션] 탭에서 [부모 경로 사용] 체크 해제



조치 시 영향	일반적으로 영향 없음
---------	-------------

## 웹(Web)

취약점 항목		1.26. 위치 공개			
대상	Web Server	위험도	상	Code	PL
취약점 개요	폴더나 파일명의 위치가 예측 가능하고 쉽게 노출되어 공격자가 이를 악용하여 대상에 대한 정보를 획득하고 민감한 데이터에 접근 가능하게 하는 취약점으로 웹 서버에서 HTML로 로드 되지 않는 불필요한 파일은 삭제하여야 함.				
보안대책					
판단기준	양호: 불필요한 파일이 존재하지 않고, 샘플 페이지가 존재하지 않을 경우				
	취약: 불필요한 파일이 존재하거나, 샘플 페이지가 존재하는 경우				
조치방법	불필요한 파일 삭제 및 샘플 페이지 삭제				
보안설정방법					
■ 점검방법					
1. .bak, .backup, .org, .old, .zip, .log, .sql, .new, .txt, .tmp, .temp 확장자의 불필요한 파일 존재 확인					
2. cgi-bin , manual, usage, iissamples, scripts, iisHelp, IISAdmin, _vit_bin, Printers, phpinfo.php, examples, jsp, servlets의 디렉터리 및 파일 존재여부 확인					
■ 보안설정방법					
삭제해야 할 파일 확장자					
*.bak	*.backup	*.org	*.old		
*.zip	*.log	*.!	*.sql		
*.new	*.txt	*.tmp	*.temp		
1. 웹 디렉터리를 조사하여 다음과 같은 백업 파일을 모두 삭제 하고, *.txt 같이 작업 중 생성된 일반 텍스트 파일이나 이미지 파일 등도 제거함					
2. 백업 파일은 백업 계획을 수립하여 안전한 곳에 정기적으로 백업해야 하며 웹 서버 상에는 운영에 필요한 최소한의 파일만을 생성하여야 함					
3. 웹 서버 설정 후 디폴트 페이지와 디폴트 디렉터리 및 Banner를 삭제하여 Banner Grab에 의한 시스템 정보 유출을 차단함					
4. Apache, IIS, Tomcat 등 각 웹 서버 설정 시 함께 제공되는 샘플 디렉터리 및 매뉴얼 디렉터리, 샘플 애플리케이션을 삭제하여 보안 위험을 최소화 함					
조치 시 영향	일반적으로 영향 없음				

## 웹(Web)

취약점 항목	1.27. 데이터 평문 전송				
대상	소스코드	위험도	상	Code	SN
취약점 개요	서버와 클라이언트 간 통신 시 데이터 암호화 프로세스가 구현되지 않아 중요 정보 등이 평문으로 전송되는 취약점으로 암호화를 통해 정보 유출의 위험을 최소화해야 함. 웹상의 데이터 통신은 대부분 텍스트 기반으로 이루어지고 있으며 이는 간단한 도청(Sniffing)을 통해 정보의 탈취 및 도용할 수 있으므로, 중요 정보 전송 구간에 암호화 통신을 적용해야 함.				
보안대책					
판단기준	양호: 중요 정보 전송 구간에 암호화 통신이 적용된 경우				
	취약: 중요 정보 전송 구간에 암호화 통신이 이루어지지 않는 경우				
조치방법	중요 정보 전송 구간 암호화 통신 적용				
보안설정방법					
■ 점검방법   1. 중요 정보(인증정보, 개인정보 등)를 송수신하는 페이지 존재여부 확인   2. 중요 정보 송수신 페이지가 암호화 통신(https, 데이터 암호화 등)을 하는지 확인   ■ 보안설정방법   1. 웹상에서의 전송 정보를 제한하여 불필요한 비밀번호, 주민등록번호, 계좌정보와 같은 중요 정보의 전송을 최소화하여야 하며, 중요 정보에 대해서는 반드시 SSL 등의 암호화 통신을 사용하여 도청으로부터의 위험을 제거함   2. 쿠키와 같이 클라이언트 측에서 노출되는 곳에 비밀번호, 인증인식 값, 개인정보 등의 정보를 기록하지 않음					
조치 시 영향	일반적으로 영향 없음				



## 웹(Web)

취약점 항목	1.28. 쿠키 변조				
대상	소스코드	위험도	상	Code	CC
취약점 개요	적절하게 보호되지 않은 쿠키를 사용하여 쿠키 인젝션 등과 같은 쿠키 값 변조를 통한 다른 사용자로의 위장 및 권한 상승 등을 가능하게 하는 취약점으로, 쿠키(Cookie)는 클라이언트에 전달되는 값으로 중요 정보로 구성되므로 이 정보의 조작을 통해 다른 사용자의 유효한 세션을 취득할 수도 있고, 기타 중요 정보의 유출 및 변조가 발생할 위험이 있음.				
보안대책					
판단기준	양호: 쿠키를 사용하지 않고 Server Side Session을 사용하는 경우				
	취약: 쿠키를 사용하거나, Client Side Session을 사용하는 경우				
조치방법	Server Side Session 사용으로 변경				
보안설정방법					
■ 점검방법   1. 쿠키 내용 및 발행되는 쿠키에 중요 정보(인증을 위한 ID, 권한을 위한 구분자 등)의 노출 여부 조사   2. 쿠키의 중요 정보를 변경하여 다른 사용자 및 권한으로 정상적 이용이 가능한지 확인   ■ 보안설정방법   1. 쿠키대신 보안성이 강한 Server Side Session을 사용   Client Side Session 방식인 쿠키는 그 구조상 다양한 취약점에 노출될 수 있으므로 가능한 웹 서버에서 제공되는 Server Side Session을 사용하는 것이 바람직함					
조치 시 영향	일반적으로 영향 없음				