과학기술정보통신부 KISA 한국인터넷진흥원

2017. 12

주요정보통신기반시설

기술적 취약점 분석 · 평가 방법 상세가이드

<유의 사항>

- 본 가이드는 기술적 취약점 분석·평가 항목별 점검 방법의 이해를 돕기 위해 발간된 것으로, 수록된 점검 방법은 취약점 분석·평가 수행 중 활용할 수 있는 참조의 대상일 뿐, 절대적이지 않습니다. 더욱이 점검 대상의 세부 버전, 패치 내용 등에 따라 점검 방법은 언제든지 변경될 수 있습니다. 따라서 본 가이드에 수록된 내용 이외에도 다양한 점검 방법을 사용하여 취약점 분석평가를 수행하시기 바랍니다.
- 본 가이드의 수록된 판단기준은 일반적으로 통용되는 권고사항으로, 양호 혹은 취약을 가르는 실제 판단기준은 각 주요정보통신기반시설 현업에 적용되고 있는 다양한 정책 및 운용 상황을 고려하여 취약점 분석·평가 수행자가 최종적으로 결정해야 합니다.
  예를 들어 본 가이드에 수록된 판단기준에 의하여 취약판단을 받게 되어도 그 위험을 부담할 수 있는 합당한 보안조치와 근거를 수반하고 있다면 양호로 판단할 수 있습니다.
- 본 가이드를 교육기관 등에서 교육 자료로 활용하는 것을 권장하지 않습니다.
- 본 가이드에 수록된 점검 및 조치 사례는 시스템 유형별로 다음(표. 분야별 점검대상 테스트 세부 버전) 버전에서 실증 되었습니다.
- 개선 사항(취약점 개요, 점검 방법, 조치 방법 등)에 대한 의견을 항상 소중히 듣겠습니다. (한국인터넷진흥원)

분야	세부 버전
1. 유닉스	• AIX 7.1 • HP-UX 11i v3 • SOLARIS 11.2 • Cent OS 6.6 (Linux)
2. 윈도우즈	• Windows Server 2000, NT 5.0 • Windows Server 2003 Standard SP2 x64 • Windows Server 2008 Standard R2 SP1 x64 • Windows Server 2012 Standard R2 x64
3. 보안 장비	• 범용 벤더 (방화벽, IPS, IDS, VPN 등)
4. 네트워크 장비	• CISCO IOS 15 • JUNIPER Junos OS 12 • Radware Alteon OS 29 • Nortel Passport • Piolink PLOS
5. 제어시스템	• 범용 벤더 (HMI, PLC, Data Historian 등)
6. PC	• Windows XP Professional SP3 x86 • Windows 7 Professional SP2 x64 • Windows 8.1 Professional x64 • Windows 10 Professional x64
7. 데이터베이스	• Oracle Database 11 • MS SQL Server 2014 • MySQL 5 • Tibero 6 • ALTIBASE 6
8. 웹 (Web)	• 소스 코드 (웹 서버, 웹 방화벽 등)

표. 분야별 점검대상 테스트 세부 버전

주요정보통신기반시설
기술적 취약점 분석 · 평가 방법 상세가이드

Contents

주요정보통신기반시설
기술적 취약점 분석 · 평가 방법 상세가이드

Contents

웹(WEB)

I

개요

1. 개요

주요정보통신기반시설 관리기관은「정보통신기반 보호법」제9조에 따라, 주요정보통신기반시설로 신규 지정된 후 6개월 이내, 그리고 매년 취약점 분석・평가를 실시하여야 한다. 취약점 분석・평가는 453개의 관리적/물리적/기술적 점검항목에 대한 주요정보통신기반시설의 취약여부를 점검하여, 악성코드 유포, 해킹 등 사이버 위협 대응을 위한 종합적 개선 과정이다.

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

이러한 기술적 점검에 대한 어려움을 해소하고, 주요정보통신기반시설 담당자들의 이해를 돕기 위해 과학기술정보통신부와 한국인터넷진흥원에서는 전체 313개 기술적 점검항목에 대한 가이드를 발간하게 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.

특히, 이번 개정판 에서는 Windows 10・2012 server, TIBERO, ALTIBASE 등 영역별 신규 시스템을 추가하여 담당자들의 활용성을 더욱 높였다.

2. 목적 및 구성

목적	주요정보통신기반시설 담당자의 기반시설 보호 역량강화를 위한 기술적 안내 제공
대상	주요정보통신기반시설 정보보호 담당자
범위	주요정보통신기반시설 기술적 취약점 분석・평가 항목 313개
구성	기술적 점검 기준(313개 항목)의 항목 설명, 점검(설정확인) 방법, 조치 방법(Unix, Windows, 보안장비, 네트워크장비, 제어시스템, PC, DBMS, Web)
활용	주요정보통신기반시설 기술적 취약점 분석 및 보안조치 시 활용

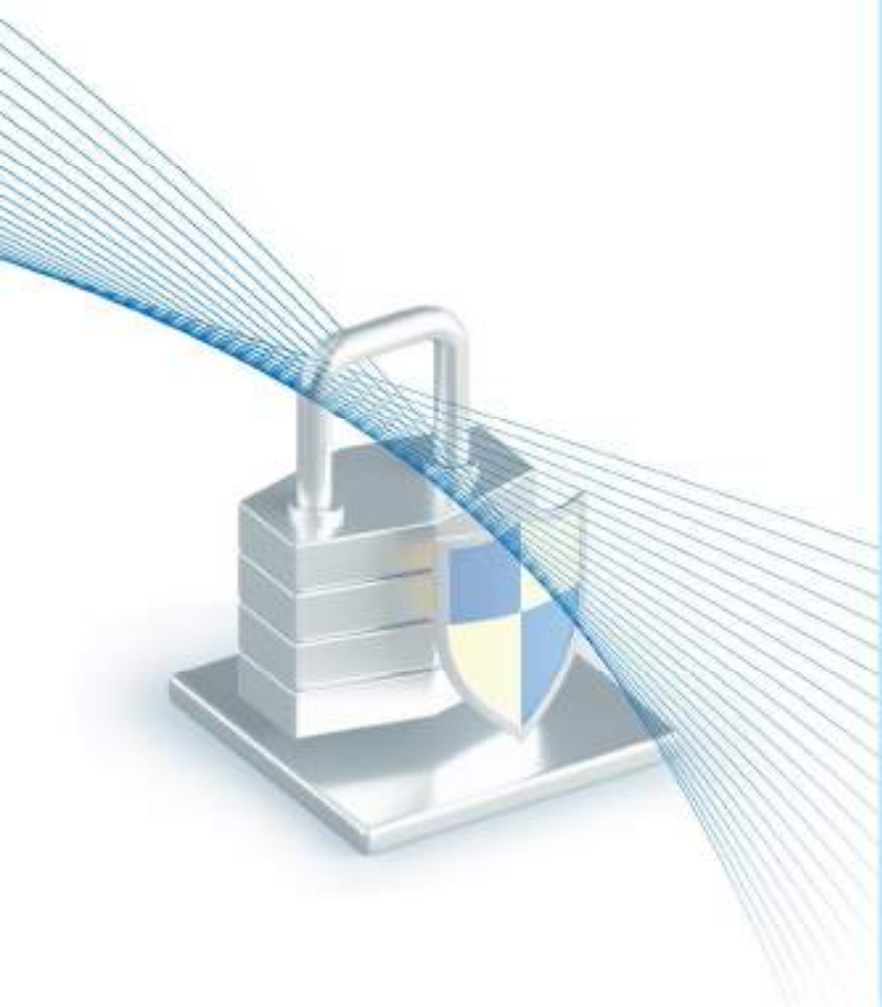
Ⅱ

보안 가이드라인

Ⅱ

UNIX 서버

기본/선택



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-44
	root 계정 su 제한	하	U-45
	패스워드 최소 길이 설정	중	U-46
	패스워드 최대 사용기간 설정	중	U-47
	패스워드 최소 사용기간 설정	중	U-48
	불필요한 계정 제거	하	U-49
	관리자 그룹에 최소한의 계정 포함	하	U-50
	계정이 존재하지 않는 GID 금지	하	U-51
	동일한 UID 금지	중	U-52
	사용자 shell 점검	하	U-53
	Session Timeout 설정	하	U-54
2. 파일 및 디렉터리 관리	root 홈, 패스 디렉터리 권한 및 패스 설정	상	U-05
	파일 및 디렉터리 소유자 설정	상	U-06
	/etc/passwd 파일 소유자 및 권한 설정	상	U-07
	/etc/shadow 파일 소유자 및 권한 설정	상	U-08
	/etc/hosts 파일 소유자 및 권한 설정	상	U-09
	/etc/(x)inetd.conf 파일 소유자 및 권한 설정	상	U-10
	/etc/syslog.conf 파일 소유자 및 권한 설정	상	U-11
	/etc/services 파일 소유자 및 권한 설정	상	U-12
	SUID, SGID, Sticky bit 설정 파일 점검	상	U-13
	사용자, 시스템 시작파일 및 환경파일 소유자 및 권한 설정	상	U-14
	world writable 파일 점검	상	U-15
	/dev에 존재하지 않는 device 파일 점검	상	U-16
	$HOME/.rhosts, hosts.equiv 사용 금지	상	U-17
	접속 IP 및 포트 제한	상	U-18
	hosts.lpd 파일 소유자 및 권한 설정	하	U-55
	NIS 서비스 비활성화	중	U-56
	UMASK 설정 관리	중	U-57
	홈디렉토리 소유자 및 권한 설정	중	U-58
	홈디렉토리로 지정한 디렉토리의 존재 관리	중	U-59
	숨겨진 파일 및 디렉토리 검색 및 제거	하	U-60

3. 서비스 관리	finger 서비스 비활성화	상	U-19
	Anonymous FTP 비활성화	상	U-20
	r 계열 서비스 비활성화	상	U-21
	cron 파일 소유자 및 권한설정	상	U-22
	Dos 공격에 취약한 서비스 비활성화	상	U-23
	NFS 서비스 비활성화	상	U-24
	NFS 접근 통제	상	U-25
	automountd 제거	상	U-26
	RPC 서비스 확인	상	U-27
	NIS, NIS+ 점검	상	U-28
	tftp, talk 서비스 비활성화	상	U-29
	Sendmail 버전 점검	상	U-30
	스팸 메일 릴레이 제한	상	U-31
	일반사용자의 Sendmail 실행 방지	상	U-32
	DNS 보안 버전 패치	상	U-33
	DNS Zone Transfer 설정	상	U-34
	Apache 디렉토리 리스팅 제거	상	U-35
	Apache 웹 프로세스 권한 제한	상	U-36
	Apache 상위 디렉토리 접근 금지	상	U-37
	Apache 불필요한 파일 제거	상	U-38
	Apache 링크 사용 금지	상	U-39
	Apache 파일 업로드 및 다운로드 제한	상	U-40
	Apache 웹 서비스 영역의 분리	상	U-41
	ssh 원격접속 허용	중	U-61
	ftp 서비스 확인	하	U-62
	ftp 계정 shell 제한	중	U-63
	Ftpusers 파일 소유자 및 권한 설정	하	U-64
	Ftpusers 파일 설정	중	U-65
	at 파일 소유자 및 권한 설정	중	U-66
	SNMP 서비스 구동 점검	중	U-67
	SNMP 서비스 커뮤니티스트링의 복잡성 설정	중	U-68
	로그온 시 경고 메시지 제공	하	U-69
	NFS 설정파일 접근 제한	중	U-70
	expn, vrfy 명령어 제한	중	U-71
	Apache 웹 서비스 정보 숨김	중	U-72
4. 패치 관리	최신 보안패치 및 벤더 권고사항 적용	상	U-42
5. 로그 관리	로그의 정기적 검토 및 보고	상	U-43
	정책에 따른 시스템 로깅 설정	하	U-73

U-01 (상)	1. 계정관리 > 1.1 root 계정 원격 접속 제한
취약점 개요	
점검내용	■ 시스템 정책에 root 계정의 원격 터미널 접속 차단 설정이 적용 되어 있는지 점검
점검목적	■ root 계정 원격 접속 차단 설정 여부를 점검하여 외부 비인가자의 root 계정 접근 시도를 원천적으로 차단하는지 확인하기 위함
보안위협	■ 각종 공격(무작위 대입 공격, 사전 대입 공격 등)을 통해 root 원격 접속 차단이 적용되지 않은 시스템의 root 계정 정보를 비인가자가 획득할 경우 시스템 계정 정보 유출, 파일 및 디렉터리 변조 등의 행위 침해사고가 발생할 수 있음
참고	※ **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 ※ **무작위 대입 공격(Brute Force Attack):** 특정한 암호를 풀기 위해 가능한 모든 값을 대입하는 공격 방법 ※ **사전 대입 공격(Dictionary Attack):** 사전에 있는 단어를 입력하여 암호를 알아내거나 암호를 해독하는 데 사용되는 컴퓨터 공격 방법
점검대상 및 판단기준	
대상	■ SOLARIS, LINUX, AIX, HP-UX 등
판단기준	**양호 :** 원격 터미널 서비스를 사용하지 않거나, 사용 시 root 직접 접속을 차단한 경우
	취약 : 원격 터미널 서비스 사용 시 root 직접 접속을 허용한 경우
조치방법	원격 접속 시 root 계정으로 바로 접속 할 수 없도록 설정파일 수정
점검 및 조치사례	

OS별 점검 파일 위치 및 점검 방법	
SOLARIS	`#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 내용으로 설정되어 있을 경우 root 원격 접속이 차단됨 / 내용 설정에 대해서는 아래의 보안설정방법을 참고함	

UNIX 서버

U-01 (상)	1. 계정관리 > 1.1 root 계정 원격 접속 제한

■ **SOLARIS**

Step 1) vi 편집기를 이용하여 "/etc/default/login" 파일 열기

Step 2) 아래와 같이 주석 제거 또는, 신규 삽입

(수정 전) `#CONSOLE=/dev/console`

(수정 후) `CONSOLE=/dev/console`

■ **LINUX**

Step 1) "/etc/securetty" 파일에서 pts/0 ~ pts/x 설정 제거 또는, 주석 처리

Step 2) "/etc/pam.d/login" 파일 수정 또는, 신규 삽입

(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

*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**

Step 1) vi 편집기를 이용하여 "/etc/security/user" 파일 열기

Step 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**

Step 1) vi 편집기를 이용하여 "/etc/securetty" 파일 열기

Step 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 내용 수정: 부록 참고)

`#vi /etc/securetty`

조치 시 영향	일반적인 경우 영향 없음

U-02 (상)	1. 계정관리 > 1.2 패스워드 복잡성 설정
취약점 개요	
점검내용	■ 시스템 정책에 사용자 계정(root 및 일반 계정 모두 해당) 패스워드 복잡성 관련 설정이 되어 있는지 점검
점검목적	■ 패스워드 복잡성 관련 정책이 설정되어 있는지 점검하여 비인가자의 공격(무작위 대입 공격, 사전 대입 공격 등)에 대비가 되어 있는지 확인하기 위함
보안위협	■ 패스워드 복잡성 설정이 되어 있지 않은 사용자 계정 패스워드 존재 시 비인가자가 각종 공격(무작위 대입 공격, 사전 대입 공격 등)을 통해 취약한 패스워드가 설정된 사용자 계정의 패스워드를 획득하여 획득한 사용자 계정 정보를 통해 해당 사용자 계정의 시스템에 접근할 수 있는 위험이 존재함
참고	※ **패스워드 복잡성:** 사용자 패스워드 설정 시 영문(대문자, 소문자), 숫자, 특수문자가 혼합된 패스워드로 설정하는 방법 ※ 공공기관인 경우 국가정보보안기본지침에 의해 패스워드를 9자리 이상의 길이로 설정해야함
점검대상 및 판단기준	
대상	■ SOLARIS, LINUX, AIX, HP-UX 등
판단기준	**양호 :** 영문·숫자·특수문자를 조합하여 2종류 조합 시 10자리 이상, 3종류 이상 조합 시 8자리 이상의 패스워드가 설정된 경우 (공공기관 9자리 이상)
	취약 : 영문·숫자·특수문자를 조합하지 않거나 2종류 조합 시 10자리 미만, 3종류이상 조합 시 8자리 미만의 길이가 패스워드로 설정된 경우 (공공기관 9자리 미만)
조치방법	계정과 유사하지 않은 8자 이상의 영문, 숫자, 특수문자의 조합으로 암호 설정 및 패스워드 복잡성 옵션 설정
점검 및 조치 사례	

OS별 점검 파일 위치 및 점검 방법	
SOLARIS, 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	

■ SOLARIS, LINUX, AIX, HP-UX

< 부적절한 패스워드 유형 >

1. 사전에 나오는 단어나 이들의 조합
2. 길이가 너무 짧거나, NULL(공백)인 패스워드

UNIX 서버

U-02 (상)	1. 계정관리 > 1.2 패스워드 복잡성 설정

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 (공공기관 9자리 이상)

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

< 패스워드 설정 파일 정리 >

■ SOLARIS

Step 1) 패스워드 복잡성 설정

#/etc/default/passwd 내용을 내부 정책에 맞도록 편집

maxweeks = 4 (최대 사용 기간 설정)
최대 4주까지 설정된 패스워드 사용 가능

minweeks = 3 (최소 사용 기간 설정)
최소 3주까지 설정된 패스워드 사용

※ 사용자에게 3주 ~ 4주 사이에 암호를 변경하도록 요구함

passlength = 8 (최소 길이 설정)
최소 8자 이상의 암호를 요구

※ 아래 설정값은 솔라리스 10부터 추가 적용된 설정값임

HISTORY = 10 (패스워드 기억 개수)
10개의 암호를 기억함

MINDIFF = 4 (이전 암호와 차이)
이전 암호와 4자 이상 차이를 요구

MINALPHA = 1 (최소 문자 요구)
최소 1자 이상 문자 요구

MINNONALPHA = 1 (최소 숫자 또는 특수문자 요구)
최소 숫자 또는 특수문자 1자 이상 요구

U-02 (상)	1. 계정관리 > 1.2 패스워드 복잡성 설정

※ DIGIT 이나 SPECIAL 이 설정되어 있을 경우 NONALPHA 설정 안 됨

MINUPPER=1 (최소 대문자 요구)
최소 1자 이상 대문자 요구

MINLOWER=1 (최소 소문자 요구)
최소 1자 이상 소문자 요구

MAXREPEATS=0 (연속문자 사용 허용)
0일 경우 문자 연속 사용이 불가능

MINSPECIAL=1 (최소 특수문자 요구)
최소 1자 이상 특수문자 요구

MINDIGIT=1 (최소 숫자 요구)
최소 1자 이상 숫자 요구

■ LINUX - RHEL5

Step 1) 패스워드 복잡성 설정 파일 확인
#/etc/pam.d/system-auth, /etc/login.defs 내용을 내부 정책에 맞도록 편집

Step 2) /etc/pam.d/system-auth 파일 설정
※ 다음 라인에 패스워드 정책을 설정함
- 패스워드 정책 설정 예시

```
password requisite /lib/security/$ISA/pam_cracklib.so retry=3 minlen=8 lcredit=-1
ucredit=-1 dcredit=-1 ocredit=-1
```

※ 각 변수에 대한 설명 / 각 항목에서 -1 값은 반드시 해당하는 문자를 포함시켜야 함

lcredit=-1 (최소 소문자 요구)
소문자 최소 1자 이상 요구

ucredit=-1 (최소 대문자 요구)
최소 대문자 1자 이상 요구

dcredit=-1 (최소 숫자 요구)
최소 숫자 1자 이상 요구

ocredit=-1 (최소 특수문자 요구)
최소 특수문자 1자 이상 요구

minlen=8 (최소 패스워드 길이 설정)
최소 8자리 이상 설정

retry=3 (패스워드 입력 실패 시 재시도 횟수)
3번 패스워드 재입력 가능

UNIX 서버

U-02 (상)	1. 계정관리 > 1.2 패스워드 복잡성 설정

difok=N (기존 패스워드와 비교. 기본값 10(50%))

Step3) /etc/login.defs 파일 설정

pass_warn_age = 7 (패스워드 기간 만료 경고)
7일이 남은 시점부터 패스워드 변경 알림

pass_max_days = 60 (최대 패스워드 사용 기간 설정)
설정일로부터 60일까지 사용 가능

pass_min_day = 1 (최소 패스워드 변경 기간 설정)
최소 1일 경과 후 패스워드 변경 가능

■ **LINUX - RHEL7**

Step 1) 패스워드 복잡성 설정 파일 확인

#/etc/security/pwquality.conf 파일 수정

※ 다음 라인에 패스워드 정책을 설정함

- 패스워드 정책 설정 예시

password requisite pam_cracklib.so try_first_pass retry=3 minlen=8 lcredit=-1 ucredit=-1 dcredit=-1 ocredit=-1

※ 각 변수에 대한 설명 / 각 항목에서 -1 값은 반드시 해당하는 문자를 포함시켜야 함

lcredit=-1 (최소 소문자 요구)
소문자 최소 1자 이상 요구

ucredit=-1 (최소 대문자 요구)
최소 대문자 1자 이상 요구

dcredit=-1 (최소 숫자 요구)
최소 숫자 1자 이상 요구

ocredit=-1 (최소 특수문자 요구)
최소 특수문자 1자 이상 요구

minlen=8 (최소 패스워드 길이 설정)
최소 8자리 이상 설정

retry=3 (패스워드 입력 실패 시 재시도 횟수)
3번 패스워드 재입력 가능

difok=N (기존 패스워드와 비교. 기본값 10(50%))

Step3) /etc/login.defs 파일 설정

pass_warn_age = 7 (패스워드 기간 만료 경고)
7일이 남은 시점부터 패스워드 변경 알림

U-02 (상)	1. 계정관리 > 1.2 패스워드 복잡성 설정

pass_max_days = 60 (최대 패스워드 사용 기간 설정)
설정일로부터 60일까지 사용 가능

pass_min_day = 1 (최소 패스워드 변경 기간 설정)
최소 1일 경과 후 패스워드 변경 가능

■ **AIX**

Step 1) 패스워드 복잡성 설정 파일 확인
#/etc/security/user 파일 내용을 내부 정책에 맞도록 설정

dictionlist = (패스워드에 unix 명령어가 포함되지 않게 함)
dictionlist = /usr/share/dict/words 으로 설정

histexpire = 26 (몇 주 후에 동일한 패스워드가 재사용될 수 있는지 설정)
26주 후에 동일한 패스워드 사용 가능

histsize = 20 (최근 사용된 패스워드를 몇 개까지 재사용할 수 없게 할지를 설정)
최근 20개 패스워드는 재사용할 수 없음

maxage = 4 (패스워드가 몇 주 동안 유효할 수 있는지 정의)
최대 패스워드 사용 기간 4주로 설정

minage = 1 (패스워드를 바꾸기 위해서 경과되어야 하는 최소한의 시간)
최소 1주 이후에 패스워드 변경 가능

maxexpired = 2(maxage가 지난 다음에 expire 된 패스워드를 변경할 있는 최대 주)
최대 패스워드 사용 기간 경과 후 2주 이내에 패스워드 변경 가능

maxrepeats = 2 (패스워드에 반복 가능한 동일 문자의 최대 수)
최대 2자까지 반복 사용 가능

minalpha = 2 (최소 몇개의 알파벳 문자를 포함해야 하는지 설정)
최소 2개 영문자 포함

minother = 2 (최소 포함해야 할 알파벳 문자 이외의 문자 개수)
영문자 외 다른 문자 최소 2개 필요

mindiff = 4 (이전 패스워드와 신규 패스워드 사이에 최소한의 다른 문자 수)
최소 4개 문자 반복 금지

minlen = 8 (패스워드 최소 길이)
패스워드 최소 8자리

pwdwarntime = 5 (패스워드 변경이 필요함을 몇 일전부터 알릴지를 설정)
5일전부터 패스워드 변경 알림

UNIX 서버

U-02 (상)	1. 계정관리 > 1.2 패스워드 복잡성 설정

■ **HP-UX**

Step 1) 패스워드 복잡성 설정

#/etc/default/security 내용을 내부 정책에 맞도록 편집

INACTIVITY_MAXDAYS = 100 (사용되지 않아 계정을 만료하기까지의 기간/일 단위)
100일 동안 계정 사용이 없을 경우 만료

PASSWORD_MINDAYS = 1 (암호를 변경할 수 있기까지의 최소 기간/일 단위)
최소 1일 이후 패스워드 변경 가능

PASSWORD_MAXDAYS =90 (암호가 유효한 최대 기간/일 단위)
최대 90일까지 패스워드 사용 가능

PASSWORD_WARNDAYS = 15 (사용자에게 암호 만료를 경고하기까지의 기간/일 단위)
암호 만료 15일 전부터 알림

MIN_PASSWORD_LENGTH = 8 (암호의 최소 길이)
최소 패스워드 길이 8

PASSWORD_MIN_UPPER_CASE_CHARS = 1 (최소 대문자 필요 개수)
최소 1개의 대문자 필요

PASSWORD_MIN_LOWER_CASE_CHARS = 1 (최소 소문자 필요 개수)
최소 1개의 소문자 필요

PASSWORD_MIN_DIGIT_CHARS = 1 (최소 숫자 필요 개수)
최소 1개의 숫자 필요

PASSWORD_MIN_SPECIAL_CHARS = 1 (최소 특수문자 필요 개수)
최소 1개의 특수문자 필요

조치 시 영향	패스워드 변경 시 Web, WAS, DB연동 구간에서 문제가 발생할 수 있으므로 연동 구간에 미칠 수 있는 영향을 고려하여 적용 필요

U-03 (상)	1. 계정관리 > 1.3 계정 잠금 임계값 설정
취약점 개요	
점검내용	■ 시스템 정책에 사용자 로그인 실패 임계값이 설정되어 있는지 점검
점검목적	■ 시스템 정책에 사용자 로그인 실패 임계값이 설정되어 있는지 점검하여 비인가자의 공격(무작위 대입 공격, 사전 대입 공격, 추측 공격 등) 시도 시 로그인 실패 임계값에 따라 로그인을 차단하고 있는지 확인하기 위함
보안위협	■ 로그인 실패 임계값이 설정되어 있지 않을 경우 반복되는 로그인 시도에 대한 차단이 이루어지지 않아 각종 공격(무작위 대입 공격, 사전 대입 공격, 추측 공격 등)에 취약하여 비인가자에게 사용자 계정 패스워드를 유출 당할 수 있음
참고	※ **사용자 로그인 실패 임계 값:** 시스템에 로그인 시 몇 번의 로그인 실패에 로그인을 차단할 것인지 결정하는 값
점검대상 및 판단기준	
대상	■ SOLARIS, LINUX, AIX, HP-UX 등
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
점검 및 조치 사례	

OS별 점검 파일 위치 및 점검 방법	
SOLARIS	#cat /etc/default/login RETRIES=5 SOLARIS 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

UNIX 서버

U-03 (상)	1. 계정관리 > 1.3 계정 잠금 임계값 설정

HP-UX	#cat /tcb/files/auth/system/default u_maxtries#5 HP-UX 11.v3 이상일 경우 "security" 파일 확인 #cat /etc/default/security AUTH_MAXTRIES=5
위에 제시한 설정이 해당 파일에 적용되지 않은 경우 아래의 보안설정방법에 따라 설정을 변경함	

■ **SOLARIS**

- SOLARIS 5.9 이하 버전 -

Step 1) vi 편집기를 이용하여 "/etc/default/login" 파일 열기

Step 2) 아래와 같이 수정 또는, 신규 삽입

(수정 전) #RETRIES=2

(수정 후) RETRIES=5

- SOLARIS 5.9 이상 버전 -

Step 1) vi 편집기를 이용하여 "/etc/default/login" 파일 열기

Step 2) 아래와 같이 수정 또는, 신규 삽입 (계정 잠금 횟수 설정)

(수정 전) #RETRIES=2

(수정 후) RETRIES=5

Step 3) vi 편집기를 이용하여 "/etc/security/policy.conf" 파일 열기

Step 4) 아래와 같이 수정 또는, 신규 삽입 (계정 잠금 정책사용 설정)

(수정 전) #LOCK_AFTER_RETRIES=NO

(수정 후) LOCK_AFTER_RETRIES=YES

■ **LINUX**

Step 1) vi 편집기를 이용하여 "/etc/pam.d/system-auth" 파일 열기

Step 2) 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
```

U-03 (상)	1. 계정관리 > 1.3 계정 잠금 임계값 설정

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

■ **AIX**

Step 1) vi 편집기를 이용하여 "/etc/security/user" 파일 열기

Step 2) 아래와 같이 수정 또는, 신규 삽입

(수정 전) `loginretries = 0`

(수정 후) `loginretries = 5`

■ **HP-UX**

- **HP-UX 11.v2 이하 버전 -**

Step 1) vi 편집기를 이용하여 /tcb/files/auth/system/default 파일 열기

Step 2) 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

- **HP-UX 11.v3 이상 버전 -**

Step 1) vi 편집기를 이용하여 `/etc/default/security` 파일 열기

Step 2) 아래와 같이 수정 또는, 신규 삽입

(수정 전) `#AUTH_MAXTRIES=0`

(수정 후) `AUTH_MAXTRIES=5`

※ Standard and Shadow modes only

조치 시 영향	HP-UX 경우 Trusted Mode로 전환 시 파일시스템 구조가 변경되어 운영 중인 서비스에 문제가 발생할 수 있으므로 충분한 테스트를 거친 후 Trusted Mode로의 전환이 필요함

UNIX 서버

U-04 (상)	1. 계정관리 > 1.4 패스워드 파일 보호
취약점 개요	
점검내용	■ 시스템의 사용자 계정(root, 일반계정) 정보가 저장된 파일(예 /etc/passwd, /etc/shadow)에 사용자 계정 패스워드가 암호화되어 저장되어 있는지 점검
점검목적	■ 일부 오래된 시스템의 경우 패스워드 정책이 적용되지 않아 /etc/passwd 파일에 평문으로 저장되므로 사용자 계정 패스워드가 암호화되어 저장되어 있는지 점검하여 비인가자의 패스워드 파일 접근 시에도 사용자 계정 패스워드가 안전하게 관리되고 있는지 확인하기 위함
보안위협	■ 비인가자에 의해 사용자 계정 패스워드가 평문으로 저장된 파일이 유출될 경우 시스템 사용자 계정 패스워드가 노출될 수 있음
참고	※ 관련 점검 항목 : U-07(상), U-08(상)
점검대상 및 판단기준	
대상	■ SOLARIS, LINUX, AIX, HP-UX 등
판단기준	**양호 :** 쉐도우 패스워드를 사용하거나, 패스워드를 암호화하여 저장하는 경우
	취약 : 쉐도우 패스워드를 사용하지 않고, 패스워드를 암호화하여 저장하지 않는 경우
조치방법	패스워드 암호화 저장·관리 설정 적용
점검 및 조치 사례	

OS별 점검 파일 위치 및 점검 방법	
SOLARIS, LINUX	Step 1) /shadow 파일 존재 확인 (일반적으로 /etc 디렉터리 내 존재) `#ls /etc` Step 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	/etc/security/passwd 파일 내 설정된 패스워드 점검
위에 제시한 설정이 적용되지 않은 경우 아래의 보안설정방법에 따라 설정을 변경함	

U-04 (상)	1. 계정관리 > 1.4 패스워드 파일 보호

■ **SOLARIS, LINUX**

Step 1) `#pwconv` ---> 쉐도우 패스워드 정책 적용 방법

Step 2) `#pwunconv` ---> 일반 패스워드 정책 적용 방법

■ **AIX**

AIX 서버는 기본적으로 "/etc/security/passwd" 파일에 패스워드를 암호화하여 저장·관리

■ **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

Step 1) Trusted Mode 전환 방법: root 계정으로 로그인한 후 아래 명령 수행

```
#/etc/tsconvert
```

Step 2) UnTrusted Mode 전환 방법: root 계정으로 로그인한 후 아래 명령 수행

```
#/etc/tsconvert -r2
```

조치 시 영향	HP-UX 경우 Trusted Mode로 전환 시 파일시스템 구조가 변경되어 운영 중인 서비스에 문제가 발생할 수 있으므로 충분한 테스트를 거친 후 Trusted Mode로의 전환 필요

UNIX 서버

U-05 (상)	2. 파일 및 디렉토리 관리 > 2.1 root홈, 패스 디렉터리 권한 및 패스 설정
취약점 개요	
점검내용	■ root 계정의 PATH 환경변수에 "."이 포함되어 있는지 점검
점검목적	■ 비인가자가 불법적으로 생성한 디렉터리를 우선으로 가리키지 않도록 설정하기 위해 환경변수 점검이 필요함
보안위협	■ 관리자가 명령어(예: ls, mv, cp등)를 수행했을 때 root 계정의 PATH 환경변수에 "." (현재 디렉터리 지칭)이 포함되어 있으면 현재 디렉터리에 명령어와 같은 이름의 악성파일이 실행되어 악의적인 행위가 일어날 수 있음
참고	※ **환경변수:** 프로세스가 컴퓨터에서 동작하는 방식에 영향을 미치는 동적인 값들의 집합으로 Path 환경변수는 실행파일을 찾는 경로에 대한 변수임
점검대상 및 판단기준	
대상	■ SOLARIS, LINUX, AIX, HP-UX 등
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
점검 및 조치 사례	

OS별 점검 파일 위치 및 점검 방법	
SOLARIS, LINUX, AIX, HP-UX	`#echo $PATH` `/usr/local/sbin:/sbin:/usr/sbin:/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	

U-05 (상)	2. 파일 및 디렉토리 관리 > 2.1 root홈, 패스 디렉터리 권한 및 패스 설정
■ **SOLARIS, LINUX, AIX, HP-UX** Step 1) vi 편집기를 이용하여 root 계정의 설정파일(~/.profile 과 /etc/profile) 열기 `#vi /etc/profile` Step 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

U-06 (상)	2. 파일 및 디렉토리 관리 > 2.2 파일 및 디렉터리 소유자 설정
취약점 개요	
점검내용	■ 소유자 불분명한 파일이나 디렉터리가 존재하는지 여부를 점검
점검목적	■ 소유자가 존재하지 않는 파일 및 디렉터리를 삭제 및 관리하여 임의의 사용자에 의한 불법적 행위를 사전에 차단하기 위함
보안위협	■ 삭제된 소유자의 UID와 동일한 사용자가 해당 파일, 디렉터리에 접근 가능하여 사용자 정보 등 중요 정보가 노출될 위험이 있음
참고	※ 소유자가 존재하지 않는 파일 및 디렉터리는 퇴직자의 자료이거나 관리 소홀로 인해 생긴 파일인 경우 또는 해킹으로 인한 공격자가 만들어 놓은 악의적인 파일인 경우가 있음
점검대상 및 판단기준	
대상	■ SOLARIS, LINUX, AIX, HP-UX 등
판단기준	**양호 :** 소유자가 존재하지 않는 파일 및 디렉터리가 존재하지 않는 경우
	취약 : 소유자가 존재하지 않는 파일 및 디렉터리가 존재하는 경우
조치방법	소유자가 존재하지 않는 파일 및 디렉터리 삭제 또는, 소유자 변경
점검 및 조치 사례	

OS별 점검 파일 위치 및 점검 방법	
SOLARIS, 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	

■ **SOLARIS, LINUX, AIX, HP-UX**

Step 1) 소유자가 존재하지 않는 파일이나 디렉터리가 불필요한 경우 rm 명령으로 삭제

```
#rm <file_name>
#rm <directory_name>
```

※ 삭제할 파일명 또는, 디렉터리명 입력

Step 2) 필요한 경우 chown 명령으로 소유자 및 그룹 변경

```
#chown <user_name> <file_name>
```

조치 시 영향	일반적인 경우 영향 없음

U-07 (상)	2. 파일 및 디렉토리 관리 > 2.3 /etc/passwd 파일 소유자 및 권한 설정
취약점 개요	
점검내용	■ /etc/passwd 파일 권한 적절성 점검
점검목적	■ /etc/passwd 파일을 통해 비인가자가 권한 상승하는 것을 막기 위함
보안위협	■ 관리자(root) 외 사용자가 "/etc/passwd" 파일의 변조가 가능할 경우 shell 변조, 사용자 추가/삭제, root를 포함한 사용자 권한 획득 시도 등 악의적인 행위가 가능함
참고	※ **/etc/passwd:** 사용자의 ID, 패스워드, UID, GID, 홈 디렉터리, 쉘 정보를 담고 있는 파일
점검대상 및 판단기준	
대상	■ SOLARIS, LINUX, AIX, HP-UX 등
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)
점검 및 조치 사례	

OS별 점검 파일 위치 및 점검 방법	
SOLARIS, LINUX, AIX, HP-UX	"/etc/passwd" 파일의 소유자 및 권한 확인 `#ls -l /etc/passwd` `rw-r—r— root <passwd 파일>`
"passwd" 파일의 소유자가 root가 아니거나 파일의 권한이 644 이하가 아닌 경우 아래의 보안설정방법에 따라 설정을 변경함	

■ **SOLARIS, LINUX, AIX, HP-UX**

"/etc/passwd" 파일의 소유자 및 권한 변경 (소유자 root, 권한 644)

```
#chown root /etc/passwd
#chmod 644 /etc/passwd
```

조치 시 영향	일반적인 경우 영향 없음

UNIX 서버

U-08 (상)	2. 파일 및 디렉토리 관리 > 2.4 /etc/shadow 파일 소유자 및 권한 설정
취약점 개요	
점검내용	■ /etc/shadow 권한 적절성 점검
점검목적	■ /etc/shadow 파일을 관리자만 제어할 수 있게 하여 비인가자들의 접근을 제한하도록 shadow 파일 소유자 및 권한을 관리해야함
보안위협	■ 해당 파일에 대한 권한 관리가 이루어지지 않을 시 ID 및 패스워드 정보가 외부로 노출될 수 있음
참고	※ **/etc/shadow:** 시스템에 등록된 모든 계정의 패스워드를 암호화된 형태로 저장 및 관리하고 있는 파일
점검대상 및 판단기준	
대상	■ SOLARIS, LINUX, AIX, HP-UX 등
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)
점검 및 조치 사례	

OS별 점검 파일 위치 및 점검 방법	
SOLARIS, 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	

■ SOLARIS, LINUX

Step 1) "/etc/shadow" 파일의 소유자 및 권한 확인

```
#ls -l /etc/shadow
```

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

```
#chown root /etc/shadow
#chmod 400 /etc/shadow
```

U-08 (상)	2. 파일 및 디렉토리 관리 > 2.4 /etc/shadow 파일 소유자 및 권한 설정

■ **AIX**

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

Step 1) /etc/security/passwd 디렉터리의 소유자 및 권한 확인

```
#ls -ld /etc/security/passwd
```

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

```
#chown root /etc/security/passwd
#chmod 400 /etc/security/passwd
```

■ **HP-UX**

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

Step 1) /tcb/files/auth 디렉터리의 소유자 및 권한 확인

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

Step 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

<table>
<tr><th>U-09 (상)</th><th>2. 파일 및 디렉토리 관리 > 2.5 /etc/hosts 파일 소유자 및 권한 설정</th></tr>
<tr><th colspan="2">취약점 개요</th></tr>
<tr><td>점검내용</td><td>■ /etc/hosts 파일의 권한 적절성 점검</td></tr>
<tr><td>점검목적</td><td>■ /etc/hosts 파일을 관리자만 제어할 수 있게 하여 비인가자들의 임의적인 파일 변조를 방지하기 위함</td></tr>
<tr><td>보안위협</td><td>■ hosts 파일에 비인가자 쓰기 권한이 부여된 경우, 공격자는 hosts파일에 악의적인 시스템을 등록하여, 이를 통해 정상적인 DNS를 우회하여 악성사이트로의 접속을 유도하는 파밍(Pharming) 공격 등에 악용될 수 있음</td></tr>
<tr><td>참고</td><td>※ /etc/hosts: IP 주소와 호스트네임을 매핑하는 파일. 일반적으로 인터넷 통신 시 주소를 찾기 위해 도메인 네임 서비스(DNS)보다 hosts 파일을 먼저 참조함. hosts 파일은 문자열 주소로부터 IP 주소를 수신받는 DNS 서버와는 달리, 파일 내에 직접 문자열 주소와 IP 주소를 매칭하여 기록하며, DNS 서버 접근 이전에 확인하여 해당 문자열 주소가 목록에 존재할 시 그 문자열 주소에 해당하는 IP 주소로 연결함
※ 파밍(Pharming): 사용자의 DNS 또는 hosts 파일을 번조함으로써 정상적인 사이트로 오인하여 접속하도록 유도한 뒤 개인정보를 훔치는 새로운 컴퓨터 범죄 수법</td></tr>
<tr><th colspan="2">점검대상 및 판단기준</th></tr>
<tr><td>대상</td><td>■ SOLARIS, LINUX, AIX, HP-UX 등</td></tr>
<tr><td rowspan="2">판단기준</td><td>양호 : /etc/hosts 파일의 소유자가 root이고, 권한이 600인 경우</td></tr>
<tr><td>취약 : /etc/hosts 파일의 소유자가 root가 아니거나, 권한이 600이 아닌 경우</td></tr>
<tr><td>조치방법</td><td>“/etc/hosts” 파일의 소유자 및 권한 변경 (소유자 root, 권한 600)</td></tr>
<tr><th colspan="2">점검 및 조치 사례</th></tr>
<tr><td colspan="2">
<table>
<tr><th colspan="2">OS별 점검 파일 위치 및 점검 방법</th></tr>
<tr><td>SOLARIS, LINUX, AIX, HP-UX</td><td># ls –l /etc/hosts
rw-———— root <hosts 파일></td></tr>
<tr><td colspan="2">“hosts” 파일의 소유자가 root가 아니거나 파일의 권한이 600이 아닌 경우 아래의 보안설정 방법에 따라 설정을 변경함</td></tr>
</table>
■ SOLARIS, LINUX, AIX, HP-UX
“/etc/hosts" 파일의 소유자 및 권한 변경 (소유자 root, 권한 600)
#chown root /etc/hosts
#chmod 600 /etc/hosts
</td></tr>
<tr><td>조치 시 영향</td><td>일반적인 경우 영향 없음</td></tr>
</table>

U-10 (상)	2. 파일 및 디렉토리 관리 > 2.6 /etc/(x)inetd.conf 파일 소유자 및 권한 설정
취약점 개요	
점검내용	■ /etc/(x)inetd.conf 파일 권한 적절성 점검
점검목적	■ /etc/(x)inetd.conf 파일을 관리자만 제어할 수 있게 하여 비인가자들의 임의적인 파일 변조를 방지하기 위함
보안위협	■ (x)inetd.conf 파일에 비인가자의 쓰기 권한이 부여되어 있을 경우, 비인가자가 악의적인 프로그램을 등록하여 root 권한으로 불법적인 서비스를 실행할 수 있음
참고	※ **인터넷 슈퍼데몬:** 외부 네트워크의 요청이 있을 때 "/etc/inetd.conf"에 등록된 내부 프로그램인 인터넷 서비스들의 데몬을 실행시켜주는 역할을 함
점검대상 및 판단기준	
대상	■ SOLARIS, LINUX, AIX, HP-UX 등
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/(x)inetd.conf" 파일의 소유자 및 권한 변경 (소유자 root, 권한 600)
점검 및 조치 사례	

OS별 점검 파일 위치 및 점검 방법	
SOLARIS, 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 디렉터리 내 모든 파일>`
인터넷 슈퍼데몬 서비스 설정파일의 소유자가 root가 아니거나 파일의 권한이 600이 아닌 경우 아래의 보안설정방법에 따라 설정을 변경함	

■ **SOLARIS, 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
```

UNIX 서버

U-10 (상)	2. 파일 및 디렉토리 관리 > 2.6 /etc/(x)inetd.conf 파일 소유자 및 권한 설정
■ **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

U-11 (상)	2. 파일 및 디렉토리 관리 > 2.7 /etc/syslog.conf 파일 소유자 및 권한 설정
취약점 개요	
점검내용	■ /etc/syslog.conf 파일 권한 적절성 점검
점검목적	■ /etc/syslog.conf 파일의 권한 적절성을 점검하여, 관리자 외 비인가자의 임의적인 syslog.conf 파일 변조를 방지하기 위함
보안위협	■ syslog.conf 파일의 접근권한이 적절하지 않을 경우, 임의적인 파일 변조로 인해 침입자의 흔적 또는, 시스템 오류 사항을 분석하기 위해 반드시 필요한 시스템 로그가 정상적으로 기록 되지 않을 수 있음
참고	※ **/etc/syslog.conf:** 시스템 운영 중 발생하는 주요 로그 기록을 설정하는 파일
점검대상 및 판단기준	
대상	■ SOLARIS, LINUX, AIX, HP-UX 등
판단기준	**양호 :** /etc/syslog.conf 파일의 소유자가 root(또는 bin, sys)이고, 권한이 644 이하인 경우
	취약 : /etc/syslog.conf 파일의 소유자가 root(또는 bin, sys)가 아니거나, 권한이 644 이하가 아닌 경우
조치방법	"/etc/syslog.conf" 파일의 소유자 및 권한 변경 (소유자 root(또는 bin, sys), 권한 644 이하)
점검 및 조치 사례	

OS별 점검 파일 위치 및 점검 방법	
SOLARIS, 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	

■ SOLARIS, LINUX, AIX, HP-UX

Step 1) "/etc/syslog.conf" 파일의 소유자 및 권한 변경 (소유자 root, 권한 644)

```
#chown root /etc/syslog.conf
#chmod 644 /etc/syslog.conf
```

■ LINUX (CentOS 6 이상일 경우)

```
#chown root /etc/rsyslog.conf
#chmod 644 /etc/rsyslog.conf
```

※ HP-UX 11이상 버전에서는 syslog.conf 소유가 bin 으로 나타남

조치 시 영향	root, bin, sys 등 시스템에서 사용하는 계정이 아닌 일반 계정에게 소유 권한이 부여되지 않도록 하여야 함

UNIX 서버

U-12 (상)	2. 파일 및 디렉토리 관리 > 2.8 /etc/services 파일 소유자 및 권한 설정
취약점 개요	
점검내용	■ /etc/services 파일 권한 적절성 점검
점검목적	■ /etc/services 파일을 관리자만 제어할 수 있게 하여 비인가자들의 임의적인 파일 변조를 방지하기 위함
보안위협	■ services 파일의 접근권한이 적절하지 않을 경우 비인가 사용자가 운영 포트 번호를 변경하여 정상적인 서비스를 제한하거나, 허용되지 않은 포트를 오픈하여 악성 서비스를 의도적으로 실행할 수 있음
참고	※ **/etc/services:** 서비스 관리를 위해 사용되는 파일. 해당 파일에 서버에서 사용하는 모든 포트(port)들에 대해 정의되어 있으며, 필요시 서비스 기본사용 포트를 변경하여 네트워크 서비스를 운용할 수 있음
점검대상 및 판단기준	
대상	■ SOLARIS, LINUX, AIX, HP-UX 등
판단기준	**양호 :** /etc/syslog.conf 파일의 소유자가 root(또는 bin, sys)이고, 권한이 644 이하인 경우
	취약 : /etc/syslog.conf 파일의 소유자가 root(또는 bin, sys)가 아니거나, 권한이 644 이하가 아닌 경우
조치방법	"/etc/syslog.conf" 파일의 소유자 및 권한 변경 (소유자 root(또는 bin, sys), 권한 644 이하)
점검 및 조치 사례	

OS별 점검 파일 위치 및 점검 방법	
SOLARIS, 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	

■ SOLARIS, 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

U-13 (상)	2. 파일 및 디렉토리 관리 > 2.9 SUID, SGID, Sticky bit 설정 및 권한 설정
취약점 개요	
점검내용	■ 불필요하거나 악의적인 파일에 SUID, SGID 설정 여부 점검
점검목적	■ 불필요한 SUID, SGID 설정 제거로 악의적인 사용자의 권한상승을 방지하기 위함
보안위협	■ SUID, SGID 파일의 접근권한이 적절하지 않을 경우 SUID, SGID 설정된 파일로 특정 명령어를 실행하여 root 권한 획득 및 정상서비스 장애를 발생시킬 수 있음
참고	※ **SUID:** 설정된 파일 실행 시, 특정 작업 수행을 위하여 일시적으로 파일 소유자의 권한을 얻게 됨 ※ **SGID:** 설정된 파일 실행 시, 특정 작업 수행을 위하여 일시적으로 파일 소유 그룹의 권한을 얻게 됨 ※ 불필요한 SUID/SGID 목록: 부록 참고
점검대상 및 판단기준	
대상	■ SOLARIS, LINUX, AIX, HP-UX 등
판단기준	**양호 :** 주요 실행파일의 권한에 SUID와 SGID에 대한 설정이 부여되어 있지 않은 경우
	취약 : 주요 실행파일의 권한에 SUID와 SGID에 대한 설정이 부여되어 있는 경우
조치방법	Step 1) 불필요한 SUID, SGID 파일 제거 Step 2) 아래의 목록 이외에 애플리케이션에서 생성한 파일이나, 사용자가 임의로 생성한 파일 등 의심스럽거나 특이한 파일의 발견 시 SUID 제거 필요
점검 및 조치 사례	

OS별 점검 파일 위치 및 점검 방법	
SOLARIS, LINUX, AIX, HP-UX	OS별 주요 실행파일에 대한 SUID/SGID 설정 여부 확인 (※ 불필요한 SUID/SGID 목록: 부록 참고) `#ls –alL [check_file] | awk '{ print $1}' | grep –i 's'`
주요 파일에 불필요한 SUID/SGID가 설정된 경우 아래의 보안설정방법에 따라 SUID/SGID를 제거함	

■ **SOLARIS, LINUX, AIX, HP-UX**

Step 1) 제거 방법

```
#chmod -s <file_name>
```

Step 2) 주기적인 감사 방법

```
#find / -user root -type f \( -perm -04000 -o -perm -02000 \) -xdev
-exec ls –al {} \;
```

UNIX 서버

U-13 (상)	2. 파일 및 디렉토리 관리 > 2.9 SUID, SGID, Sticky bit 설정 및 권한 설정
Step 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>`	
조치 시 영향	SUID 제거 시 OS 및 응용 프로그램 등 서비스 정상작동 유무 확인 필요

U-14 (상)	2. 파일 및 디렉토리 관리 > 2.10 사용자, 시스템 시작파일 및 환경파일 소유자 및 권한 설정
취약점 개요	
점검내용	■ 홈 디렉터리 내의 환경변수 파일에 대한 소유자 및 접근권한이 관리자 또는 해당 계정으로 설정되어 있는지 점검
점검목적	■ 비인가자의 환경변수 조작으로 인한 보안 위험을 방지하기 위함
보안위협	■ 홈 디렉터리 내의 사용자 파일 및 사용자별 시스템 시작파일 등과 같은 환경변수 파일의 접근권한 설정이 적절하지 않을 경우 비인가자가 환경변수 파일을 변조하여 정상 사용중인 사용자의 서비스가 제한 될 수 있음
참고	※ **환경변수 파일 종류:** ".profile", ".kshrc", ".cshrc", ".bashrc", ".bash_profile", ".login", ".exrc", ".netrc" 등
점검대상 및 판단기준	
대상	■ SOLARIS, LINUX, AIX, HP-UX 등
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
점검 및 조치 사례	

OS별 점검 파일 위치 및 점검 방법	
SOLARIS, 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	

■ SOLARIS, LINUX, AIX , HP-UX

Step 1) 소유자 변경 방법

```
#chown <user_name> <file_name>
```

Step 2) 일반 사용자 쓰기 권한 제거 방법

```
#chmod o-w <file_name>
```

조치 시 영향	일반적인 경우 영향 없음

UNIX 서버

<table>
<tr><th>U-15 (상)</th><th>2. 파일 및 디렉토리 관리 > 2.11 world writable 파일 점검</th></tr>
<tr><th colspan="2">취약점 개요</th></tr>
<tr><td>점검내용</td><td>■ 불필요한 world writable 파일 존재 여부 점검</td></tr>
<tr><td>점검목적</td><td>■ world writable 파일을 이용한 시스템 접근 및 악의적인 코드 실행을 방지하기 위함</td></tr>
<tr><td>보안위협</td><td>■ 시스템 파일과 같은 중요 파일에 world writable 설정이 될 경우, 악의적인 사용자가 해당 파일을 마음대로 파일을 덧붙이거나 지울 수 있게 되어 시스템의 무단 접근 및 시스템 장애를 유발할 수 있음</td></tr>
<tr><td>참고</td><td>※ world writable 파일: 파일의 내용을 소유자나 그룹 외 모든 사용자에 대해 쓰기가 허용된 파일</td></tr>
<tr><th colspan="2">점검대상 및 판단기준</th></tr>
<tr><td>대상</td><td>■ SOLARIS, LINUX, AIX, HP-UX 등</td></tr>
<tr><td rowspan="2">판단기준</td><td>양호 : world writable 파일이 존재하지 않거나, 존재 시 설정 이유를 확인하고 있는 경우</td></tr>
<tr><td>취약 : world writable 파일이 존재하나 해당 설정 이유를 확인하고 있지 않는 경우</td></tr>
<tr><td>조치방법</td><td>world writable 파일 존재 여부를 확인하고 불필요한 경우 제거</td></tr>
<tr><th colspan="2">점검 및 조치 사례</th></tr>
<tr><td colspan="2">
<table>
<tr><th colspan="2">OS별 점검 파일 위치 및 점검 방법</th></tr>
<tr><td>SOLARIS, LINUX, AIX, HP-UX</td><td>world writable 파일 존재 여부 확인
<code>#find / -type f -perm -2 -exec ls -l {} \;</code></td></tr>
<tr><td colspan="2">“world writable” 파일 존재 시 사용 목적을 확실히 알고 불필요 시 삭제, 필요 시 아래의 보안설정방법에 따라 설정을 변경함</td></tr>
</table>

■ SOLARIS, LINUX, AIX, HP-UX
Step 1) 일반 사용자 쓰기 권한 제거 방법
<code>#chmod o-w <file_name></code>
Step 2) 파일 삭제 방법
<code>#rm -rf <world-writable 파일명></code>
</td></tr>
<tr><td>조치 시 영향</td><td>일반적인 경우 영향 없음</td></tr>
</table>

U-16 (상)	2. 파일 및 디렉토리 관리 > 2.12 /dev에 존재하지 않는 device 파일 점검
취약점 개요	
점검내용	■ 존재하지 않는 device 파일 존재 여부 점검
점검목적	■ 실제 존재하지 않는 디바이스를 찾아 제거함으로써 root 파일 시스템 손상 및 다운 등의 문제를 방지하기 위함
보안위협	■ 공격자는 rootkit 설정파일들을 서버 관리자가 쉽게 발견하지 못하도록 /dev에 device 파일인 것처럼 위장하는 수법을 많이 사용함
참고	※ **/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 ※ /dev 디렉터리 내 불필요한 device 파일이 존재할 시 삭제 권고
점검대상 및 판단기준	
대상	■ SOLARIS, LINUX, AIX, HP-UX 등
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
점검 및 조치 사례	

OS별 점검 파일 위치 및 점검 방법	
SOLARIS, 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	

■ SOLARIS, LINUX, AIX, HP-UX

Step 1) /dev 디렉터리 파일 점검

```
#find /dev -type f -exec ls -l {} \;
```

Step 2) major, minor number를 가지지 않는 device일 경우 삭제

조치 시 영향	일반적인 경우 영향 없음

UNIX 서버

U-17 (상)	2. 파일 및 디렉토리 관리 > 2.13 $HOME/.rhosts, hosts.equiv 사용 금지
취약점 개요	
점검내용	■ /etc/hosts.equiv 파일 및 .rhosts 파일 사용자를 root 또는, 해당 계정으로 설정한 뒤 권한을 600으로 설정하고 해당파일 설정에 '+' 설정(모든 호스트 허용)이 포함되지 않도록 설정되어 있는지 점검
점검목적	■ 'r' command 사용을 통한 원격 접속은 인증 없이 관리자 원격접속이 가능하므로 서비스 포트를 차단해야 함
보안위협	■ rlogin, rsh 등과 같은 'r' command의 보안 설정이 적용되지 않은 경우, 원격지의 공격자가 관리자 권한으로 목표 시스템상의 임의의 명령을 수행시킬 수 있으며, 명령어 원격 실행을 통해 중요 정보 유출 및 시스템 장애를 유발시킬 수 있음. 또한 공격자 백도어 등으로도 활용될 수 있음
참고	※ **'r'command:** 인증 없이 관리자의 원격접속을 가능하게 하는 명령어들로 rsh(remsh), rlogin, rexec 등이 있으며, 포트번호 512,513,514 (TCP)를 사용함
점검대상 및 판단기준	
대상	■ SOLARIS, LINUX, AIX, HP-UX 등
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	Step 1) /etc/hosts.equiv 및 $HOME/.rhosts 파일 소유자를 root 또는, 해당 계정으로 변경 Step 2) /etc/hosts.equiv 및 $HOME/.rhosts 파일 권한을 600 이하로 변경 Step 3) /etc/hosts.equiv 및 $HOME/.rhosts 파일에서 "+"를 제거하고 반드시 필요한 호스트 및 계정만 등록 (해당 내역 요청)

U-17 (상)	2. 파일 및 디렉토리 관리 > 2.13 $HOME/.rhosts, hosts.equiv 사용 금지

점검 및 조치 사례

OS별 점검 파일 위치 및 점검 방법	
SOLARIS, LINUX, AIX, HP-UX	Step 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>` Step 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	

■ SOLARIS, LINUX, AIX, HP-UX

Step 1) "/etc/hosts.equiv" 및 "$HOME/.rhosts" 파일의 소유자를 root 또는, 해당 계정으로 변경

```
#chown root /etc/hosts.equiv
#chown <user_name> $HOME/.rhosts
```

Step 2) "/etc/hosts.equiv" 및 "$HOME/.rhosts" 파일의 권한을 600 이하로 변경

```
#chmod 600 /etc/hosts.equiv
#chmod 600 $HOME/.rhosts
```

Step 3) "/etc/hosts.equiv" 및 "$HOME/.rhosts" 파일에서 "+"를 제거하고 허용 호스트 및 계정 등록

```
#cat /etc/hosts.equiv (or $HOME/.rhosts)
```

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

조치 시 영향	일반적인 경우 영향 없음

UNIX 서버

U-18 (상)	2. 파일 및 디렉토리 관리 > 2.14 접속 IP 및 포트 제한
취약점 개요	
점검내용	■ 허용할 호스트에 대한 접속 IP 주소 제한 및 포트 제한 설정 여부 점검
점검목적	■ 허용한 호스트만 서비스를 사용하게 하여 서비스 취약점을 이용한 외부자 공격을 방지하기 위함
보안위협	■ 허용할 호스트에 대한 IP 및 포트제한이 적용되지 않은 경우, Telnet, FTP같은 보안에 취약한 네트워크 서비스를 통하여 불법적인 접근 및 시스템 침해사고가 발생할 수 있음
참고	▪ 접속 IP 및 포트제한 애플리케이션 종류 예시 ※ **TCP Wrapper:** 네트워크 서비스에 관련한 트래픽을 제어하고 모니터링 할 수 있는 UNIX 기반의 방화벽 툴 ※ **IPFilter:** 유닉스 계열에서 사용하는 공개형 방화벽 프로그램으로써 Packet Filter로 시스템 및 네트워크 보안에 아주 강력한 기능을 보유한 프로그램 ※ **IPtables:** 리눅스 커널 방화벽이 제공하는 테이블들과 그것을 저장하는 체인, 규칙들을 구성할 수 있게 해주는 응용프로그램
점검대상 및 판단기준	
대상	■ SOLARIS, LINUX, AIX, HP-UX 등
판단기준	**양호 :** 접속을 허용할 특정 호스트에 대한 IP 주소 및 포트 제한을 설정한 경우
	취약 : 접속을 허용할 특정 호스트에 대한 IP 주소 및 포트 제한을 설정하지 않은 경우
조치방법	OS에 기본으로 제공하는 방화벽 애플리케이션이나 TCP Wrapper와 같은 호스트별 서비스 제한 애플리케이션을 사용하여 접근 허용 IP 등록
점검 및 조치 사례	

OS별 점검 파일 위치 및 점검 방법	
SOLARIS, LINUX, AIX	1. TCP Warrper 사용할 경우 All deny 적용 확인 및 접근 허용 IP 적절성 확인 `#cat /etc/hosts.deny` `#cat /etc/hosts.allow` 2. IPtables 사용할 경우 (Linux) `#iptalbes -L` 3. IPfilter 사용할 경우 (SOLARIS) `#cat /etc/ipf/ipf.conf` 4. TCP Warrper (SOLARIS 10 이상) `# inetadm -p`

U-18 (상)	2. 파일 및 디렉토리 관리 > 2.14 접속 IP 및 포트 제한

	tcp_wrappers=true <- 현재 실행되어 있는 상태 tcp_wrappers=false <- 현재 정지된 상태
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	

■ IPtables 사용하는 경우

Step 1) iptables 명령어를 통해 접속할 IP 및 포트 정책 추가

(예) SSH 서비스 제한

```
#iptables –A INPUT –p tcp –s 192.168.1.0/24 ––dport 22 –j ACCEPT
#iptables -A INPUT -p tcp --dport 22 -j DROP
```

Step 2) iptables 설정 저장

```
#/etc/rc.d/init.d/iptables save
```

■ IPfilter 사용하는 경우

Step 1) vi 편집기를 이용하여 "/etc/ipf/ipf.conf" 파일 열기

Step 2) 접속할 IP 및 포트 정책 추가

(예) SSH 서비스 제한

```
pass in quick proto tcp from 192.168.1.0/24 to any port = 22 keep
state
block in quick proto tcp from any to any port = 22 keep state
```

Step 3) IPfilter 서비스 재시작

■ TCP Wrapper 사용하는 경우

Step 1) vi 편집기를 이용하여 "/etc/hosts.deny" 파일 열기 (해당 파일이 없을 경우 새로 생성)

Step 2) 아래와 같이 수정 또는, 신규 삽입 (ALL Deny 설정)

(수정 전) 설정 없음

(수정 후) ALL:ALL

Step 3) vi 편집기를 이용하여 "/etc/hosts.allow" 파일 열기 (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)

U-18 (상)	2. 파일 및 디렉토리 관리 > 2.14 접속 IP 및 포트 제한

< 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

■ 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

Step 1) vi 편집기를 이용하여 "/var/adm/inetd.sec" 파일 열기
(해당 파일이 없을 경우 새로 생성)

Step 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 서비스 사용이 불가함

U-19 (상)	3. 서비스 관리 > 3.1 Finger 서비스 비활성화
취약점 개요	
점검내용	■ finger 서비스 비활성화 여부 점검
점검목적	■ Finger(사용자 정보 확인 서비스)를 통해서 네트워크 외부에서 해당 시스템에 등록된 사용자 정보를 확인할 수 있어 비인가자에게 사용자 정보가 조회되는 것을 차단하고자 함
보안위협	■ 비인가자에게 사용자 정보가 조회되어 패스워드 공격을 통한 시스템 권한 탈취 가능성이 있으므로 사용하지 않는다면 해당 서비스를 중지하여야 함
참고	※ **Finger(사용자 정보 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
점검대상 및 판단기준	
대상	■ SOLARIS, Linux, AIX, HP-UX 등
판단기준	**양호 :** Finger 서비스가 비활성화 되어 있는 경우
	취약 : Finger 서비스가 활성화 되어 있는 경우
조치방법	Finger 서비스 비활성화
점검 및 조치 사례	

OS별 점검 파일 위치 및 점검 방법	
LINUX, AIX, HP-UX, SOLARIS 5.9 이하 버전	`#cat /etc/inetd.conf` `#finger stream tcp nowait bin /usr/lbin/fingered fingerd` 주석처리 확인
SOLARIS 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, SOLARIS 5.9 이하 버전

Step 1) "/etc/inetd.conf" 파일에서 finger 서비스 라인 #처리(주석처리)

(수정 전) `finger stream tcp nowait bin /usr/lbin/fingered fingerd`

(수정 후) `#finger stream tcp nowait bin /usr/lbin/fingered fingerd`

U-19 (상)	3. 서비스 관리 > 3.1 Finger 서비스 비활성화

Step 2) inetd 서비스 재시작

```
#ps -ef | grep inetd
 root 141 1 0 15:03:22 ? 0:01 /usr/sbin/inetd -s
#kill -HUP [PID]
```

■ **SOLARIS 5.10 이상 버전**

inetadm –d "중지하고자 하는 데몬" 명령으로 서비스 데몬 중지

```
#inetadm -d svc:/network/finger:default
```

■ **LINUX (xinetd일 경우)**

Step 1) vi 편집기를 이용하여 "/etc/xinetd.d/finger" 파일 열기

Step 2) 아래와 같이 설정 (Disable = yes 설정)

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

Step 3) xinetd 서비스 재시작

```
#service xinetd restart
```

조치 시 영향	일반적인 경우 영향 없음

U-20 (상)	3. 서비스 관리 > 3.2 Anonymous FTP 비활성화
취약점 개요	
점검내용	■ 익명 FTP 접속 허용 여부 점검
점검목적	■ 실행중인 FTP 서비스에 익명 FTP 접속이 허용되고 있는지 확인하여 접속허용을 차단하는 것을 목적으로 함
보안위협	■ Anonymous FTP(익명 FTP)를 사용 시 anonymous 계정으로 로그인 후 디렉터리에 쓰기 권한이 설정되어 있다면 악의적인 사용자가 local exploit을 사용하여 시스템에 대한 공격을 가능하게 함
참고	※ **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
점검대상 및 판단기준	
대상	■ SOLARIS, Linux, AIX, HP-UX 등
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
점검 및 조치 사례	

OS별 점검 파일 위치 및 점검 방법	
SOLARIS, 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	

■ SOLARIS, LINUX, AIX, HP-UX

Step 1) 일반 FTP - Anonymous FTP 접속 제한 설정 방법
"/etc/passwd" 파일에서 ftp 또는, anonymous 계정 삭제
- SOLARIS, LINUX, HP-UX 설정: `#userdel ftp`
- AIX 설정: `#rmuser ftp`

Step 2) ProFTP - Anonymous FTP 접속 제한 설정 방법
"/etc/passwd" 파일에서 ftp 계정 삭제
- SOLARIS, LINUX, HP-UX 설정: `#userdel ftp`
- AIX 설정: `#rmuser ftp`

Step 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

<table>
<tr><th>U-21 (상)</th><th>3. 서비스 관리 > 3.3 r 계열 서비스 비활성화</th></tr>
<tr><td colspan="2">취약점 개요</td></tr>
<tr><td>점검내용</td><td>■ r command 서비스 비활성화 여부 점검</td></tr>
<tr><td>점검목적</td><td>■ ‘r’command 사용을 통한 원격 접속은 NET Backup이나 다른 용도로 사용되기도 하나, 인증 없이 관리자 원격접속이 가능하여 이에 대한 보안위협을 방지하고자 함</td></tr>
<tr><td>보안위협</td><td>■ 서비스 포트가 열려있을 경우, 비인가자에 의한 중요 정보 유출 및 시스템 장애 발생 등 침해사고의 원인이 될 수 있음</td></tr>
<tr><td>참고</td><td>※ ‘r’command: 인증 없이 관리자의 원격접속을 가능하게 하는 명령어들로 rsh(remsh), rlogin, rexec 등이 있음</td></tr>
<tr><td colspan="2">점검대상 및 판단기준</td></tr>
<tr><td>대상</td><td>■ SOLARIS, Linux, AIX, HP-UX 등</td></tr>
<tr><td rowspan="2">판단기준</td><td>양호 : 불필요한 r 계열 서비스가 비활성화 되어 있는 경우</td></tr>
<tr><td>취약 : 불필요한 r 계열 서비스가 활성화 되어 있는 경우</td></tr>
<tr><td>조치방법</td><td>NET Backup등 특별한 용도로 사용하지 않는다면 아래의 서비스 중지
<table>
<tr><td>shell(514)</td><td>login(513)</td><td>exec(512)</td></tr>
</table>
</td></tr>
<tr><td colspan="2">점검 및 조치 사례</td></tr>
<tr><td colspan="2">
<table>
<tr><th colspan="2">OS별 점검 파일 위치 및 점검 방법</th></tr>
<tr><td>SOLARIS 5.9
이하 버전</td><td>‘r’command 서비스 활성화 여부 확인
<code>#vi /etc/inetd.conf</code></td></tr>
<tr><td>AIX</td><td><code>#cat /etc/inetd.conf | grep rlogin</code> (# 처리 되어 있으면 비활성화)
<code>#cat /etc/inetd.conf | grep rsh</code> (# 처리 되어 있으면 비활성화)</td></tr>
<tr><td>HP-UX</td><td><code>#vi /etc/inetd.conf</code>
r로 시작하는 필드 존재 시 취약</td></tr>
<tr><td>SOLARIS 5.10
이상 버전</td><td><code>#inetadm | egrep "shell|rlogin|rexec"</code>
r'command 관련 데몬 확인</td></tr>
<tr><td>LINUX
(xinetd일 경우)</td><td>rsh, rlogin, rexec (shell, login, exec) 서비스 구동 확인
<code>#ls alL /etc/xinetd.d/* | egrep "rsh|rlogin|rexec" | egrep -v "grep|klogin|kshell|kexec"</code></td></tr>
<tr><td colspan="2">위에 제시된 파일 내 "r 계열" 서비스가 활성화 된 경우 아래의 보안설정방법에 따라 서비스 중지</td></tr>
</table>
</td></tr>
</table>

U-21 (상)	3. 서비스 관리 > 3.3 r 계열 서비스 비활성화

■ **SOLARIS 5.9 이하, HP-UX**

Step 1) r 계열 서비스 활성화 여부 확인

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

Step 2) r로 시작하는 필드 주석처리 후 재가동

(수정 전)

```
shell     stream    tcp     nowait    root    /usr/sbin/in.rshd      in.rshd
shell     stream    tcp6    nowait    root    /usr/sbin/in.rshd      in.rshd
login     stream    tcp     nowait    root    /usr/sbin/in.rlogin.d  in.rlogind
exec      stream    tcp     nowait    root    /usr/sbin/in.rexecd    in.rexecd
exec      stream    tcp6    nowait    root    /usr/sbin/in.rexecd    in.rexecd
```

(수정 후)

```
#shell    stream    tcp     nowait    root    /usr/sbin/in.rshd      in.rshd
#shell    stream    tcp     nowait    root    /usr/sbin/in.rshd      in.rshd
#shell    stream    tcp6    nowait    root    /usr/sbin/in.rshd      in.rshd
#login    stream    tcp6    nowait    root    /usr/sbin/in.rlogind   in.rlogind
#exec     stream    tcp     nowait    root    /usr/sbin/in.rexecd    in.rexecd
#exec     stream    tcp6    nowait    root    /usr/sbin/in.rexecd    in.rexecd
```

SOLARIS) `# kill -HUP [inetd PID]`

HP-UX) `# inetd -c`

■ **AIX**

Step 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)

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

Step 2) /etc/hosts.equiv 파일은 TRUSTED 시스템을 등록

Step 3) .rhosts 파일은 사용자 별로 'r'command를 통해 접근이 가능하도록 설정할 수 있음 ($HOME/.rhosts)

U-21 (상)	3. 서비스 관리 > 3.3 r 계열 서비스 비활성화

■ **SOLARIS 5.10 이상 버전**

Step 1) r'command 관련 데몬 확인

```
• svc:/network/login:rlogin
• svc:/network/rexec:default
• svc:/network/shell:kshell
```

Step 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)**

Step 1) vi 편집기를 이용하여 "/etc/xinetd.d/" 디렉터리 내 rlogin, rsh, rexec 파일 열기

Step 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/sdin/in.fingerd
          disable                 = yes
}
```

Step 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 해당파일 내에 설정이 없다면 사용하지 않는 것으로 파악

U-22 (상)	3. 서비스 관리 > 3.4 cron 파일 소유자 및 권한 설정
취약점 개요	
점검내용	■ Cron 관련 파일의 권한 적절성 점검
점검목적	■ 비인가자가 allow, deny 파일에 접근할 수 없도록 설정하고 있는지 점검하는 것을 목적으로 함
보안위협	■ root 외 일반사용자에게도 crontab 명령어를 사용할 수 있도록 할 경우, 고의 또는 실수로 불법적인 예약 파일 실행으로 시스템 피해를 일으킬 수 있음
참고	※ **Cron 시스템:** 특정 작업을 정해진 시간에 주기적이고 반복적으로 실행하기 위한 데몬과 그 설정들을 말함 ※ **cron.allow:** 해당 파일에 사용자 ID를 등록하면 등록된 사용자는 crontab 명령어 사용이 가능함 ※ **cron.deny:** 해당 파일에 사용자 ID를 등록하면 등록된 사용자는 crontab 명령어 사용이 불가능함
점검대상 및 판단기준	
대상	■ SOLARIS, Linux, AIX, HP-UX 등
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)
점검 및 조치 사례	

OS별 점검 방법	
SOLARIS, 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/*
SOLARIS	/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	

UNIX 서버

U-22 (상)	3. 서비스 관리 > 3.4 cron 파일 소유자 및 권한 설정

■ **SOLARIS**

Step 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
```

Step 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**

Step 1) "/etc/cron.allow" 및 "/etc/cron.deny" 파일의 소유자 및 권한 확인

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

Step 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**

Step 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
```

Step 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

U-23 (상)	3. 서비스 관리 > 3.5 DoS 공격에 취약한 서비스 비활성화
취약점 개요	
점검내용	■ 사용하지 않는 Dos 공격에 취약한 서비스의 실행 여부 점검
점검목적	■ 시스템 보안성을 높이기 위해 취약점이 많이 발표된 echo, discard, daytime, chargen, ntp, snmp 등 서비스를 중지함
보안위협	■ 해당 서비스가 활성화되어 있는 경우 시스템 정보 유출 및 DoS(서비스 거부 공격)의 대상이 될 수 있음
참고	※ **DoS(Denial of Service attack):** 시스템을 악의적으로 공격해 해당 시스템의 자원을 부족하게 하여 원래 의도된 용도로 사용하지 못하게 하는 공격. 특정 서버에게 수많은 접속 시도를 만들어 다른 이용자가 정상적으로 서비스 이용을 하지 못하게 하거나, 서버의 TCP 연결을 바닥내는 등의 공격이 이 범위에 포함됨
점검대상 및 판단기준	
대상	■ SOLARIS, Linux, AIX, HP-UX 등
판단기준	**양호 :** 사용하지 않는 DoS 공격에 취약한 서비스가 비활성화 된 경우
	취약 : 사용하지 않는 DoS 공격에 취약한 서비스가 활성화 된 경우
조치방법	echo, discard, daytime, charge, ntp, dns, snmp 등 서비스 비활성화 설정
점검 및 조치 사례	

OS별 점검 파일 위치 및 점검 방법	
SOLARIS	`#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
SOLARIS 5.10 이상 버전	`#inetadm | grep enable | egrep "echo|discard|daytime|chargen"` 명령으로 기타 서비스 데몬 확인
아래 제시된 DoS 공격에 취약한 서비스 중 사용하지 않는 서비스가 활성화 된 경우 아래의 보안설정방법에 따라 서비스 중지	

UNIX 서버

U-23 (상)	3. 서비스 관리 > 3.5 DoS 공격에 취약한 서비스 비활성화

DoS 공격에 취약한 서비스 예시	
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
NTP(123)	네트워크로 연결되어 있는 컴퓨터들끼리 클록 시각을 동기화시키는데 사용되는 서비스
DNS(53)	호스트의 도메인 이름을 호스트의 네트워크 주소로 바꾸거나 그 반대의 변환을 수행하는데 사용되는 서비스
SNMP(161/162)	네트워크 장비들로부터 필요한 정보를 가져와 장비 상태를 모니터링 하거나 설정값을 변경하는 등의 작업을 하여 네트워크 장비를 관리하는데 사용되는 서비스
SMTP(25)	인터넷에서 메일을 보내기 위해 사용되는 서비스

※ 일반적으로 사용하지 않는 서비스인 echo, discard, daytime, chargen 비활성화 방법

■ SOLARIS

Step 1) echo 서비스 비활성화 설정

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

Step 2) discard 서비스 비활성화 설정

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

Step 3) daytime 서비스 비활성화 설정

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

Step 4) chargen 서비스 비활성화 설정

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

U-23 (상)	3. 서비스 관리 > 3.5 DoS 공격에 취약한 서비스 비활성화

■ **AIX**

Step 1) vi편집기를 이용하여 echo, discard, daytime, chargen 필드 주석처리

```
#vi /etc/inetd.conf
<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
#echo       dgram     udp    wait     root      internal
#discard    dgram     udp    wait     root      internal
#chargen    dgram     udp    wait     root      internal
#daytime    dgram     udp    wait     root      internal
```

Step 2) 필드 주석처리 후 재가동

```
#refresh -s inetd
```

■ **HP-UX**

Step 1) vi편집기를 이용하여 echo, discard, daytime, chargen 필드 주석처리

```
#vi /etc/inetd.conf
<inetd.conf>
#daytime    stream    udp6   nowait   root      internal
#daytime    dgram     udp6   nowait   root      internal
#echo       stream    tcp6   nowait   root      internal
#echo       dgram     udp6   nowait   root      internal
#discard    stream    tcp6   nowait   root      internal
#discard    dgram     udp6   nowait   root      internal
#chargen    stream    tcp6   nowait   root      internal
#chargen    dgram     udp6   nowait   root      internal
```

Step 2) 필드 주석처리 후 재가동

```
# inetd -c
```

■ **SOLARIS 5.10 이상 버전**

Step 1) 기타 서비스 데몬 확인

```
#inetadm | grep echo
 enabled   online    svc:/network/echo:dgram
 enabled   online    svc:/network/echo:stream
```

U-23 (상)	3. 서비스 관리 > 3.5 DoS 공격에 취약한 서비스 비활성화

```
#inetadm | grep daytime
 enabled   online    svc:/network/daytime:dgram
 enabled   online    svc:/network/daytime:stream
#inetadm | grep discard
 enabled   online    svc:/network/discard:dgram
 enabled   online    svc:/network/discard:stream
#inetadm | grep chargen
 enabled   online    svc:/network/chargen:dgram
 enabled   online    svc:/network/chargen:stream
```

Step 2) inetadm –d "중지하고자 하는 데몬" 명령으로 서비스 데몬 중지

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

■ **LINUX (xinetd일 경우)**

Step 1) vi 편집기를 이용하여 "/etc/xinetd.d/" 디렉터리 내 echo, discard, daytime, chargen 파일 열기

Step 2) 아래와 같이 설정 (Disable = yes 설정)

- /etc/xinetd.d/echo 파일(echo-dgram, echo-stream)
- /etc/xinetd.d/discard 파일(discard-dgram, discard-stream)
- /etc/xinetd.d/daytime 파일(daytime-dgram, daytime-stream)
- /etc/xinetd.d/chargen 파일(chargen-dgram, chargen-stream)

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

Step 3) xinetd 서비스 재시작

```
#service xinetd restart
```

조치 시 영향	echo, discard, daytime, chargen는 일반적으로 사용하지 않는 서비스들임

U-24 (상)	3. 서비스 관리 > 3.6 NFS 서비스 비활성화
취약점 개요	
점검내용	■ 불필요한 NFS 서비스 사용여부 점검
점검목적	■ NFS(Network File System) 서비스는 한 서버의 파일을 많은 서비스 서버들이 공유하여 사용할 때 많이 이용되는 서비스이지만 이를 이용한 침해사고 위험성이 높으므로 사용하지 않는 경우 중지함
보안위협	■ 비인가자가 NFS 서비스로 인가되지 않은 시스템이 NFS 시스템 마운트 하여 비 인가된 시스템 접근 및 파일변조 등의 침해 행위 가능성이 존재함
참고	※ **NFS(Network File System):** 원격 컴퓨터의 파일시스템을 로컬 시스템에 마운트하여 마치 로컬 파일시스템처럼 사용할 수 있는 프로그램임 ※ NFS 서비스 사용은 원칙적으로 금지되어 있지만 불가피하게 필요한 경우 U-25(상) 항목을 참조하여 통제해야함
점검대상 및 판단기준	
대상	■ SOLARIS, Linux, AIX, HP-UX 등
판단기준	**양호 :** 불필요한 NFS 서비스 관련 데몬이 비활성화 되어 있는 경우
	취약 : 불필요한 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
점검 및 조치 사례	

OS별 점검 파일 위치 및 점검 방법	
LINUX, AIX, HP-UX, SOLARIS 5.9 이하 버전	NFS 서비스 데몬 확인 (NFS 동작 SID 확인) `#ps -ef | egrep "nfs|statd|lockd"` `root 3809 3721 0 08:44:40 ? 0:00 /usr/lib/nfs/nfsd`
SOLARIS 5.10 이상 버전	`#inetadm | egrep "nfs|statd|lockd"`
불필요한 "NFS" 서비스가 활성화된 경우 아래의 보안설정방법에 따라 서비스 데몬 중지	

■ LINUX, AIX, SOLARIS 5.9 이하 버전

Step 1) NFS 서비스 데몬 중지

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

U-24 (상)	3. 서비스 관리 > 3.6 NFS 서비스 비활성화

Step 2) 시동 스크립트 삭제 또는, 스크립트 이름 변경

1.. 위치 확인

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

2. 이름 변경

```
#mv /etc/rc.d/rc2.d/S60nfs /etc/rc.d/rc2.d/_S60nfs
```

■ **HP-UX**

Step 1) NFS 서비스 데몬 중지

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

Step 2) /etc/rc.config.d/nfsconf 파일 설정 수정

```
#vi /etc/rc.config.d/nfsconf
(수정 전) NFS_SERVER=1
(수정 후) NFS_SERVER=0
```

■ **SOLARIS 5.10 이상 버전 설정 방법**

Step 1) NFS 서비스 데몬 확인

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

Step 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

U-25 (상)	3. 서비스 관리 > 3.7 NFS 접근 통제
취약점 개요	
점검내용	■ NFS(Network File System) 사용 시 허가된 사용자만 접속할 수 있도록 접근 제한 설정 적용 여부 점검
점검목적	■ 접근권한이 없는 비인가자의 접근을 통제함
보안위협	■ 접근제한 설정이 적절하지 않을 경우 인증절차 없이 비인가자의 디렉터리나 파일의 접근이 가능하며, 해당 공유 시스템에 원격으로 마운트하여 중요 파일을 변조하거나 유출할 위험이 있음
참고	※ **NFS(Network File System):** 원격 컴퓨터의 파일시스템을 로컬 시스템에 마운트하여 마치 로컬 파일시스템처럼 사용할 수 있는 프로그램임 ※ NFS 서비스 사용 금지가 원칙이나 불가피하게 사용이 필요한 경우 NFS v2, v3은 평문으로 전송되는 취약점이 있기 때문에 암호화 되는 v4를 사용하는 것을 권고함
점검대상 및 판단기준	
대상	■ SOLARIS, Linux, AIX, HP-UX 등
판단기준	**양호 :** 불필요한 NFS 서비스를 사용하지 않거나, 불가피하게 사용 시 everyone 공유를 제한한 경우
	취약 : 불필요한 NFS 서비스를 사용하고 있고, everyone 공유를 제한하지 않은 경우
조치방법	사용하지 않는다면 NFS 서비스 중지, 사용할 경우 NFS 설정파일에 everyone 공유 설정 제거
점검 및 조치 사례	

OS별 NFS 접근제어 파일	
SOLARIS, HP-UX	"/etc/dfs/dfstab, /etc/dfs/sharetab 파일
LINUX, AIX, HP-UX	"/etc/exports" 파일
불가피하게 NFS 서비스를 사용하여야 하는 경우 NFS 접근제어 파일에 꼭 필요한 공유 디렉터리만 나열하고, everyone으로 시스템이 마운트 되지 않도록 설정	

■ **/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

U-25 (상)	3. 서비스 관리 > 3.7 NFS 접근 통제

■ /etc/exports 설정 예문

Step 1) everyone으로 시스템 마운트 금지

`#showmount -e hostname` 명령어로 확인

Step 2) /etc/exports 파일에 접근 가능한 호스트명 추가

(예) /stand host1 host2 ....

Step 3. NFS 서비스 재구동

```
#/etc/exportfs –u
#/etc/exportfs –a
```

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

U-26 (상)	3. 서비스 관리 > 3.8 automountd 제거
취약점 개요	
점검내용	■ automountd 서비스 데몬의 실행 여부 점검
점검목적	■ 로컬 공격자가 automountd 데몬에 RPC(Remote Procedure Call)를 보낼 수 있는 취약점이 존재하기 때문에 해당 서비스가 실행중일 경우 서비스를 중지시키기 위함
보안위협	■ 파일 시스템의 마운트 옵션을 변경하여 root 권한을 획득할 수 있으며, 로컬 공격자가 automountd 프로세스 권한으로 임의의 명령을 실행할 수 있음
참고	※ **automountd:** 클라이언트에서 자동으로 서버에 마운트를 시키고 일정 시간 사용하지 않으면 unmount 시켜 주는 기능을 말함 ※ **RPC(Remote Procedure Call):** 별도의 원격 제어를 위한 코딩 없이 다른 주소 공간에서 함수나 프로시저를 실행할 수 있게 하는 프로세스 간 프로토콜
점검대상 및 판단기준	
대상	■ SOLARIS, Linux, AIX, HP-UX 등
판단기준	**양호 :** automountd 서비스가 비활성화 되어 있는 경우
	취약 : automountd 서비스가 활성화 되어 있는 경우
조치방법	automountd 서비스 비활성화
점검 및 조치 사례	

OS별 점검 파일 위치 및 점검 방법	
LINUX, AIX, HP-UX, SOLARIS 5.9 이하 버전	automountd 서비스 데몬 확인 (automountd 동작 SID 확인) `#ps -ef | grep automount(or autofs)` `root 1131 1 0 jun 15 ? 32:11 /usr/sbin/automountd`
SOLARIS 5.10 이상 버전	`automount` 서비스 데몬 확인 `#svcs -a | grep "autofs"`
"automount" 서비스가 활성화된 경우 아래의 보안설정방법에 따라 서비스 데몬 중지	

■ LINUX, AIX, SOLARIS 5.9 이하 버전

Step 1) automountd 서비스 데몬 중지

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

Step 2) 시동 스크립트 삭제 또는, 스크립트 이름 변경

1.. 위치 확인

```
#ls -al /etc/rc.d/rc*.d/* | grep automount(or autofs)
```

U-26 (상)	3. 서비스 관리 > 3.8 automountd 제거

2. 이름 변경

```
#mv /etc/rc.d/rc2.d/S28automountd /etc/rc.d/rc2.d/_S28automountd
```

■ **HP-UX**

Step 1) automount 서비스 데몬 중지

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

Step 2) /etc/rc.config.d/nfsconf 파일 설정 수정

```
#vi /etc/rc.config.d/nfsconf
(수정 전) AUTOFS=1
(수정 후) AUTOFS=0
```

■ **SOLARIS 5.10 이상 버전**

Step 1) autofs 서비스 데몬 확인

```
svc:/system/filesystem/autofs:default
```

Step 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

U-27 (상)	3. 서비스 관리 > 3.9 RPC 서비스 확인
취약점 개요	
점검내용	■ 불필요한 RPC 서비스의 실행 여부 점검
점검목적	■ 다양한 취약성(버퍼 오버플로우, Dos, 원격실행 등)이 존재하는 RPC 서비스를 점검하여 해당 서비스를 비활성화 하도록 함
보안위협	■ 버퍼 오버플로우(Buffer Overflow), Dos, 원격실행 등의 취약성이 존재하는 RPC 서비스를 통해 비인가자의 root 권한 획득 및 침해사고 발생 위험이 있으므로 서비스를 중지하여야 함
참고	※ **RPC(Remote Procedure Call):** 별도의 원격 제어를 위한 코딩 없이 다른 주소 공간에서 함수나 프로시저를 실행할 수 있게 하는 프로세스 간 프로토콜 ※ **불필요한 RPC 서비스:** rpc.cmsd, rpc.ttdbserverd, sadmind, rusersd, walld, sprayd, rstatd, rpc.nisd, rexd, rpc.pcnfsd, rpc.statd, rpc.ypupdated, rpc.rquotad, kcms_server, cachefsd (※ 각 서비스 설명은 부록 참조)
점검대상 및 판단기준	
대상	■ SOLARIS, Linux, AIX, HP-UX 등
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)
점검 및 조치 사례	

OS별 점검 파일 위치 및 점검 방법	
LINUX, AIX, HP-UX, SOLARIS 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]`
SOLARIS 5.10 이상 버전	RPC 서비스 관련 데몬 확인 `#inetadm | grep rpc | grep enabled | egrep "ttdbserver|rex|rstart|rusers|spray|wall|rquota"`
불필요한 "RPC" 서비스가 활성화된 경우 아래의 보안설정방법에 따라 서비스 데몬 중지	

■ **LINUX, AIX, HP-UX, SOLARIS 5.9 이하 버전**

U-27 (상)	3. 서비스 관리 > 3.9 RPC 서비스 확인

Step 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

Step 2) inetd 서비스 재시작

```
#ps -ef | grep inetd
 root 141 1 0 15:03:22 ? 0:01 /usr/sbin/inetd -s
#kill -HUP 141
```

■ LINUX (xinetd일 경우)

Step 1) vi 편집기를 이용하여 "/etc/xinetd.d/" 디렉터리 내의 불필요한 RPC 서비스 파일 열기

Step 2) 아래와 같이 설정 (Disable = yes 설정)

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

Step 3) xinetd 서비스 재시작

```
#service xinetd restart
```

■ SOLARIS 5.10 이상 버전

Step 1) 불필요한 rpc 서비스 관련 데몬 확인

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

Step 2) svcadm disable "중지하고자 하는 데몬" 명령으로 서비스 데몬 중지

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

조치 시 영향	일반적인 경우 영향 없음

U-28 (상)	3. 서비스 관리 > 3.10 NIS, NIS+ 점검
취약점 개요	
점검내용	■ 안전하지 않은 NIS 서비스의 비활성화, 안전한 NIS+ 서비스의 활성화 여부 점검
점검목적	■ 안전하지 않은 NIS 서비스를 비활성화 하고 안전한 NIS+ 서비스를 활성화 하여 시스템 보안수준을 향상하고자 함
보안위협	■ 보안상 취약한 서비스인 NIS를 사용하는 경우 비인가자가 타시스템의 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
참고	※ NIS 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
점검대상 및 판단기준	
대상	■ SOLARIS, Linux, AIX, HP-UX 등
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
점검 및 조치 사례	

OS별 점검 파일 위치 및 점검 방법	
LINUX, AIX, HP-UX, SOLARIS 5.9 이하 버전	NIS, NIS+ 서비스 구동 확인 `#ps -ef | egrep "ypserv|ypbind|ypxfrd|rpc.yppasswdd|rpc.ypupdated"` `root 3809 3721 0 08:44:40 ? 0:00 /usr/lib/nis/ypserv`
SOLARIS 5.10 이상 버전	서비스 데몬 구동 여부 확인 `#svcs -a | grep nis`
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.ypupdated	NIS 마스터 서버에서만 실행되며 고속으로 암호화하여 NIS 맵 전송

UNIX 서버

U-28 (상)	3. 서비스 관리 > 3.10 NIS, NIS+ 점검

■ **LINUX, AIX, SOLARIS 5.9 이하 버전**

Step 1) NFS 서비스 데몬 중지

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

Step 2) 시동 스크립트 삭제 또는, 스크립트 이름 변경

1.. 위치 확인

```
#ls -al /etc/rc.d/rc*.d/* | egrep "ypserv|ypbind|ypxfrd|rpc.yppasswdd
 | rpc.ypupdated”
```

2. 이름 변경

```
#mv /etc/rc.d/rc2.d/S73ypbind /etc/rc.d/rc2.d/_S73ypbind
```

■ **HP-UX**

Step 1) NFS 서비스 데몬 중지

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

Step 2) 시동 스크립트 삭제 또는, 스크립트 이름 변경

1. 위치 확인

```
#ls -al /etc/rc.d/rc*.d/* | egrep "ypserv|ypbind|ypxfrd|rpc.yppasswdd
 | rpc.ypupdated”
```

2. /etc/rc.config.d/namesvrs 파일에서 NIS_MASTER_SERVER, NIS_SLAVE_SERVER, NIS_CLIENT 값을 0으로 설정

```
NIS_MASTER_SERVER=0
NIS_SLAVE_SERVER=0
NIS_CLIENT_SERVER=0
```

■ **SOLARIS 5.10 이상 버전**

Step 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
```

Step 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
```

※ NIS 사용이 반드시 필요 시 NIS+ 사용

조치 시 영향	일반적인 경우 영향 없음

U-29 (상)	3. 서비스 관리 > 3.11 tftp, talk 서비스 비활성화
취약점 개요	
점검내용	■ ftp, tftp, telnet, talk 등의 서비스를 사용하지 않거나 취약점이 발표된 서비스의 활성화 여부 점검
점검목적	■ 안전하지 않거나 불필요한 서비스를 제거함으로써 시스템 보안성 및 리소스의 효율적 운용
보안위협	■ 사용하지 않는 서비스나 취약점이 발표된 서비스 운용 시 공격 시도 가능
참고	-
점검대상 및 판단기준	
대상	■ SOLARIS, LINUX, AIX, HP-UX 등
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
점검 및 조치 사례	

OS별 점검 파일 위치 및 점검 방법	
LINUX, AIX, HP-UX, SOLARIS 5.9 이하 버전	불필요한 서비스 데몬 확인 `#cat /etc/inetd.conf | grep "tftp|talk|ntalk"` `tftp dgram udp6 SRC nobody /usr/sbin/tftpd tftpd -n`
LINUX(xinetd)	tftp, talk, ntalk 서비스 활성화 여부 확인 `#vi /etc/xinetd.d/tftp` `#vi /etc/xinetd.d/talk` `#vi /etc/xinetd.d/ntalk`
SOLARIS 5.10 이상 버전	서비스 데몬 확인 `#inetadm | egrep "tftp|talk"`
불필요한 "tftp, talk ntalk" 서비스가 활성화된 경우 아래의 보안설정방법에 따라 서비스 데몬 중지	

OS별 점검 파일 위치 및 점검 방법	
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

U-29 (상)	3. 서비스 관리 > 3.11 tftp, talk 서비스 비활성화

■ **LINUX, AIX, HP-UX, SOLARIS 5.9 이하 버전**

Step 1) vi 편집기를 이용하여 "/etc/inetd.conf" 파일 열기

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

Step 2) tftp, talk, ntalk 서비스 주석 처리

```
#tftp    dgram   udp6   SRC    nobody   /usr/sbin/tftpd   tftpd -n
#talk    dgram   udp    wait   root     /usr/sbin/talkd   talkd
#ntalk   dgram   udp    wait   root     /usr/sbin/talkd   talkd
```

Step 3) inetd 데몬 재시작

AIX) #refresh -s inetd

HP-UX) #inetd -c

LINUIX, SOLARIS) #kill -HUP [inetd pid]

■ **LINUX (xinetd일 경우)**

Step 1) vi 편집기를 이용하여 "/etc/xinetd.d/" 디렉터리 내 tftp, talk, ntalk 파일 열기

Step 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
}
```

Step 3) xinetd 서비스 재시작

```
#service xinetd restart
```

U-29 (상)	3. 서비스 관리 > 3.11 tftp, talk 서비스 비활성화

■ **SOLARIS 5.10 이상 버전**

Step 1) 불필요한 서비스 데몬 확인

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

Step 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	일반적인 경우 영향 없음

UNIX 서버

U-30 (상)	3. 서비스 관리 > 3.12 Sendmail 버전 점검
취약점 개요	
점검내용	■ 취약한 버전의 Sendmail 서비스 이용 여부 점검
점검목적	■ Sendmail 서비스 사용 목적 검토 및 취약점이 없는 버전의 사용 유무 점검으로 최적화된 Sendmail 서비스의 운영
보안위협	■ 취약점이 발견된 Sendmail 버전의 경우 버퍼 오버플로우(Buffer Overflow) 공격에 의한 시스템 권한 획득 및 주요 정보 요출 가능성이 있음
참고	※ Sendmail 서비스의 경우 최신버전(2016.01 기준 8.15.2) 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
점검대상 및 판단기준	
대상	■ SOLARIS, LINUX, AIX, HP-UX 등
판단기준	**양호 :** Sendmail 버전이 최신버전인 경우
	취약 : Sendmail 버전이 최신버전이 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
점검 및 조치 사례	

OS별 점검 파일 위치 및 점검 방법	
SOLARIS, 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	

■ **SOLARIS, 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

U-31 (상)	3. 서비스 관리 > 3.13 스팸 메일 릴레이 제한
취약점 개요	
점검내용	■ SMTP 서버의 릴레이 기능 제한 여부 점검
점검목적	■ 스팸 메일 서버로의 악용방지 및 서버 과부하의 방지를 위함
보안위협	■ SMTP 서버의 릴레이 기능을 제한하지 않는 경우, 악의적인 사용목적을 가진 사용자들이 스팸메일 서버로 사용하거나 Dos공격의 대상이 될 수 있음
참고	※ **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
점검대상 및 판단기준	
대상	■ SOLARIS, LINUX, AIX, HP-UX 등
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
점검 및 조치 사례	

OS별 점검 파일 위치 및 점검 방법	
SOLARIS, LINUX, AIX, 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$\*" \| grep "Relaying denied"` `R$*  $#error $@ 5.7.1 $: "550 Relaying denied"`
"SMTP" 서비스가 실행중이며, 위에 제시한 설정이 적용되지 않은 경우 아래의 보안설정방법에 따라 설정을 변경함	

sendmail.cf 설정파일 위치	
SOLARIS, LINUX, AIX, HP-UX	`"/etc/mail/sendmail.cf"`
※ sendmail 버전에 따라 /etc/sendmail.cf 존재함	

UNIX 서버

U-31 (상)	3. 서비스 관리 > 3.13 스팸 메일 릴레이 제한

■ **SOLARIS, LINUX, HP-UX, AIX**

Step 1) vi 편집기를 이용하여 sendmail.cf 설정파일 열기

Step 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"`

Step 3) 특정 IP, domain, Email Address 및 네트워크에 대한 sendmail 접근 제한 확인 (없을 시 파일생성)

```
#cat /etc/mail/access
```

예)

```
localhost.localdomain     RELAY
localhost                 RELAY
127.0.0.1                 RELAY
spam.com                  REJECT
```

Step 4) 수정을 했거나 생성했을 경우 DB 파일 생성

```
#makemap hash /etc/mail/access.db < /etc/mail/access
```

조치 시 영향	릴레이를 허용할 대상에 대한 정보를 입력한다면 영향 없음

U-32 (상)	3. 서비스 관리 > 3.14 일반사용자의 Sendmail 실행 방지
취약점 개요	
점검내용	■ SMTP 서비스 사용 시 일반사용자의 q 옵션 제한 여부 점검
점검목적	■ 일반사용자의 q 옵션을 제한하여 Sendmail 설정 및 메일큐를 강제적으로 drop 시킬 수 없게 하여 비인가자에 의한 SMTP 서비스 오류 방지
보안위협	■ 일반 사용자가 q 옵션을 이용해서 메일큐, Sendmail 설정을 보거나 메일큐를 강제적으로 drop 시킬 수 있어 악의적으로 SMTP 서버의 오류를 발생시킬 수 있음
참고	※ **SMTP(Simple Mail Transfer Protocol):** 인터넷상에서 전자우편(E-mail)을 전송할 때 이용하게 되는 표준 통신 규약을 말함
점검대상 및 판단기준	
대상	■ SOLARIS, LINUX, AIX, HP-UX 등
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
점검 및 조치 사례	

OS별 점검 파일 위치 및 점검 방법	
SOLARIS, LINUX, AIX, HP-UX	SMTP 서비스 사용 여부 및 restrictqrun 옵션 확인 `#ps -ef | grep sendmail | grep -v "grep"` `#grep -v '^ *#' /etc/mail/sendmail.cf | grep PrivacyOptions`
"SMTP" 서비스가 실행중이며, 위에 제시한 설정이 적용되지 않은 경우 아래의 보안설정방법에 따라 설정을 변경함	

■ SOLARIS, LINUX, AIX, HP-UX

Step 1) vi 편집기를 이용하여 sendmail.cf 설정파일 열기

Step 2) O PrivacyOptions= 설정 부분에 restrictqrun 옵션 추가

(수정 전) `O PrivacyOptions=authwarnings, novrfy, noexpn`

(수정 후) `O PrivacyOptions=authwarnings, novrfy, noexpn, restrictqrun`

Step 3. Sendmail 서비스 재시작

조치 시 영향	일반적인 경우 영향 없음

UNIX 서버

U-33 (상)	3. 서비스 관리 > 3.15 DNS 보안 버전 패치
취약점 개요	
점검내용	■ BIND 최신버전 사용 유무 및 주기적 보안 패치 여부 점검
점검목적	■ 취약점이 발표되지 않은 BIND 버전의 사용을 목적으로 함
보안위협	■ 최신버전(2016.01 기준 9.10.3-P2) 이하의 버전에서는 서비스거부 공격, 버퍼 오버플로우(Buffer Overflow) 및 DNS 서버 원격 침입 등의 취약성이 존재함
참고	※ **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
점검대상 및 판단기준	
대상	■ SOLARIS, LINUX, AIX, HP-UX 등
판단기준	**양호 :** DNS 서비스를 사용하지 않거나 주기적으로 패치를 관리하고 있는 경우
	취약 : DNS 서비스를 사용하며 주기적으로 패치를 관리하고 있지 않는 경우
조치방법	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
점검 및 조치 사례	

OS별 점검 파일 위치 및 점검 방법	
SOLARIS, 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	

■ SOLARIS, 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

U-33 (상)	3. 서비스 관리 > 3.15 DNS 보안 버전 패치

- NXT버그 (buffer overflow) : BIND 8.2, 8.2 p1, 8.2.1버전
- solinger버그 (Denial of Service) : BIND 8.1 이상버전
- 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
- nxt 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 enial of service 취약점

※ Bind 최신버전 다운로드 사이트
http://www.isc.org/downloads/

※ 각 버전에 대한 취약점 정보 사이트
(1) BIND 8 Vulnerability matrix :
https://kb.isc.org/article/AA-00959/0/BIND-8-Security-Vulnerability-Matrix.html

(2) BIND 9 Vulnerability matrix :
https://kb.isc.org/article/AA-00913/74/BIND-9-Security-Vulnerability-Matrix.html

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

UNIX 서버

U-34 (상)	3. 서비스 관리 > 3.16 DNS Zone Transfer 설정
취약점 개요	
점검내용	■ Secondary Name Server로만 Zone 정보 전송 제한 여부 점검
점검목적	■ 허가되지 않는 사용자에게 Zone Transfer를 제한함으로써 호스트 정보, 시스템 정보 등 정보 유출의 방지를 목적으로 함
보안위협	■ 비인가자 Zone Transfer를 이용해 Zone 정보를 전송받아 호스트 정보, 시스템 정보, 네트워크 구성 형태 등의 많은 정보를 파악할 수 있음
참고	※ DNS Zone Transfer는 Primary Name Server와 Secondary Name Server 간에 Zone 정보를 일관성 있게 유지하기 위하여 사용하는 기능
점검대상 및 판단기준	
대상	■ SOLARIS, LINUX, AIX, HP-UX 등
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 DNS 설정을 통해 내부 Zone 파일을 임의의 외부 서버에서 전송 받지 못하게 하고, 아무나 쿼리 응답을 받을 수 없도록 수정
점검 및 조치 사례	

< DNS 서비스를 사용할 경우 >

OS별 점검 파일 위치 및 점검 방법	
SOLARIS, 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"`
"DNS" 서비스 사용 시 위에 제시된 파일의 DNS 설정을 아래의 보안설정방법에 따라 수정함	

■ BIND8 DNS 설정(named.conf) 수정 예

```
Options {
            allow-transfer (존 파일 전송을 허용하고자 하는 IP;);
};
```

U-34 (상)	3. 서비스 관리 > 3.16 DNS Zone Transfer 설정

■ **BIND4.9 DNS 설정(named.conf) 수정 예**

```
Options
        xfrnets 허용하고자 하는 IP
```

< DNS 서비스를 사용하지 않는 경우 >

OS별 점검 파일 위치 및 점검 방법	
LINUX, AIX, HP-UX, SOLARIS 5.9 이하 버전	DNS 서비스 데몬 확인 (DNS 동작 SID 확인) #ps -ef | grep named root 3809 3721 0 08:44:40 ? 0:00 /usr/sbin/in.named
SOLARIS 5.10 이상 버전	#svcs -a | egrep "dns"
"DNS" 서비스를 사용하지 않는 경우 서비스 데몬 중지	

■ **LINUX, AIX, HP-UX, SOLARIS 5.9 이하 버전**

DNS 서비스 데몬 중지

#kill -9 [PID]

■ **SOLARIS 5.10 이상 버전**

Step 1) DNS 서비스 데몬 확인

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

Step 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

U-35 (상)	3. 서비스 관리 > 3.17 Apache 디렉토리 리스팅 제거
취약점 개요	
점검내용	■ 디렉터리 검색 기능의 활성화 여부 점검
점검목적	■ 외부에서 디렉터리 내의 모든 파일에 대한 접근 및 열람을 제한함을 목적으로 함
보안위협	■ 디렉터리 검색 기능이 활성화 되어 있을 경우, WEB 서버 구조 노출뿐만 아니라 백업 파일이나 소스파일, 공개되어서는 안되는 파일 등이 노출 가능함
참고	-
점검대상 및 판단기준	
대상	■ SOLARIS, LINUX, AIX, HP-UX 등
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)
점검 및 조치 사례	

OS별 점검 파일 위치 및 점검 방법	
SOLARIS, 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	

■ SOLARIS, LINUX, AIX, HP-UX

Step 1) vi 편집기를 이용하여 /[Apache_home]/conf/httpd.conf 파일 열기

```
#vi /[Apache_home]/conf/httpd.conf
```

Step 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>
```

U-35 (상)	3. 서비스 관리 > 3.17 Apache 디렉토리 리스팅 제거

(수정 후) Option 지시자에 None 변경 후 저장

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

조치 시 영향	일반적인 경우 영향 없음

UNIX 서버

U-36 (상)	3. 서비스 관리 > 3.18 Apache 웹 프로세스 권한 제한
취약점 개요	
점검내용	■ Apache 데몬이 root 권한으로 구동되는지 여부 점검
점검목적	■ Apache 데몬을 root 권한으로 구동하지 않고 별도의 권한으로 서비스함으로써 침해사고 발생 시 피해범위 확산 방지를 목적으로 함
보안위협	■ 웹 프로세스 취약점 공격으로 Apache 권한이 탈취 당할 경우 Apache 프로세스의 권한이 root이면 시스템 전체의 제어권을 탈취 당해 피해범위가 확산될 가능성이 있음
참고	-
점검대상 및 판단기준	
대상	■ SOLARIS, LINUX, AIX, HP-UX 등
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
점검 및 조치 사례	

OS별 점검 파일 위치 및 점검 방법	
SOLARIS, LINUX, AIX, HP-UX	Apache 데몬 구동 권한(User 및 Group) 확인 `#vi /[Apache_home]/conf/httpd.conf` `User [root`가 아닌 별도 계정명`]` `Group [root`가 아닌 별도 계정명`]`
위에 제시한 설정이 적용되지 않은 경우 아래의 보안설정방법에 따라 설정을 변경함	

■ SOLARIS, LINUX, AIX, HP-UX

Step 1) 데몬 User & Group 변경

User & Group 부분에 root가 아닌 별도 계정으로 변경

```
User [root가 아닌 별도 계정명]
Group [root가 아닌 별도 계정명]
```

Step 2) Apache 서비스 재시작

조치 시 영향	일반적인 경우 영향 없음

U-37 (상)	3. 서비스 관리 > 3.19 Apache 상위 디렉토리 접근 금지
취약점 개요	
점검내용	■ ".." 와 같은 문자 사용 등으로 상위 경로로 이동이 가능한지 여부 점검
점검목적	■ 상위 경로 이동 명령으로 비인가자의 특정 디렉터리에 대한 접근 및 열람을 제한하여 중요 파일 및 데이터 보호를 목적으로 함
보안위협	■ 상위 경로로 이동하는 것이 가능할 경우 접근하고자 하는 디렉터리의 하위 경로에 접속하여 상위경로로 이동함으로써 악의적인 목적을 가진 사용자의 접근이 가능함
참고	-
점검대상 및 판단기준	
대상	■ SOLARIS, LINUX, AIX, HP-UX 등
판단기준	**양호 :** 상위 디렉터리에 이동제한을 설정한 경우
	취약 : 상위 디렉터리에 이동제한을 설정하지 않은 경우
조치방법	Step 1) 사용자 인증을 하기 위해서 각 디렉터리 별로 httpd.conf 파일 내 AllowOverride 지시자의 옵션 설정을 변경 (None에서 AuthConfig 또는, All로 변경) Step 2) 사용자 인증을 설정할 디렉터리에 .htaccess 파일 생성 Step 3) 사용자 인증 계정 생성: htpasswd -c <인증 파일> <사용자 계정>
점검 및 조치 사례	

OS별 점검 파일 위치 및 점검 방법	
SOLARIS, 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	

■ SOLARIS, LINUX, AIX, HP-UX

Step 1) vi 편집기를 이용하여 /[Apache_home]/conf/httpd.conf 파일 열기

```
#vi /[Apache_home]/conf/httpd.conf
```

Step 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>
```

UNIX 서버

U-37 (상)	3. 서비스 관리 > 3.19 Apache 상위 디렉토리 접근 금지

(수정 후) AllowOverride 지시자에 AuthConfig 옵션이 설정되어 있음

```
<Directory “/usr/local/apache2/htdocs”>
    AllowOverride AuthConfig
    Allow from all
</Directory>
```

Step 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

Step 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]#
```

Step 5) 변경된 설정 내용을 적용하기 위하여 Apache 데몬 재시작

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

U-38 (상)	3. 서비스 관리 > 3.20 Apache 불필요한 파일 제거
취약점 개요	
점검내용	■ Apache 설치 시 기본으로 생성되는 불필요한 파일의 삭제 여부 점검
점검목적	■ Apache 설치 시 디폴트로 설치되는 불필요한 파일을 제거함을 목적으로 함.
보안위협	■ Apache 설치 시 htdocs 디렉터리 내에 매뉴얼 파일은 시스템 관련정보를 노출하거나 해킹에 악용될 수 있음.
참고	※ 불필요한 파일: 샘플 파일, 매뉴얼 파일, 임시 파일, 테스트 파일, 백업 파일 등
점검대상 및 판단기준	
대상	■ SOLARIS, LINUX, AIX, HP-UX 등
판단기준	**양호 :** 기본으로 생성되는 불필요한 파일 및 디렉터리가 제거되어 있는 경우
	취약 : 기본으로 생성되는 불필요한 파일 및 디렉터리가 제거되지 않은 경우
조치방법	불필요한 파일 및 디렉터리 제거 ("/[Apache_home]/htdocs/manual", "/[Apache_home]/manual" 파일 제거 등)
점검 및 조치 사례	

OS별 점검 파일 위치 및 점검 방법	
SOLARIS, LINUX, AIX, HP-UX	불필요한 파일 및 디렉터리 존재 여부 확인 `#ls -ld /[Apache_home]/htdocs/manual` `#ls -ld /[Apache_home]/manual`
위에 제시한 불필요한 파일 및 디렉터리가 존재하는 경우 아래의 보안설정방법에 따라 불필요한 파일 및 디렉터리 제거 또는, 설정을 변경함	

■ SOLARIS, LINUX, AIX, HP-UX

Step 1) #ls 명령어로 확인된 매뉴얼 디렉터리 및 파일 제거

```
#rm -rf /[Apache_home]/htdocs/manual
#rm -rf /[Apache_home]/manual
```

Step 2) #ls 명령어로 정상적인 제거 확인

```
#ls -ld /[Apache_home]/htdocs/manual
#ls -ld /[Apache_home]/manual
```

Step 3) 추가적으로 웹서비스 운영에 불필요한 파일이나 디렉터리가 있을 시 제거

조치 시 영향	일반적인 경우 영향 없음

UNIX 서버

U-39 (상)	3. 서비스 관리 > 3.21 Apache 링크 사용금지
취약점 개요	
점검내용	■ 심볼릭 링크, aliases 사용 제한 여부 점검
점검목적	■ 무분별한 심볼릭 링크, aliases 사용제한으로 시스템 권한의 탈취 방지를 목적으로 함
보안위협	■ 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
참고	※ **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
점검대상 및 판단기준	
대상	■ SOLARIS, LINUX, AIX, HP-UX 등
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)
점검 및 조치 사례	

OS별 점검 파일 위치 및 점검 방법	
SOLARIS, 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	

■ **SOLARIS, LINUX, AIX, HP-UX**

Step 1) vi 편집기를 이용하여 /[Apache_home]/conf/httpd.conf 파일 열기

```
#vi /[Apache_home]/conf/httpd.conf
```

Step 2) 설정된 모든 디렉터리의 Options 지시자에서 FollowSymLinks 옵션 제거

(수정 전) Options 지시자에 FollowSymLinks 옵션이 설정되어 있음

U-39 (상)	3. 서비스 관리 > 3.21 Apache 링크 사용금지

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

(수정 후) Options 지시자에 None 변경 후 저장

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

조치 시 영향	일반적인 경우 영향 없음

UNIX 서버

U-40 (상)	3. 서비스 관리 > 3.22 Apache 파일 업로드 및 다운로드 제한
취약점 개요	
점검내용	■ 파일 업로드 및 다운로드의 사이즈 제한 여부 점검
점검목적	■ 기반시설 특성상 원칙적으로 파일 업로드 및 다운로드를 금지하고 있지만 불가피하게 필요시 용량 사이즈를 제한함으로써 불필요한 업로드와 다운로드를 방지해 서버의 과부하 예방 및 자원을 효율적으로 관리하기 위함
보안위협	■ 악의적 목적을 가진 사용자가 반복 업로드 및 웹 쉘 공격 등으로 시스템 권한을 탈취하거나 대용량 파일의 반복 업로드로 서버자원을 고갈시키는 공격의 위험이 있음
참고	※ **불필요한 업로드와 다운로드:** 내부 정책에 맞지 않는 업로드와 다운로드를 말함. 예를 들어 5Mb 이상의 대용량 파일이나 확장자를 화이트 리스트 방식으로 제한함을 말함
점검대상 및 판단기준	
대상	■ SOLARIS, LINUX, AIX, HP-UX 등
판단기준	**양호 :** 파일 업로드 및 다운로드를 제한한 경우
	취약 : 파일 업로드 및 다운로드를 제한하지 않은 경우
조치방법	1. 파일 업로드 및 다운로드 용량 제한 (/[Apache_home]/conf/httpd.conf 파일에 설정된 모든 디렉터리의 LimitRequestBody 지시자에 파일 사이즈 용량 제한 설정)
점검 및 조치 사례	

OS별 점검 파일 위치 및 점검 방법	
SOLARIS, 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	

■ SOLARIS, LINUX, AIX, HP-UX

Step 1) vi 편집기를 이용하여 /[Apache_home]/conf/httpd.conf 파일 열기

```
#vi /[Apache_home]/conf/httpd.conf
```

Step 2) 설정된 모든 디렉터리의 LimitRequestBody 지시자에서 파일 사이즈 용량 제한 설정

```
예)
<Directory />
LimitRequestBody 5000000 (※ "/" 는 모든 파일 사이즈를 5M로 제한하는 설정 단위:byte)
</Directory>
```

조치 시 영향	일반적인 경우 영향 없음

U-41 (상)	3. 서비스 관리 > 3.23 Apache 웹 서비스 영역의 분리
취약점 개요	
점검내용	■ 웹 서버의 루트 디렉터리와 OS의 루트 디렉터리를 다르게 지정하였는지 점검
점검목적	■ 웹 서비스 영역과 시스템 영역을 분리시켜서 웹 서비스의 침해가 시스템 영역으로 확장될 가능성을 최소화하기 위함
보안위협	■ 웹 서버의 루트 디렉터리와 OS의 루트 디렉터리를 다르게 지정하지 않았을 경우, 비인가자가 웹 서비스를 통해 해킹이 성공할 경우 시스템 영역까지 접근이 가능하여 피해가 확장될 수 있음
참고	-
점검대상 및 판단기준	
대상	■ SOLARIS, LINUX, AIX, HP-UX 등
판단기준	**양호 :** DocumentRoot를 별도의 디렉터리로 지정한 경우
	취약 : DocumentRoot를 기본 디렉터리로 지정한 경우
조치방법	DocumentRoot "/usr/local/apache/htdocs", "/usr/local/apache2/htdocs", "/var/www/html" 셋 중 하나일 경우 -> DocumentRoot "별도 디렉터리" 로 변경
점검 및 조치 사례	

OS별 점검 파일 위치 및 점검 방법	
SOLARIS, LINUX, AIX, HP-UX	DocumentRoot의 별도 디렉터리 지정 여부 확인 `#vi /[Apache_home]/conf/httpd.conf` `DocumentRoot "/usr/local/apache/htdocs"` 또는 `DocumentRoot "/usr/local/apache2/htdocs"` 또는 `DocumentRoot "/var/www/html"`
DocumentRoot가 별도의 디렉터리로 지정되지 않은 경우 아래의 보안설정방법에 따라 설정을 변경함	

■ SOLARIS, LINUX, AIX, HP-UX

Step 1) vi 편집기를 이용하여 /[Apache_home]/conf/httpd.conf 파일 열기

```
#vi /[Apache_home]/conf/httpd.conf
```

Step 2) DocumentRoot 설정 부분에 "/usr/local/apache/htdocs", "/usr/local/apache2/htdocs", "/var/www/html" 셋 중 하나가 아닌 별도의 디렉터리로 변경

```
DocumentRoot "디렉터리"
```

조치 시 영향	일반적인 경우 영향 없음

UNIX 서버

<table>
<tr><th>U-42 (상)</th><th>4 패치 관리 > 4.1 최신 보안패치 및 벤더 권고사항 적용</th></tr>
<tr><th colspan="2">취약점 개요</th></tr>
<tr><td>점검내용</td><td>■ 시스템에서 최신 패치가 적용되어 있는지 점검</td></tr>
<tr><td>점검목적</td><td>■ 주기적인 패치 적용을 통하여 보안성 및 시스템 안정성을 확보함</td></tr>
<tr><td>보안위협</td><td>■ 최신 보안패치가 적용되지 않을 경우, 이미 알려진 취약점을 통하여 공격자에 의해 시스템 침해사고 발생 가능성이 존재함</td></tr>
<tr><td>참고</td><td>-</td></tr>
<tr><th colspan="2">점검대상 및 판단기준</th></tr>
<tr><td>대상</td><td>■ SOLARIS, Linux, AIX, HP-UX 등</td></tr>
<tr><td rowspan="2">판단기준</td><td>양호 : 패치 적용 정책을 수립하여 주기적으로 패치관리를 하고 있으며, 패치 관련 내용을 확인하고 적용했을 경우</td></tr>
<tr><td>취약 : 패치 적용 정책을 수립하지 않고 주기적으로 패치관리를 하지 않거나 패치 관련 내용을 확인하지 않고 적용하지 않았을 경우</td></tr>
<tr><td>조치방법</td><td>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</td></tr>
<tr><th colspan="2">점검 및 조치 사례</th></tr>
<tr><td colspan="2">
<table>
<tr><th colspan="2">OS별 점검 방법</th></tr>
<tr><td>SOLARIS, LINUX, AIX, HP-UX</td><td>패치 적용 정책 수립 여부 및 정책에 따른 패치 적용 여부 확인</td></tr>
</table>

■ SOLARIS
1. “showrev –p” 서버에 적용되어 있는 패치 리스트 확인
2. 아래 사이트에 접속하여 패치를 찾아 적용
https://support.oracle.com

• 패치를 검색하는 방법
1. Patches & Updates(패치 및 업데이트) 탭을 클릭
2. Patch Search(패치 검색) 섹션에서 Product or the Family (Advanced Search)(제품 또는 제품군(고급 검색)) 옵션을 클릭
3. 제품으로 Solaris Operating System(Solaris 운영 체제)을 선택
</td></tr>
</table>

U-42 (상)	4 패치 관리 > 4.1 최신 보안패치 및 벤더 권고사항 적용

4. 릴리스로 Solaris xx Operating System(Solaris xx 운영 체제)을 선택
5. 유형으로 Patch(패치) 또는 Patchset(패치 세트) 또는 둘 다 선택
6. Search(검색)을 클릭 후 파일 다운로드

< 패치 적용 방법 >

MOS(My Oracle Support) 웹 사이트에서 패치 파일(119784-17.zip)을 다운로드 했다고 가정

Step 1) 슈퍼유저가 되어야 함.

Step 2) 패치 파일을 임시 디렉터리에 복사

```
#cp /<patch download location>/119784-17.zip /tmp
```

Step 3) 패치 파일의 압축 풀기.

```
#cd /tmp
#unzip 119784-17.zip
```

Step 4) 패치를 적용

```
#patchadd 119784-17
```

Step 5) (옵션)패치가 적용되었는지 확인

```
#patchadd -p | grep 119784-17
```

※ 패치 시 주의점

patchadd -M 명령이 개선되어 더 이상 정확한 설치 순서로 패치ID를 지정할 필요가 없고 디렉터리의 모든 패치가 시스템에 설치 됨

■ LINUX

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

LINUX는 오픈되고, 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 <pakage-name>
```

UNIX 서버

U-42 (상)	4 패치 관리 > 4.1 최신 보안패치 및 벤더 권고사항 적용

■ **AIX**

1. "oslevel –s, instfix-i |grep ML, instfix –i |grep ML, instfix –i |grep SP"로 서버에 적용되어 있는 패치 리스트 확인
2. 아래 사이트에 접속하여 패치를 찾아 적용
   http://techsupport.services.ibm.com/server/mlfixes/43/

< 패치 적용 방법>

Step 1) 패치를 다운로드 후 서버에 파일 업로드 한 뒤 "installp"를 이용하여 OS패치 설치

```
#smitty installp
```

Step 2) install Software 선택 후 INPUT device / directory for software에서 패치파일 업로드 한 경로 입력

Step 3) SOFTWARE to install 항목은 all-latest 선택

Step 4) PREVIEW only? (install operation will NOT occur) 항목을 yes로 설정할 경우 실제 설치가 아닌 사전 설치가 진행되고 문제 발생 시 Failed 결과값 출력함

Step 5) COMMIT software updates? 항목을 no로 설정할 경우 Apply설치가 진행되고 향후 이전버전의 OS Patch 단계로 롤백이 가능. YES로 설정 시 롤백 불가

Step 6) ACCEPT new license agreements? 항목은 YES로 설정해야만 설치 진

※ 패치 시 문제가 발생한 경우 Apply 설치에 한해 기본버전으로 재설정 가능
Apply, commit 된 패키지 확인은 "lslpp –l"로 확인 가능

```
# smitty install_reject
```

1. SOFTWARE name 항목에서 Apply설치된 OS Patch를 선택
2. Preview 항목을 Yes로 설정
3. 소프트웨어 제거에 문제가 없는지 확인 후 진행

■ **HP-UX**

1. 'swlist –l product'로 서버에 적용된 패치 리스트 확인
2. 아래 사이트에 접속하여 패치를 찾아 적용(ID, password가 필요함)
   http://h20565.www2.hp.com/portal/site/hpsc/

• 패치를 검색하는 방법

1. 유지보수 및 지원 (hp 제품) 에서 "개별패치"를 선택
2. patch database main에서 원하는 패치 database를 선택(여기서 firmware 부분 선택)
3. search for patches 에서 원하는 항목을 선택(여기서 CPU 선택)
4. 검색할 키워드에서 원하는 항목을 선택 후 search 클릭
5. most recently에서 체크박스에 체크하고 add to selected patch list 버튼 클릭
6. selected patch list가 나오면 패치의 체크박스 선택 후 download patch 버튼 클릭 후 다운로드
 - 설치되는 방법을 보고 싶다면 패치이름의 링크 클릭

U-42 (상)	4 패치 관리 > 4.1 최신 보안패치 및 벤더 권고사항 적용

< 패치 적용 방법 >

Step 1) patch 파일을 /tmp 밑에 다운로드 받음

- 파일명을 patch_10으로 가정

Step 2) HP-UX에서 shell archive를 품

```
#sh patch_10
```

- patch_10.depot와 patch_10.text가 생성됨

Step 3) patch_10.depot 설치

```
#swinstall –s /tmp/patch_10.depot
```
(경로는 절대경로를 써야함)

```
#swinstall ?x autoreboot=true ?x patch_match_target=true \ -s /tmp/patch_10.depot
```

조치 시 영향	일반적인 경우 영향 없음

UNIX 서버

U-43 (상)	5. 로그 관리 > 5.1 로그의 정기적 검토 및 보고
취약점 개요	
점검내용	■ 로그의 정기적 검토 및 보고 여부 점검
점검목적	■ 정기적인 로그 점검을 통해 안정적인 시스템 상태 유지 및 외부 공격 여부를 파악하기 위함
보안위협	■ 로그의 검토 및 보고 절차가 없는 경우 외부 침입 시도에 대한 식별이 누락될 수 있고, 침입 시도가 의심되는 사례 발견 시 관련 자료를 분석하여 해당 장비에 대한 접근을 차단하는 등의 추가 조치가 어려움
참고	※ 시스템 접속 기록, 계정 관리 로그 등 U-73(하) 점검 항목에서 설정한 보안 로그를 포함하여 응용 프로그램, 시스템 로그 기록에 대하여 주기적인 검토 및 보고가 필요함 ※ 관련 점검 항목 : A-85(하), U-73(하)
점검대상 및 판단기준	
대상	■ SOLARIS, Linux, AIX, HP-UX 등
판단기준	**양호 :** 접속기록 등의 보안 로그, 응용 프로그램 및 시스템 로그 기록에 대해 정기적으로 검토, 분석, 리포트 작성 및 보고 등의 조치가 이루어지는 경우
	취약 : 위 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
점검 및 조치 사례	

OS별 점검 방법	
SOLARIS, LINUX, AIX, HP-UX	로그 분석 계획 수립 여부 및 로그 분석 결과에 따른 점검

■ SOLARIS, LINUX, AIX, HP-UX

정기적인 로그 분석을 위하여 아래와 같은 절차 수립

Step 1) 정기적인 로그 검토 및 분석 주기 수립

1. utmp, wtmp ,btmp 등의 로그를 확인하여 마지막 로그인 시간, 접속 IP, 실패한 이력 등을 확인하여 계정 탈취 공격 및 시스템 해킹 여부를 검토
2. sulog를 확인하여 허용된 계정 외에 su 명령어를 통해 권한상승을 시도하였는지 검토
3. xferlog를 확인하여 비인가자의 ftp 접근 여부를 검토

Step 2) 로그 분석에 대한 결과 보고서 작성

Step 3) 로그 분석 결과보고서 보고 체계 수립

조치 시 영향	일반적인 경우 영향 없음

U-44 (중)	1. 계정관리 > 1.5 root 이외의 UID가 '0' 금지
취약점 개요	
점검내용	■ 사용자 계정 정보가 저장된 파일(예 /etc/passwd)에 root(UID=0) 계정과 동일한 UID(User Identification)를 가진 계정이 존재하는지 점검
점검목적	■ root 계정과 동일한 UID가 존재하는지 점검하여 root권한이 일반 사용자 계정이나 비인가자의 접근 위협에 안전하게 보호되고 있는지 확인하기 위함
보안위협	■ root 계정과 동일 UID 계정이 존재하여 비인가자에 노출되었을 경우 root 계정 권한과 동일한 권한으로 시스템에 로그인 하여 시스템 계정 정보 유출, 환경설정 파일 및 디렉터리 변조 및 삭제 등의 행위를 하여 시스템 가용성(서비스 다운, 악성코드 유포지 감염)에 영향을 미칠 수 있는 위협이 존재함 ■ root와 동일한 UID를 사용하므로 사용자 감사 추적 시 어려움이 발생함
참고	※ **UID(User Identification):** 여러 명의 사용자가 동시에 사용하는 시스템에서 사용자가 자신을 대표하기 위해 쓰는 이름
점검대상 및 판단기준	
대상	■ SOLARIS, LINUX, AIX, HP-UX 등
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
점검 및 조치 사례	

OS별 점검 파일 위치 및 점검 방법	
SOLARIS, LINUX, AIX, HP-UX	`#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` "/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 적용되지 않은 경우 아래의 보안설정방법에 따라 설정을 변경함	

UNIX 서버

U-44 (중)	1. 계정관리 > 1.5 root 이외의 UID가 '0' 금지

■ **SOLARIS, LINUX, HP-UX**

Step 1) usermod 명령으로 UID가 0인 일반 계정의 UID를 100 이상으로 수정

- SOLARIS, 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**

Step 1) chuser 명령으로 UID가 0인 일반 계정의 UID를 100 이상으로 수정

(예) test 계정의 UID 를 2002 로 바꿀 경우

#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

U-45 (하)	1. 계정관리 > 1.6 root 계정 su 제한
취약점 개요	
점검내용	■ 시스템 사용자 계정 그룹 설정 파일(예 /etc/group)에 su 관련 그룹이 존재하는지 점검 ■ su 명령어가 su 관련 그룹에서만 허용되도록 설정되어 있는지 점검
점검목적	■ su 관련 그룹만 su 명령어 사용 권한이 부여되어 있는지 점검하여 su 그룹에 포함되지 않은 일반 사용자의 su 명령 사용을 원천적으로 차단하는지 확인하기 위함
보안위협	■ su 명령어를 모든 사용자가 사용하도록 설정되어 있는 경우 root 계정 권한을 얻기 위해 패스워드 무작위 대입 공격(Brute Force Attack)이나 패스워드 추측 공격(Password Guessing)을 시도하여 root 계정 패스워드가 유출될 위협이 있음
참고	-
점검대상 및 판단기준	
대상	■ SOLARIS, LINUX, AIX, HP-UX 등
판단기준	**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 Step 1) Group 생성(생성할 그룹 요청, 일반적으로 wheel 사용) Step 2) su 명령어의 그룹을 su 명령어 허용할 그룹으로 변경 Step 3) su 명령어의 권한 변경(4750) Step 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

U-45 (하)	1. 계정관리 > 1.6 root 계정 su 제한

점검 및 조치 사례

OS별 점검 파일 위치 및 점검 방법	
SOLARIS, LINUX, AIX, HP-UX	Step 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` Step 2) wheel 그룹이 su 명령어를 사용할 수 있는지 설정 여부 확인 [SOLARIS] `#ls –al /usr/bin/su` `#chgrp security su` `#chmod 4750 su` [AIX] `#cat /etc/security/user` ---> default의 "sugroup=staff" 설정 확인 [HP-UX] `#vi /etc/default/security` ---> `SU_ROOT_GROUP=wheel` 설정 확인 Step 3) 파일 권한 확인 `#ls –l /usr/bin/su` `-rwsr-x---  /usr/bin/su` (파일 권한이 4750인 경우 양호)
LINUX PAM 모듈 이용 시	Step 1) "wheel" 그룹 (su 명령어 사용 그룹) 및 그룹 내 구성원 존재 여부 확인 `#cat /etc/group` **`wheel`**`:x:10:root,admin` Step 2) 허용 그룹 (su 명령어 사용 그룹) 설정 여부 확인 `#cat /etc/pam.d/su` `auth required /lib/security/pam_wheel.so debug group=wheel` 또는, `auth required /lib/security/$ISA/pam_wheel.so use_id`
위에 제시한 설정이 적용되지 않은 경우 아래의 보안설정방법에 따라 설정을 변경함	

■ SOLARIS, LINUX, HP-UX

Step 1) wheel group 생성 (wheel 그룹이 존재하지 않는 경우)

```
#groupadd wheel
```

Step 2) su 명령어 그룹 변경

```
#chgrp wheel /usr/bin/su
```

U-45 (하)	1. 계정관리 > 1.6 root 계정 su 제한

Step 3) su 명령어 사용권한 변경

```
#chmod 4750 /usr/bin/su
```

Step 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**

Step 1) wheel group 생성(wheel 그룹이 존재하지 않는 경우)

```
#mkgroup wheel
```

Step 2) su 명령어 그룹 변경

```
#chgrp wheel /usr/bin/su
```

Step 3) su 명령어 사용권한 변경

```
#chmod 4750 /usr/bin/su
```

Step 4) wheel 그룹에 su 명령 허용 계정 등록

```
#chgroup users=<user_name> wheel
```

(예) `chgroup users=admin wheel`

■ **LINUX PAM 모듈을 이용한 설정 방법**

Step 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
```

Step 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

U-46 (중)	1. 계정관리 > 1.7 패스워드 최소 길이 설정
취약점 개요	
점검내용	■ 시스템 정책에 패스워드 최소(8자 이상) 길이 설정이 적용되어 있는 점검
점검목적	■ 패스워드 최소 길이 설정이 적용되어 있는지 점검하여 짧은(8자 미만) 패스워드 길이로 발생하는 취약점을 이용한 공격(무작위 대입 공격, 사전 대입 공격 등)에 대한 대비(사용자 패스워드 유출)가 되어 있는지 확인하기 위함
보안위협	■ 패스워드 최소 길이 설정이 적용되어 있지 않을 경우 비인가자의 각종 공격(무작위 대입 공격, 사전 대입 공격 등)에 취약하여 사용자 계정 패스워드 유출 우려가 있음
참고	※ 공공기관인 경우 국가정보보안기본지침에 의해 패스워드를 9자리 이상의 길이로 설정해야함
점검대상 및 판단기준	
대상	■ SOLARIS, LINUX, AIX, HP-UX 등
판단기준	**양호 :** 패스워드 최소 길이가 8자 이상으로 설정되어 있는 경우 (공공기관의 경우 9자리 이상)
	취약 : 패스워드 최소 길이가 8자 미만으로 설정되어 있는 경우 (공공기관의 경우 9자리 미만)
조치방법	패스워드 정책 설정파일을 수정하여 패스워드 최소 길이를 8자 이상으로 설정 (공공기관의 경우 9자리 이상으로 설정)
점검 및 조치 사례	

OS별 점검 파일 위치 및 점검 방법	
SOLARIS	`#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	

U-46 (중)	1. 계정관리 > 1.7 패스워드 최소 길이 설정

■ **SOLARIS**

Step 1) vi 편집기를 이용하여 "/etc/default/passwd" 파일 열기

Step 2) 아래와 같이 수정 또는, 신규 삽입

(수정 전) `PASSLENGTH=6`

(수정 후) `PASSLENGTH=8(or 9)`

■ **LINUX**

Step 1) vi 편집기를 이용하여 "/etc/login.defs" 파일 열기

Step 2) 아래와 같이 수정 또는, 신규 삽입

(수정 전) `PASS_MIN_LEN 6`

(수정 후) `PASS_MIN_LEN 8(or 9)`

■ **AIX**

Step 1.) vi 편집기를 이용하여 "/etc/security/user" 파일 열기

Step 2) default: 부분을 아래와 같이 수정 또는, 신규 삽입

(수정 전) `minlen=4`

(수정 후) `minlen=8(or 9)`

■ **HP-UX**

Step 1) vi 편집기를 이용하여 "/etc/default/security" 파일 열기

Step 2) 아래와 같이 수정 또는, 신규 삽입

(수정 전) `MIN_PASSWORD_LENGTH=`

(수정 후) `MIN_PASSWORD_LENGTH=8(or 9)`

조치 시 영향	일반적인 경우 영향 없음

UNIX 서버

U-47 (중)	1. 계정관리 > 1.8 패스워드 최대 사용기간 설정
취약점 개요	
점검내용	■ 시스템 정책에 패스워드 최대(90일 이하) 사용기간 설정이 적용되어 있는지 점검
점검목적	■ 패스워드 최대 사용 기간 설정이 적용되어 있는지 점검하여 시스템 정책에서 사용자 계정의 장기간 패스워드 사용을 방지하고 있는지 확인하기 위함
보안위협	■ 패스워드 최대 사용기간을 설정하지 않은 경우 비인가자의 각종 공격(무작위 대입 공격, 사전 대입 공격 등)을 시도할 수 있는 기간 제한이 없으므로 공격자 입장에서는 장기적인 공격을 시행할 수 있어 시행한 기간에 비례하여 사용자 패스워드가 유출될 수 있는 확률이 증가함
참고	-
점검대상 및 판단기준	
대상	■ SOLARIS, LINUX, AIX, HP-UX 등
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
점검 및 조치 사례	

OS별 점검 파일 위치 및 점검 방법	
SOLARIS	`#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	

U-47 (중)	1. 계정관리 > 1.8 패스워드 최대 사용기간 설정

■ **SOLARIS**

Step 1) vi 편집기를 이용하여 "/etc/default/passwd" 파일 열기

Step 2) 아래와 같이 수정 또는, 신규 삽입

(수정 전) `MAXWEEKS=`

(수정 후) `MAXWEEKS=12` (단위: 주)

■ **LINUX**

Step 1) vi 편집기를 이용하여 "/etc/login.defs" 파일 열기

Step 2) 아래와 같이 수정 또는, 신규 삽입

(수정 전) `PASS_MAX_DAYS 99999`

(수정 후) `PASS_MAX_DAYS 90` (단위: 일)

■ **AIX**

Step 1) vi 편집기를 이용하여 "/etc/security/user" 파일 열기

Step 2) default: 부분을 아래와 같이 수정 또는, 신규 삽입

(수정 전) `maxage=0`

(수정 후) `maxage=12` (단위: 주)

■ **HP-UX**

Step 1) vi 편집기를 이용하여 "/etc/default/security" 파일 열기

Step 2.) 아래와 같이 수정 또는, 신규 삽입

(수정 전) `PASSWORD_MAXDAYS=99999`

(수정 후) `PASSWORD_MAXDAYS=90` (단위: 일)

조치 시 영향	일반적인 경우 영향 없음

UNIX 서버

U-48 (중)	1. 계정관리 > 1.9 패스워드 최소 사용기간 설정
취약점 개요	
점검내용	■ 시스템 정책에 패스워드 최소 사용기간 설정이 적용되어 있는지 점검
점검목적	■ 패스워드 최소 사용 기간 설정이 적용되어 있는지 점검하여 사용자가 자주 패스워드를 변경할 수 없도록 하고 관련 설정(최근 암호 기억)과 함께 시스템에 적용하여 패스워드 변경 전에 사용했던 패스워드를 재사용 할 수 없도록 방지하는지 확인하기 위함
보안위협	■ 패스워드 변경 후 최소 사용 기간이 설정되지 않은 경우 사용자에게 익숙한 패스워드로 즉시 변동이 가능하여, 이를 재사용함으로써 원래 암호를 같은 날 다시 사용할 수 있음 ■ 패스워드 변경 정책에 따른 주기적인 패스워드 변경이 무의미해 질 수 있으며, 이로 인해 조직의 계정 보안성을 낮출 수 있음
참고	※ **최근 암호 기억:** 사용자가 현재 암호 또는 최근에 사용했던 암호와 동일한 새 암호를 만드는 것을 방지하는 설정. 예를 들어 값 1은 마지막 암호만 기억한다는 의미이며 값 5는 이전 암호 5개를 기억한다는 의미임
점검대상 및 판단기준	
대상	■ SOLARIS, LINUX, AIX, HP-UX 등
판단기준	**양호 :** 패스워드 최소 사용기간이 설정되어 있는 경우
	취약 : 패스워드 최소 사용기간이 설정되어 있지 않는 경우
조치방법	패스워드 정책 설정파일을 수정하여 패스워드 최소 사용기간을 1일(1주)로 설정
점검 및 조치 사례	

OS별 점검 파일 위치 및 점검 방법	
SOLARIS	#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	

U-48 (중)	1. 계정관리 > 1.9 패스워드 최소 사용기간 설정

■ **SOLARIS**

Step 1) vi 편집기를 이용하여 "/etc/default/passwd" 파일 열기

Step 2) 아래와 같이 수정 또는, 신규 삽입

(수정 전) `MINWEEKS=`

(수정 후) `MINWEEKS=1` (단위: 주)

■ **LINUX**

Step 1) vi 편집기를 이용하여 "/etc/login.defs" 파일 열기

Step 2) 아래와 같이 수정 또는, 신규 삽입

(수정 전) `PASS_MIN_DAYS`

(수정 후) `PASS_MIN_DAYS 1` (단위: 일)

■ **AIX**

Step 1) vi 편집기를 이용하여 "/etc/security/user" 파일 열기

Step 2) default 부분을 아래와 같이 수정 또는, 신규 삽입

(수정 전) `minage=`

(수정 후) `minage=1` (단위: 주)

■ **HP-UX**

Step 1) vi 편집기를 이용하여 "/etc/default/security" 파일 열기

Step 2) 아래와 같이 수정 또는, 신규 삽입

(수정 전) `PASSWORD_MINDAYS=`

(수정 후) `PASSWORD_MINDAYS=1` (단위: 일)

조치 시 영향	일반적인 경우 영향 없음

UNIX 서버

U-49 (하)	1. 계정관리 > 1.10 불필요한 계정 제거
취약점 개요	
점검내용	■ 시스템 계정 중 불필요한 계정(퇴직, 전직, 휴직 등의 이유로 사용하지 않는 계정 및 장기적으로 사용하지 않는 계정 등)이 존재하는지 점검
점검목적	■ 불필요한 계정이 존재하는지 점검하여 관리되지 않은 계정에 의한 침입에 잘 대비하는지 확인하기 위함
보안위협	■ OS나 Package 설치 시 Default로 생성되는 계정 및 불필요한 계정들은 비인가자의 공격(무작위 대입 공격, 사전 대입 공격)에 의해 패스워드가 유출될 위험이 존재함
참고	※ **Default 계정:** OS나 Package 설치 시 기본적으로 생성되는 계정(예 lp, uucp, nuucp 등) ※ 불필요한 default 계정 삭제 시 업무 영향도 파악 후 삭제 권고
점검대상 및 판단기준	
대상	■ SOLARIS, LINUX, AIX, HP-UX 등
판단기준	**양호 :** 불필요한 계정이 존재하지 않는 경우
	취약 : 불필요한 계정이 존재하는 경우
조치방법	현재 등록된 계정 현황 확인 후 불필요한 계정 삭제
점검 및 조치 사례	

OS별 점검 파일 위치 및 점검 방법	
SOLARIS, LINUX, AIX, HP-UX	Step 1) 미사용 계정 및 의심스러운 계정 존재 여부 확인 (※ "passwd" 파일 구조: 부록 참조) `#cat /etc/passwd` Step 2) 사용하지 않는 Default 계정 점검 (lp, uucp, nuucp 계정 존재 확인 예시) `#cat /etc/passwd | egrep "lp|uucp|nuucp"`
LOG를 통한 확인	Step 1) 최근 로그인하지 않은 계정 및 의심스러운 계정 확인 `#cat /var/adm/wtmp` (SOLARIS, AIX, HP-UX) `#cat /var/log/wtmp` (LINUX) `#cat /var/adm/authlog` (AIX, HP-UX) `#cat /var/log/authlog` (SOLARIS) `#cat /var/adm/sulog` (SOLARIS, AIX, HP-UX) `#cat /var/log/sulog` (LINUX) ※ 파일의 위치는 버전마다 다를 수 있음
위에 제시한 점검 방법에 의해 불필요한 계정 발견 시 아래의 보안설정방법에 따라 조치함	

U-49 (하)	1. 계정관리 > 1.10 불필요한 계정 제거

■ **SOLARIS, LINUX, HP-UX**

Step 1) 서버에 등록된 불필요한 사용자 계정 확인

Step 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**

Step 1) 서버에 등록된 불필요한 사용자 계정 확인

Step 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	일반적인 경우 영향 없음

UNIX 서버

U-50 (하)	1. 계정관리 > 1.11 관리자 그룹에 최소한의 계정 포함
취약점 개요	
점검내용	■ 시스템 관리자 그룹에 최소한(root 계정과 시스템 관리에 허용된 계정)의 계정만 존재하는지 점검
점검목적	■ 관리자 그룹에 최소한의 계정만 존재하는지 점검하여 취약한 계정 관리로 발생하는 시스템 침입에 잘 대비되어 있는지 확인하기 위함
보안위협	■ 시스템을 관리하는 root 계정이 속한 그룹은 시스템 운영 파일에 대한 접근 권한이 부여되어 있으므로 해당 관리자 그룹에 속한 계정이 비인가자에게 유출될 경우 관리자 권한으로 시스템에 접근하여 계정 정보 유출, 환경설정 파일 및 디렉터리 변조 및 삭제 등의 행위를 하여 시스템 가용성(서비스 다운, 악성코드 유포지 감염)에 영향을 미칠 수 있는 위협이 존재함
참고	-
점검대상 및 판단기준	
대상	■ SOLARIS, LINUX, AIX, HP-UX 등
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
점검 및 조치 사례	

OS별 점검 파일 위치 및 점검 방법	
SOLARIS, 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	

■ SOLARIS, LINUX, HP-UX

Step 1) vi 편집기를 이용하여 "/etc/group" 파일 열기

Step 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`

U-50 (하)	1. 계정관리 > 1.11 관리자 그룹에 최소한의 계정 포함

■ **AIX**

Step 1) vi 편집기를 이용하여 "/etc/group" 파일 열기

Step 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	일반적인 경우 영향 없음

UNIX 서버

U-51 (하)	1. 계정관리 > 1.12 계정이 존재하지 않는 GID 금지
취약점 개요	
점검내용	■ 그룹(예 /etc/group) 설정 파일에 불필요한 그룹(계정이 존재하지 않고 시스템 관리나 운용에 사용되지 않는 그룹, 계정이 존재하고 시스템 관리나 운용에 사용되지 않는 그룹 등)이 존재하는지 점검
점검목적	■ 시스템에 불필요한 그룹이 존재하는지 점검하여 불필요한 그룹의 소유권으로 설정되어 있는 파일의 노출에 의해 발생할 수 있는 위험에 대한 대비가 되어 있는지 확인하기 위함
보안위협	■ 시스템에 불필요한 그룹이 존재할 경우 해당 그룹 소유의 파일이 비인가자에게 노출될 수 있는 위험이 존재함
참고	※ **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. ※ /etc/group 파일만으로 구성원이 없는 group이라 판단하기 힘듦. /etc/passwd와 /etc/group을 같이 확인하여 판단하기를 권고
점검대상 및 판단기준	
대상	■ SOLARIS, LINUX, AIX, HP-UX 등
판단기준	**양호 :** 시스템 관리나 운용에 불필요한 그룹이 삭제 되어있는 경우
	취약 : 시스템 관리나 운용에 불필요한 그룹이 존재할 경우
조치방법	불필요한 그룹이 있을 경우 관리자와 검토하여 제거
점검 및 조치 사례	

OS별 점검 파일 위치 및 점검 방법	
SOLARIS, LINUX, HP-UX, AIX	`#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

U-51 (하)	1. 계정관리 > 1.12 계정이 존재하지 않는 GID 금지
LINUX	#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 다음 같은 구조로 구성됨 [그룹명 : 패스워드 : 관리자, 관리자, … : 멤버, 멤버 …]
불필요한(계정이 존재하지 않고 시스템 관리나 운용에 사용되지 않는 그룹, 계정이 존재하고 시스템 관리나 운용에 사용되지 않는 그룹 등) 그룹이 존재하는 경우 아래의 보안설정방법에 따라 그룹을 제거함	
■ **SOLARIS, LINUX, AIX, HP-UX** #groupdel <group_name> ※ 구성원이 없거나, 더 이상 사용하지 않는 그룹명 삭제	
조치 시 영향	일반적인 경우 영향 없음

UNIX 서버

U-52 (중)	1. 계정관리 > 1.13 동일한 UID 금지
취약점 개요	
점검내용	■ /etc/passwd 파일 내 UID가 동일한 사용자 계정 존재 여부 점검
점검목적	■ 동일 UID로 설정된 사용자 계정을 점검함으로써 타 사용자 계정 소유의 파일 및 디렉터리로의 악의적 접근 예방 및 침해사고 시 명확한 감사추적을 목적으로 함
보안위협	■ 동일한 UID의 다른 사용자 계정을 가진 사용자가 타 사용자 권한으로 시스템 접근이 가능하고 침해사고 시 UID 중복으로 인한 권한 중복으로 사용자 감사 추적이 어려움
참고	※ **UID**(User Identification): 여러 명의 사용자가 동시에 사용하는 시스템에서 사용자가 자신을 대표하기 위해 쓰는 이름 ※ 패스워드 파일 수정 변경 및 신규 사용자 추가 시 UID가 동일한 계정이 존재하는지 확인해야 함
점검대상 및 판단기준	
대상	■ SOLARIS, LINUX, AIX, HP-UX 등
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
점검 및 조치 사례	

OS별 점검 파일 위치 및 점검 방법

SOLARIS, LINUX, HP-UX, AIX

`#cat /etc/passwd` (※ "passwd" 파일 구조: 부록 참조)

```
[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
```

동일한 UID를 갖는 계정이 존재하는 경우 아래의 보안설정방법에 따라 설정을 변경함

■ SOLARIS, 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	일반적인 경우 영향 없음

U-53 (하)	1. 계정관리 > 1.14 사용자 shell 점검
취약점 개요	
점검내용	■ 로그인이 불필요한 계정(adm, sys, daemon 등)에 쉘 부여 여부 점검
점검목적	■ 로그인이 불필요한 계정에 쉘 설정을 제거하여, 로그인이 필요하지 않은 계정을 통한 시스템 명령어를 실행하지 못하게 하기 위함
보안위협	■ 로그인이 불필요한 계정은 일반적으로 OS 설치 시 기본적으로 생성되는 계정으로 쉘이 설정되어 있을 경우, 공격자는 기본 계정들을 통하여 중요파일 유출이나 악성코드를 이용한 root 권한 획득 등의 공격을 할 수 있음
참고	※ **쉘(Shell):** 대화형 사용자 인터페이스로써, 운영체제(OS) 가장 외곽계층에 존재하여 사용자의 명령어를 이해하고 실행함
점검대상 및 판단기준	
대상	■ SOLARIS, LINUX, AIX, HP-UX 등
판단기준	**양호 :** 로그인이 필요하지 않은 계정에 /bin/false(/sbin/nologin) 쉘이 부여되어 있는 경우
	취약 : 로그인이 필요하지 않은 계정에 /bin/false(/sbin/nologin) 쉘이 부여되지 않은 경우
조치방법	로그인이 필요하지 않은 계정에 대해 /bin/false(/sbin/nologin) 쉘 부여
점검 및 조치 사례	

OS별 점검 파일 위치 및 점검 방법

SOLARIS, LINUX, HP-UX, AIX

```
#cat /etc/passwd | egrep
"^daemon|^bin|^sys|^adm|^listen|^nobody|^nobody4|^noacces
s|^diag|^operator|^games|^gopher" | grep -v "admin"
```

```
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
```

시스템에 불필요한 계정을 확인한 후 /bin/false(nologin) 쉘이 부여되어 있지 않은 경우 아래의 보안설정방법에 따라 설정을 변경함
(※ 불필요한 계정은 시스템 용도에 따라 차이가 있음)

UNIX 서버

U-53 (하)	1. 계정관리 > 1.14 사용자 shell 점검

■ **SOLARIS, LINUX, AIX, HP-UX**

Step 1) vi 편집기를 이용하여 "/etc/passwd" 파일 열기

Step 2) 로그인 쉘 부분인 계정 맨 마지막에 /bin/false(/sbin/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

U-54 (하)	1. 계정관리 > 1.15 Session Timeout 설정
취약점 개요	
점검내용	■ 사용자 쉘에 대한 환경설정 파일에서 session timeout 설정 여부 점검
점검목적	■ 사용자의 고의 또는 실수로 시스템에 계정이 접속된 상태로 방치됨을 차단하기 위함
보안위협	■ Session timeout 값이 설정되지 않은 경우 유휴 시간 내 비인가자의 시스템 접근으로 인해 불필요한 내부 정보의 노출 위험이 존재함
참고	※ **session:** 프로세스들 사이에 통신을 수행하기 위해서 메시지 교환을 통해 서로를 인식한 이후부터 통신을 마칠 때까지의 시간
점검대상 및 판단기준	
대상	■ SOLARIS, LINUX, AIX, HP-UX 등
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
점검 및 조치 사례	

OS별 점검 파일 위치 및 점검 방법	
SOLARIS, LINUX, AIX, HP-UX	<sh, ksh, bash 사용 시> `#cat /etc/profile(.profile)` `TMOUT=600` `export TMOUT` <csh 사용 시> `#cat /etc/csh.login` 또는, `#cat /etc/csh.cshrc` `set autologout=10`
위에 제시한 설정이 해당 파일에 적용되지 않은 경우 아래의 보안설정방법에 따라 설정을 변경함	

■ **SOLARIS, LINUX, AIX, HP-UX**

- sh(born shell), ksh(korn shell), bash(born again shell)을 사용하는 경우 -

Step 1) vi 편집기를 이용하여 "/etc/profile(.profile)" 파일 열기

Step 2) 아래와 같이 수정 또는, 추가

`TMOUT=600` (단위: 초)

export TMOUT

- csh 을 사용하는 경우 -

Step 1) vi 편집기를 이용하여 "/etc/csh.login" 또는, "/etc/csh.cshrc" 파일 열기

Step 2) 아래와 같이 수정 또는, 추가

`set autologout=10` (단위: 분)

조치 시 영향	모니터링 용도일 경우 세션 타임 설정 시 모니터링 업무가 불가 할 수 있으므로 예외처리 필요

UNIX 서버

U-55 (하)	2. 파일 및 디렉토리 관리 > 2.15 hosts.lpd 파일 소유자 및 권한 설정
취약점 개요	
점검내용	■ /etc/hosts.lpd 파일의 삭제 및 권한 적절성 점검
점검목적	■ 비인가자의 임의적인 hosts.lpd 변조를 막기 위해 hosts.lpd 파일 삭제 또는 소유자 및 권한 관리를 해야 함
보안위협	■ hosts.lpd 파일의 접근권한이 적절하지 않을 경우 비인가자가 /etc/hosts.lpd 파일을 수정하여 허용된 사용자의 서비스를 방해할 수 있으며, 호스트 정보를 획득 할 수 있음
참고	※ **hosts.lpd 파일:** 로컬 프린트 서비스를 사용할 수 있는 허가된 호스트(사용자) 정보를 담고 있는 파일 (hostname 또는, IP 주소를 포함하고 있음)
점검대상 및 판단기준	
대상	■ SOLARIS, LINUX, AIX, HP-UX 등
판단기준	**양호 :** hosts.lpd 파일이 삭제되어 있거나 불가피하게 hosts.lpd 파일을 사용할 시 파일의 소유자가 root이고 권한이 600인 경우
	취약 : hosts.lpd 파일이 삭제되어 있지 않거나 파일의 소유자가 root가 아니고 권한이 600이 아닌 경우
조치방법	hosts.lpd 파일을 삭제하거나 hosts.lpd 파일의 퍼미션을 확인하여 퍼미션 600, 파일 소유자를 root로 변경
점검 및 조치 사례	

OS별 점검 파일 위치 및 점검 방법	
SOLARIS, LINUX, AIX, HP-UX	`#ls -l /etc/hosts.lpd` `rw------- root <hosts.lpd 파일>`
"hosts.lpd" 파일이 존재하고 소유자가 root가 아니거나 파일의 권한이 600이 아닌 경우 아래의 보안설정방법에 따라 설정을 변경함	

■ SOLARIS, LINUX, AIX, HP-UX

Step 1) hosts.lpd 파일 삭제

```
#rm -rf /etc/hosts.lpd
```

Step 2) 파일의 퍼미션 변경 (hosts.lpd 파일이 필요시)

```
#chmod 600 /etc/hosts.lpd
```

Step 3) 소유자를 root로 변경 (hosts.lpd 파일이 필요시)

```
#chown root /etc/hosts.lpd
```

조치 시 영향	일반적인 경우 영향 없음

U-56 (중)	2. 파일 및 디렉토리 관리 > 2.16 NIS 서비스 비활성화
취약점 개요	
점검내용	■ NIS 서비스 비활성화 여부 점검
점검목적	■ 안전하지 않은 NIS 서비스를 이용 시 네트워크 상에 암호화되지 않은 중요 정보 전달을 방지하기 위함
보안위협	■ NIS 이용 시 호스트 인증 메커니즘이 없으며 암호 해시를 포함한 모든 정보를 네트워크 상에서 암호화되지 않은 채로 전달되어 스니핑(sniffing) 가능 우려
참고	※ **NIS 서비스:** ypserv 라고 불리는 RPC 서비스로 동일한 도메인에 위치한 컴퓨터에 사용자명, 암호와 다른 기밀 정보를 배포하는 기능을 함 ※ 관련 점검 항목 : U-28(상)
점검대상 및 판단기준	
대상	■ SOLARIS, LINUX, AIX, HP-UX 등
판단기준	**양호 :** 불필요한 NIS 서비스가 비활성화 되어있는 경우
	취약 : 불필요한 NIS 서비스가 활성화 되어있는 경우
조치방법	NIS 서비스를 사용하지 않는 경우 NIS 서비스 비활성화
점검 및 조치 사례	

OS별 점검 파일 위치 및 점검 방법	
SOLARIS, LINUX, AIX, HP-UX	NIS 서비스 활성화 여부 확인 `#ps –ef | grep yp`
불필요한 “NIS” 서비스가 실행중인 경우 아래의 보안설정방법에 따라 비활성화 상태로 변경함	

■ LINUX, AIX, SOLARIS 5.9 이하 버전

Step 1) NFS 서비스 데몬 중지

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

Step 2) 시동 스크립트 삭제 또는, 스크립트 이름 변경

1.. 위치 확인

```
#ls -al /etc/rc.d/rc*.d/* | egrep "ypserv|ypbind|ypxfrd|rpc.yppasswdd
 | rpc.ypupdated”
```

2. 이름 변경

```
#mv /etc/rc.d/rc2.d/S73ypbind /etc/rc.d/rc2.d/_S73ypbind
```

U-56 (중)	2. 파일 및 디렉토리 관리 > 2.16 NIS 서비스 비활성화

■ **HP-UX**

Step 1) NFS 서비스 데몬 중지

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

Step 2) 시동 스크립트 삭제 또는, 스크립트 이름 변경

1. 위치 확인

```
#ls -al /etc/rc.d/rc*.d/* | egrep "ypserv|ypbind|ypxfrd|rpc.yppasswdd
 | rpc.ypupdated"
```

2. /etc/rc.config.d/namesvrs 파일에서 NIS_MASTER_SERVER, NIS_SLAVE_SERVER, NIS_CLIENT 값을 0으로 설정

```
NIS_MASTER_SERVER=0
NIS_SLAVE_SERVER=0
NIS_CLIENT_SERVER=0
```

■ **SOLARIS 5.10 이상 버전**

Step 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
```

Step 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
```

※ NIS 사용이 반드시 필요 시 NIS+ 사용

조치 시 영향	일반적인 경우 영향 없음

U-57 (중)	2. 파일 및 디렉토리 관리 > 2.17 UMASK 설정 관리
취약점 개요	
점검내용	■ 시스템 UMASK 값이 022 이상인지 점검
점검목적	■ 잘못 설정된 UMASK 값으로 인해 신규 파일에 대한 과도한 권한 부여되는 것을 방지하기 위함
보안위협	■ 잘못된 UMASK 값으로 인해 시스템 내 신규 생성 파일에 대하여 과도한 권한이 부여될 수 있으며, 이로 인해 파일의 시스템 악용이 우려됨
참고	■ 시스템 내에서 사용자가 새로 생성하는 파일의 접근권한은 UMASK 값에 따라 정해지며, 계정의 Start Profile 에 명령을 추가하면 사용자가 로그인 한 후에도 변경된 UMASK 값을 적용받게 됨 ※ **Start Profile:** /etc/profile, /etc/default/login, .cshrc, .kshrc, .bashrc, .login, .profile 등 ※ **umask:** 파일 및 디렉터리 생성 시 기본 퍼미션을 지정해 주는 명령어
점검대상 및 판단기준	
대상	■ SOLARIS, Linux, AIX, HP-UX 등
판단기준	**양호 :** UMASK 값이 022 이상으로 설정된 경우
	취약 : UMASK 값이 022 이상으로 설정되지 않은 경우
조치방법	설정파일에 UMASK 값을 "022"로 설정
점검 및 조치 사례	

OS별 점검 파일 위치 및 점검 방법	
SOLARIS, LINUX, AIX, HP-UX	`#vi /etc/profile` `UMASK=022`
위에 제시한 UMASK 값이 해당 파일에 적용되지 않은 경우 아래의 보안설정방법에 따라 적용함	

■ **SOLARIS**

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

Step 1) vi 편집기를 이용하여 "/etc/profile" 파일 열기

Step 2) 아래와 같이 수정 또는, 신규 삽입

```
umask 022
export umask
```

방법-2. "/etc/default/login" 파일을 이용한 UMASK 설정 변경

Step 1) vi 편집기를 이용하여 "/etc/default/login" 파일 열기

UNIX 서버

U-57 (중)	2. 파일 및 디렉토리 관리 > 2.17 UMASK 설정 관리

Step 2) 아래와 같이 수정 또는, 신규 삽입

(수정 전) #UMASK=022

(수정 후) UMASK=022

■ **LINUX**

Step 1) vi 편집기를 이용하여 "/etc/profile" 파일 열기

Step 2) 아래와 같이 수정 또는, 신규 삽입

```
umask 022
export umask
```

■ **HP-UX**

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

Step 1) vi 편집기를 이용하여 "/etc/profile" 파일 열기

Step 2) 아래와 같이 수정 또는, 신규 삽입

```
umask 022
export umask
```

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

Step 1) vi 편집기를 이용하여 "/etc/defualt/security" 파일 열기

Step 2) default 설정 부분을 아래와 같이 수정 또는, 신규 삽입

(수정 전) # UMASK=022

(수정 후) UMASK=022

■ **AIX**

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

Step 1) vi 편집기를 이용하여 "/etc/profile" 파일 열기

Step 2) 아래와 같이 수정 또는, 신규 삽입

```
umask 022
export umask
```

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

Step 1) vi 편집기를 이용하여 "/etc/security/user" 파일 열기

Step 2) default 설정 부분을 아래와 같이 수정 또는, 신규 삽입

(수정 전) umask =

(수정 후) umask = 022

조치 시 영향	일반적인 경우 영향 없음

U-58 (중)	2. 파일 및 디렉토리 관리 > 2.18 홈디렉토리 소유자 및 권한 설정
취약점 개요	
점검내용	■ 홈 디렉터리의 소유자 외 타사용자가 해당 홈 디렉터리를 수정할 수 없도록 제한하는지 점검
점검목적	■ 사용자 홈 디렉터리 내 설정파일이 비인가자에 의한 변조를 방지함
보안위협	■ 홈 디렉터리 내 설정파일 변조 시 정상적인 서비스 이용이 제한될 우려가 존재함
참고	-
점검대상 및 판단기준	
대상	■ SOLARIS, LINUX, AIX, HP-UX 등
판단기준	**양호 :** 홈 디렉터리 소유자가 해당 계정이고, 타 사용자 쓰기 권한이 제거된 경우
	취약 : 홈 디렉터리 소유자가 해당 계정이 아니고, 타 사용자 쓰기 권한이 부여된 경우
조치방법	사용자별 홈 디렉터리 소유주를 해당 계정으로 변경하고, 타사용자의 쓰기 권한 제거 ("/etc/passwd" 파일에서 홈 디렉터리 확인, 사용자 홈 디렉터리 외 개별적으로 만들어 사용하는 사용자 디렉터리 존재여부 확인하여 점검)
점검 및 조치 사례	

OS별 점검 파일 위치 및 점검 방법	
SOLARIS, 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	

■ **SOLARIS, 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	일반적인 경우 영향 없음

UNIX 서버

U-59 (중)	2. 파일 및 디렉토리 관리 > 2.19 홈디렉토리로 지정한 디렉토리의 존재 관리
취약점 개요	
점검내용	■ 사용자 계정과 홈 디렉터리의 일치 여부를 점검
점검목적	■ /home 이외 사용자의 홈 디렉터리 존재 여부를 점검하여 비인가자가 시스템 명령어의 무단 사용을 방지하기 위함
보안위협	■ 사용자에게 지정된 디렉터리가 아닌 곳이 홈 디렉터리로 설정될 경우 해당 디렉터리 내 명령어 사용이 가능하며 이에 따라 시스템 관리·보안상 문제가 발생할 수 있음
참고	※ **홈디렉터리:** 사용자가 로그인한 후 작업을 수행하는 디렉터리 ※ **일반 사용자의 홈 디렉터리 위치:** /home/user명
점검대상 및 판단기준	
대상	■ SOLARIS, LINUX, AIX, HP-UX 등
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
점검 및 조치 사례	

OS별 점검 파일 위치 및 점검 방법	
SOLARIS, 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	

■ SOLARIS, LINUX, AIX, HP-UX

Step 1) 홈 디렉터리가 없는 사용자 계정 삭제

- SOLARIS, LINUX, HP-UX 설정: `#userdel <user_name>`
- AIX 설정: `#rmuser <user_name>`

Step 2) 홈 디렉터리가 없는 사용자 계정에 홈 디렉터리 지정

```
#vi /etc/passwd
#test:x:501:501::/:/bin/bash (홈 디렉터리가 /로 설정 된 경우)
#test:x:501:501::/home/test:/bin/bash (홈 디렉터리 수정 / -> /home/test)
```

조치 시 영향	일반적인 경우 영향 없음

U-60 (하)	2. 파일 및 디렉토리 관리 > 2.20 숨겨진 파일 및 디렉토리 검색 및 제거
취약점 개요	
점검내용	■ 숨김 파일 및 디렉터리 내 의심스러운 파일 존재 여부 점검
점검목적	■ 숨겨진 파일 및 디렉터리 중 의심스러운 내용은 정상 사용자가 아닌 공격자에 의해 생성되었을 가능성이 높음으로 이를 발견하여 제거함
보안위협	■ 공격자는 숨겨진 파일 및 디렉터리를 통해 시스템 정보 습득, 파일 임의 변경 등을 할 수 있음
참고	-
점검대상 및 판단기준	
대상	■ SOLARIS, Linux, AIX, HP-UX 등
판단기준	**양호 :** 불필요하거나 의심스러운 숨겨진 파일 및 디렉터리를 삭제한 경우
	취약 : 불필요하거나 의심스러운 숨겨진 파일 및 디렉터리를 방치한 경우
조치방법	ls –al 명령어로 숨겨진 파일 존재 파악 후 불법적이거나 의심스러운 파일을 삭제함
점검 및 조치 사례	

OS별 점검 파일 위치 및 점검 방법	
SOLARIS, LINUX, AIX, HP-UX	특정 디렉터리 내 불필요한 파일 점검 `#ls -al [디렉터리명]` 전체 숨김 디렉터리 및 숨김 파일 점검 `#find / -type f –name ".*"` (파일 점검) `#find / -type d -name ".*"` (디렉터리 점검)
특정 디렉터리 내 숨겨진 파일을 확인한 후 불필요한 경우 파일 삭제를 권고함	

■ SOLARIS, LINUX, AIX, HP-UX

Step 1) 숨겨진 파일 목록에서 불필요한 파일 삭제

Step 2) 마지막으로 변경된 시간에 따라, 최근 작업한 파일 확인 시 [-t] 플래그 사용

조치 시 영향	일반적인 경우 영향 없음

UNIX 서버

U-61 (중)	3. 서비스 관리 > 3.24 ssh 원격접속 허용
취약점 개요	
점검내용	■ 원격 접속 시 SSH 프로토콜을 사용하는지 점검
점검목적	■ 비교적 안전한 SSH 프로토콜을 사용함으로써 스니핑 등 아이디/패스워드의 누출의 방지를 목적으로 함
보안위협	■ 원격 접속 시 Telnet, FTP 등은 암호화되지 않은 상태로 데이터를 전송하기 때문에 아이디/패스워드 및 중요 정보가 외부로 유출될 위험성이 있음
참고	※ SSH 사용 시 TCP/22번 포트를 기본 포트로 사용하기 때문에 공격자가 기본 포트를 통하여 공격을 시도할 수 있으므로 기본 포트를 변경하여 사용하는 것을 권고함
점검대상 및 판단기준	
대상	■ SOLARIS, LINUX, AIX, HP-UX 등
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
점검 및 조치 사례	

■ **SOLARIS, LINUX, AIX, HP-UX**

Step 1) SSH 서비스 활성화 명령어 실행

- **SOLARIS**

<SOLARIS 5.9 이하 버전>

```
#/etc/init.d/sshd start
```

<SOLARIS 5.10 이상 버전>

```
#svcadm enable ssh
```

- **LINUX**

```
#service start sshd 또는, #service start ssh
```

- **AIX**

```
#startsrc -s sshd
```

- **HP-UX**

```
#/sbin/init.d/secsh start
```

Step 2) SSH 설치가 필요할 경우 각 OS 벤더사로부터 SSH 서비스 설치 방법을 문의한 후 서버에 설치

조치 시 영향	일반적인 경우 영향 없음

U-62 (하)	3. 서비스 관리 > 3.25 ftp 서비스 확인
취약점 개요	
점검내용	■ FTP 서비스가 활성화 되어있는지 점검
점검목적	■ 취약한 서비스인 FTP서비스를 가급적 제한함을 목적으로 함
보안위협	■ FTP 서비스는 아이디 및 패스워드가 암호화되지 않은 채로 전송되어 스니핑이 가능함
참고	※ 기반시설 시스템에서 ftp 서비스의 이용은 원칙적으로 금지하나, 부득이 해당 기능을 활용해야 하는 경우 SFTP 사용을 권고함
점검대상 및 판단기준	
대상	■ SOLARIS, LINUX, AIX, HP-UX 등
판단기준	**양호 :** FTP 서비스가 비활성화 되어 있는 경우
	취약 : FTP 서비스가 활성화 되어 있는 경우
조치방법	FTP 서비스 중지
점검 및 조치 사례	

FTP 종류별 점검 방법	
SOLARIS, AIX, HP-UX	일반 ftp 서비스 비활성화 여부 확인 `#vi /etc/inetd.conf`
	proftpd 서비스 데몬 확인 (proftpd 동직 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`
LINUX	일반 ftp 서비스 비활성화 여부 확인 `#ps -ef | grep ftp`
	vsftpd 또는 ProFTP 서비스 데몬 확인(vsftpd, proftpd 동작 SID 확인) `#ps -ef | egrep "vsftpd|proftp"` `root 3809 3721 0 08:44:40 ? 0:00 /usr/sbin/vsftpd`
불필요한 "ftp" 서비스 실행 시 아래의 보안설정방법에 따라 서비스 중지	

U-62 (하)	3. 서비스 관리 > 3.25 ftp 서비스 확인

■ **SOLARIS, AIX, HP-UX**

< 일반 FTP 서비스 중지 방법 >

Step 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
```

Step 2) inetd 서비스 재시작

```
#ps -ef | grep inetd
 root 141 1 0 15:03:22 ? 0:01 /usr/sbin/inetd -s
#kill –HUP [PID]
```

<SOLARIS 5.10 이상 버전>

```
# svcs | grep ftp
  online                12:51:49      svc:/network/ftp:default
# svcadm disable svc:/network/ftp:default
```

■ **SOLARIS, LINUX, AIX, HP-UX**

< vsFTP, ProFTP 서비스 중지 방법 >

Step 1) 서비스 확인

```
# ps –ef | egrep "vsftpd|proftpd"
```

Step 2) vsftpd 또는 ProFTP 서비스 데몬 중지

```
# service vsftpd(proftp) stop 또는 /etc/rc.d/init.d/vsftpd(proftp)
  stop 또는 kill –9 [PID]
```

조치 시 영향	일반적인 경우 영향 없음

U-63 (중)	3. 서비스 관리 > 3.26 ftp 계정 shell 제한
취약점 개요	
점검내용	■ ftp 기본 계정에 쉘 설정 여부 점검
점검목적	■ FTP 서비스 설치 시 기본으로 생성되는 ftp 계정은 로그인이 필요하지 않은 계정으로 쉘을 제한하여 해당 계정으로의 시스템 접근을 차단하기 위함
보안위협	■ 불필요한 기본 계정에 쉘(Shell)을 부여할 경우, 공격자에게 해당 계정이 노출되어 ftp 기본 계정으로 시스템 접근하여 공격이 가능해짐
참고	※ **쉘(Shell):** 대화형 사용자 인터페이스로써, 운영체제(OS) 가장 외곽계층에 존재하여 사용자의 명령어를 이해하고 실행함 ※ 기반시설 시스템에서 ftp 서비스의 이용은 원칙적으로 금지하나, 부득이 해당 기능을 활용해야 하는 경우 shell 제한 등의 보안 조치를 반드시 적용하여야 함 ※ 관련 점검 항목 : U-64(하), U-65(중)
점검대상 및 판단기준	
대상	■ SOLARIS, LINUX, AIX, HP-UX 등
판단기준	**양호 :** ftp 계정에 /bin/false 쉘이 부여되어 있는 경우
	취약 : ftp 계정에 /bin/false 쉘이 부여되어 있지 않은 경우
조치방법	ftp 계정에 /bin/false 쉘 부여
점검 및 조치 사례	

OS별 점검 파일 위치 및 점검 방법	
SOLARIS, 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	

■ SOLARIS, LINUX, AIX, HP-UX

Step 1) vi 편집기를 이용하여 "/etc/passwd" 파일 열기

Step 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

Step 3) # usermod –s /bin/false [계정ID] 부여로 변경 가능

* Step 2 로 적용이 되지 않을경우는 Step3의 usermod 명령어를 사용하여 쉘 변경

조치 시 영향	일반적인 경우 영향 없음

UNIX 서버

U-64 (하)	3. 서비스 관리 > 3.27 ftpusers 파일 소유자 및 권한 설정
취약점 개요	
점검내용	■ FTP 접근제어 설정파일에 관리자 외 비인가자들이 수정 제한 여부 점검
점검목적	■ 비인가자가의 ftpusers 파일 수정을 막아 비인가자들의 ftp 접속을 차단하기 위해 ftpusers 파일 소유자 및 권한을 관리해야함
보안위협	■ 해당 파일에 대한 권한 관리가 이루어지지 않을 시 비인가자의 FTP 접근을 통해 계정을 등록하고 서버에 접속하여 침해사고가 발생할 수 있음
참고	※ **ftpusers 파일:** FTP 접근제어 설정파일로써 해당 파일에 등록된 계정은 ftp에 접속할 수 없음 ※ 기반시설 시스템에서 ftp 서비스의 이용은 원칙적으로 금지하나, 부득이 해당 기능을 활용해야 하는 경우 shell 제한 등의 보안 조치를 반드시 적용하여야 함 ※ 관련 점검 항목 : U-63(중), U-65(중)
점검대상 및 판단기준	
대상	■ SOLARIS, LINUX, AIX, HP-UX 등
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)
점검 및 조치 사례	

OS별 점검 파일 위치 및 점검 방법	
SOLARIS, 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`

U-64 (하)	3. 서비스 관리 > 3.27 ftpusers 파일 소유자 및 권한 설정

■ **SOLARIS, LINUX, AIX, HP-UX**

Step 1) "/etc/ftpusers" 파일의 소유자 및 권한 확인

```
#ls -l /etc/ftpusers
```

Step 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.user_list 또는 ftpusers, user_list 파일의 소유자 및 권한 확인 후 변경
(ftpusers, user_list 파일에 등록된 모든 계정의 접속이 차단됨)

(2) vsftpd.conf 파일에서 userlist_enable=NO 또는, 옵션 설정이 없는 경우: vsftpd.ftpusers 또는 ftpusers 파일의 소유자 및 권한 확인 후 변경
(ftpusers 파일에 등록된 계정들만 접속이 차단됨)

조치 시 영향	일반적인 경우 영향 없음

UNIX 서버

U-65 (중)	3. 서비스 관리 > 3.28 ftpusers 파일 설정
취약점 개요	
점검내용	■ FTP 서비스를 사용할 경우 ftpusers 파일 root 계정이 포함 여부 점검
점검목적	■ root의 FTP 직접 접속을 방지하여 root 패스워드 정보를 노출되지 않도록 하기 위함
보안위협	■ FTP 서비스는 아이디 및 패스워드가 암호화되지 않은 채로 전송되어 스니핑에 의해서 아이디 및 패스워드가 노출될 수 있음
참고	※ **스니핑:** 컴퓨터 네트워크상에 흘러 다니는 트래픽을 도청하는 행위 ※ 기반시설 시스템에서 ftp 서비스의 이용은 원칙적으로 금지하나, 부득이 해당 기능을 활용해야 하는 경우 shell 제한 등의 보안 조치를 반드시 적용하여야 함 ※ 관련 점검 항목 : U-63(중), U-64(하)
점검대상 및 판단기준	
대상	■ SOLARIS, LINUX, AIX, HP-UX 등
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)
점검 및 조치 사례	

FTP 종류별 점검 방법	
SOLARIS, 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.conf` `RootLogin on`
	vsFTP `#cat /etc/vsftp/ftpusers` `#cat /etc/vsftp/user_list` 또는 `#cat /etc/vsftpd.ftpusers` `#cat /etc/vsftpd.user_list` `#root` (주석처리) 또는, `root` 계정 미등록
root 계정으로 FTP 접속이 가능하도록 위와 같이 설정된 경우 아래의 보안설정방법에 따라 설정을 변경함	

U-65 (중)	3. 서비스 관리 > 3.28 ftpusers 파일 설정

■ **SOLARIS, LINUX, AIX, HP-UX**

< 일반 FTP 서비스 root 계정 접속 제한 방법 >

Step 1) vi 편집기를 이용하여 ftpusers 파일 열기 (“/etc/ftpusers” 또는 “/etc/ftpd/ftpusers”)

```
#vi /etc/ftpusers 또는 /etc/ftpd/ftpusers
```

Step 2) ftpusers 파일에 root 계정 추가 또는, 주석제거

(수정 전) #root 또는, root 계정 미등록

(수정 후) root

< ProFTP 서비스 ROOT 접속 차단 >

Step 1) vi 편집기를 이용하여 proftpd 설정파일(“/etc/proftpd.conf”) 열기

```
#vi /etc/proftpd.conf
```

Step 2) proftpd 설정파일 (“/etc/proftpd.conf”)에서 RootLogin off 설정

(수정 전) RootLogin on

(수정 후) RootLogin off

Step 3) ProFTP 서비스 재시작

< vsFTP 서비스 ROOT 접속 차단 >

Step 1) vi 편집기를 이용하여 ftpusers 파일 열기 (“/etc/vsftp/ftpusers” 또는, “/etc/vsftpd.ftpusers”)

```
#vi /etc/vsftp/ftpusers
```

Step 2) ftpusers 파일에 root 계정 추가 또는, 주석제거

(수정 전) #root 또는, root 계정 미등록

(수정 후) root

Step 3) vsFTP 서비스 재시작

※ vsFTP를 사용할 경우 FTP 접근제어 파일

(1) vsftpd.conf 파일에서 userlist_enable=YES인 경우: vsftpd.ftpusers, vsftpd.user_list 또는 ftpusers, user_list
(ftpusers, user_list 파일에 등록된 모든 계정의 접속이 차단됨)

(2) vsftpd.conf 파일에서 userlist_enable=NO 또는, 옵션 설정이 없는 경우: vsftpd.ftpusers 또는 ftpusers
(ftpusers 파일에 등록된 계정들만 접속이 차단됨)

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

UNIX 서버

U-66 (중)	3. 서비스 관리 > 3.29 at 파일 소유자 및 권한 설정
취약점 개요	
점검내용	■ 관리자(root)만 at.allow파일과 at.deny 파일을 제어할 수 있는지 점검
점검목적	■ at 명령어 사용자 제한은 at.allow 파일과 at.deny 파일에서 할 수 있으므로 보안상 해당 파일에 대한 접근제한이 필요함
보안위협	■ 해당 파일에 대한 권한 관리가 이루어지지 않을 시 공격자가 권한을 획득한 사용자 계정을 등록하여 불법적인 예약 파일 실행으로 시스템 피해가 발생할 수 있음
참고	※ **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 ※ 기반시설 시스템에서 at 데몬의 이용은 원칙적으로 금지하나, 부득이 해당 기능을 활용해야 하는 경우 소유자 및 권한 설정 등의 보안 조치를 반드시 적용하여야 함
점검대상 및 판단기준	
대상	■ SOLARIS, LINUX, AIX, HP-UX 등
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)
점검 및 조치 사례	

OS별 점검 파일 위치 및 점검 방법	
SOLARIS	“/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	

U-66 (중)	3. 서비스 관리 > 3.29 at 파일 소유자 및 권한 설정

■ **SOLARIS**

"/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
```

■ **LINUX**

"/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**

"/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

U-67 (중)	3. 서비스 관리 > 3.30 SNMP 서비스 구동 점검
취약점 개요	
점검내용	■ SNMP 서비스 활성화 여부 점검
점검목적	■ 불필요한 SNMP 서비스 활성화로 인해 필요 이상의 정보가 노출되는 것을 막기 위해 SNMP 서비스를 중지해야함
보안위협	■ SNMP 서비스로 인하여 시스템의 주요 정보 유출 및 정보의 불법수정이 발생할 수 있음
참고	※ **SNMP(Simple Network Management Protocol):** TCP/IP 기반 네트워크상의 각 호스트에서 정기적으로 여러 정보를 자동으로 수집하여 네트워크 관리를 하기 위한 프로토콜을 의미함 ※ 기반시설 시스템에서 SNMP 서비스의 이용은 원칙적으로 금지하나, 부득이 해당 기능을 활용해야 하는 경우 기본 Community String 변경, 네트워크 모니터링 등의 보안 조치를 반드시 적용하여야 함 ※ 관련 점검 항: U-68(중)
점검대상 및 판단기준	
대상	■ SOLARIS, LINUX, AIX, HP-UX 등
판단기준	**양호 :** SNMP 서비스를 사용하지 않는 경우
	취약 : SNMP 서비스를 사용하는 경우
조치방법	SNMP 서비스를 사용하지 않는 경우 서비스 중지 후 시작 스크립트 변경
점검 및 조치 사례	

OS별 점검 파일 위치 및 점검 방법	
SOLARIS	`#ps -ef | grep snmp` 또는 `#svcs -a | grep snmp`
LINUX, AIX, HP-UX	`#ps -ef | grep snmp`
불필요한 "SNMP" 서비스를 사용하지 않는 경우 중지함	

< 서비스 중지 방법 >

■ SOLARIS 5.9 이하

Step 1) `ps -ef | grep snmp`로 검색하여 위치 확인 후 이름 변경

Step 2) `#/etc/init.d/init.snmpdx stop`

Step 3) `#mv /etc/rc3.d/S76snmpdx /etc/rc3.d/_S76snmpdx` (rc*/_S**snmpdx 의 *수치는 각각 다름)

U-67 (중)	3. 서비스 관리 > 3.30 SNMP 서비스 구동 점검

■ **SOLARIS 5.10**

Step 1) `svcs -a | grep snmp` 명령으로 데몬 확인

Step 2) 데몬 활성화 확인

`#ps ef | grep snmp` 또는 `#svcs -a | grep snmp`

Step 3. `svcadm disable` 명령으로 데몬 중지

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

`svcadm disable svs:/application/management/dmi:default`

■ **LINUX, AIX, HP-UX 설정**

Step 1) `ps –ef | grep snmp`로 검색

```
root  2028     1  0  Nov 24  ?        0:00 /usr/sbin/snmpdm
```

Step 2) snmp 사용하지 않을 시 서비스 중지

<LINUX>

```
#service snmpd stop
```

<AIX>

Step 1) `#kill -9 [PID]`

Step 2) `vi /etc/rc.tcpip` 실행하여 다음 라인 #처리(주석처리)

(수정 전) `start /usr/sbin/snmpd "$src_running"`

(수정 후) `#start /usr/sbin/snmpd "$src_running"`

<HP-UX>

Step 1) `#kill -9 [PID]` 또는 `/sbin/SnmpAgtStart.d/S560SnmpMaster stop`

Step 2) `mv /sbin/SnmpAgtStart.d/S560SnmpMaster/sbin/SnmpAgtStart.d/_S560SnmpMaster`

조치 시 영향	일반적인 경우 영향 없음

UNIX 서버

U-68 (중)	3. 서비스 관리 > 3.31 SNMP 서비스 Community String의 복잡성 설정
취약점 개요	
점검내용	■ SNMP Community String 복잡성 설정 여부 점검
점검목적	■ Community String 기본 설정인 Public, Private는 공개된 내용으로 공격자가 이를 이용하여 SNMP 서비스를 통해 시스템 정보를 얻을 수 있기 때문에 Community String을 유추하지 못하도록 설정해야함
보안위협	■ Community String은 Default로 public, private로 설정된 경우가 많으며, 이를 변경하지 않으면 이 String을 악용하여 환경설정 파일 열람 및 수정을 통한 공격, 간단한 정보수집에서부터 관리자 권한 획득 및 Dos공격까지 다양한 형태의 공격이 가능함
참고	※ **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 ※ 기반시설 시스템에서 SNMP 서비스의 이용은 원칙적으로 금지하나, 부득이 해당 기능을 활용해야 하는 경우 기본 Comunity String 변경, 네트워크 모니터링 등의 보안 조치를 반드시 적용하여야 함
점검대상 및 판단기준	
대상	■ SOLARIS, LINUX, AIX, HP-UX
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
점검 및 조치 사례	

OS별 점검 파일 위치 및 점검 방법	
SOLARIS 9이하 버전	`#vi /etc/snmp/conf/snmpd.conf` `read-community public / write-community private`
SOLARIS 10이상 버전	`#vi /etc/sma/snmp/snmpd.conf` `rocommunity public / rwcommunity private`
LINUX	`#vi /etc/snmp/snmpd.conf` `com2sec notConfigUser default public`

U-68 (중)	3. 서비스 관리 > 3.31 SNMP 서비스 Community String의 복잡성 설정

AIX	#vi /etc/snmpdv3.conf COMMUNITY public public noAuthNoPriv 0.0.0.0 0.0.0.0 -
HP-UX	#vi /etc/snmpd.conf get-community-name: public / set-community-name: private
위의 설정과 같이 디폴트 커뮤니티명인 "public" 또는, "private"을 사용하는 경우 아래의 보안설정방법에 따라 설정을 변경함	

■ **SOLARIS**

Step 1) vi 편집기를 이용하여 SNMP 설정파일 열기

Step 2) Community String 값 설정 변경 (추측하기 어려운 값으로 설정)

<SOLARIS9 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>
```

<SOLARIS10 이상 버전>

```
#vi /etc/sma/snmp/snmpd.conf
 (수정 전) rocommunity public / rwcommunity private
 (수정 후) rocommunity <변경 값> / rwcommunity <변경 값>
```

Step 3) 서비스 재구동

<SOLARIS9 이하 버전>

```
# ps –ef | grep snmp
# kill –HUP [PID]
```

<SOLARIS10 이상 버전>

```
# svcs –a | grep snmpdx
# svcadm disable svc:/application/management/snmpdx:default
# svcadm enable svc:/application/management/snmpdx:default
```

■ **LINUX**

Step 1) vi 편집기를 이용하여 SNMP 설정파일 열기

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

Step 2) Community String 값 설정 변경 (추측하기 어려운 값으로 설정)

```
 (수정 전) com2sec notConfigUser default public
 (수정 후) com2sec notConfigUser default <변경 값>
```

Step 3) 서비스 재구동

```
# service snmpd rstart
```

UNIX 서버

U-68 (중)	3. 서비스 관리 > 3.31 SNMP 서비스 Community String의 복잡성 설정

■ **AIX**

Step 1) vi 편집기를 이용하여 SNMP 설정파일 열기

```
#vi /etc/snmpdv3.conf
```

Step 2) Community String 값 설정 변경 (추측하기 어려운 값으로 설정)

(수정 전) `COMMUNITY public public noAuthNoPriv 0.0.0.0 0.0.0.0 -`

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

Step 3) 서비스 재구동

```
# ps –ef | grep snmp
# kill –HUP [PID]
```

■ **HP-UX**

Step 1) vi 편집기를 이용하여 SNMP 설정파일 열기

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

Step 2) Community String 값 설정 변경 (추측하기 어려운 값으로 설정)

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

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

Step 3) 서비스 재구동

```
# ps –ef | grep snmp
# kill –HUP [PID]
```

조치 시 영향	Community String 수정 시 Server/Client에 모두 같은 Community String으로 변경하지 않을 시 통신 장애가 일어날 수 있음

U-69 (하)	3. 서비스 관리 > 3.32 로그온 시 경고 메시지 제공
취약점 개요	
점검내용	■ 서버 및 서비스에 로그온 시 불필요한 정보 차단 설정 및 불법적인 사용에 대한 경고 메시지 출력 여부 점검
점검목적	■ 비인가자들에게 서버에 대한 불필요한 정보를 제공하지 않고, 서버 접속 시 관계자만 접속해야 한다는 경각심을 심어 주기위해 경고 메시지 설정이 필요함
보안위협	■ 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
참고	※ 로그온 시 경고 메시지는 공격자의 활동을 주시하고 있다는 생각을 상기시킴으로써 간접적으로 공격 피해를 감소시키는 효과를 줄 수 있음
점검대상 및 판단기준	
대상	■ SOLARIS, LINUX, AIX, HP-UX 등
판단기준	**양호 :** 서버 및 Telnet, FTP, SMTP, DNS 서비스에 로그온 메시지가 설정되어 있는 경우
	취약 : 서버 및 Telnet, FTP, SMTP, DNS 서비스에 로그온 메시지가 설정되어 있지 않은 경우
조치방법	Telnet, FTP, SMTP, DNS 서비스를 사용할 경우 설정파일 조치 후 inetd 데몬 재시작
점검 및 조치 사례	

■ **SOLARIS**

Step 1) 서버 로그온 메시지 설정: vi 편집기로 "/etc/motd" 파일을 연 후 로그온 메시지 입력

```
#vi /etc/motd
 경고 메시지 입력
```

Step 2) Telnet 배너 설정: vi 편집기로 "/etc/default/telnetd" 파일을 연 후 로그온 메시지 입력

```
#vi /etc/default/telnetd
 BANNER="WARNING:Authorized use only" or BANNER=""
```

Step 3) FTP 배너 설정: vi 편집기로 "/etc/default/ftpd" 파일을 연 후 로그인 메시지 입력

```
#vi /etc/default/ftpd
 BANNER="WARNING:Authorized use only" or BANNER=""
```

Step 4) SMTP 배너 설정: vi 편집기로 "/etc/mail/sendmail.cf" 파일을 연 후 로그인 메시지 입력

```
#vi /etc/mail/sendmail.cf
 O Smtp GreetingMessage="경고 메시지 입력"
```

Step 5) DNS 배너 설정: vi 편집기로 "/etc/named.conf" 파일을 연 후 로그인 메시지 입력

U-69 (하)	3. 서비스 관리 > 3.32 로그온 시 경고 메시지 제공

```
#vi /etc/named.conf
 경고 메시지 입력
```

■ LINUX

Step 1) 서버 로그온 메시지 설정: vi 편집기로 "/etc/motd" 파일을 연 후 로그온 메시지 입력

```
#vi /etc/motd
 경고 메시지 입력
```

Step 2) Telnet 배너 설정: vi 편집기로 "/etc/issue.net" 파일을 연 후 로그온 메시지 입력

```
#vi /etc/issue.net
 경고 메시지 입력
```

Step 3) FTP 배너 설정: vi 편집기로 "/etc/vsftpd/vsftpd.conf" 파일을 연 후 로그인 메시지 입력

```
#vi /etc/vsftpd/vsftpd.conf
 ftpd_banner="경고 메시지 입력"
```

Step 4) SMTP 배너 설정: vi 편집기로 "/etc/mail/sendmail.cf" 파일을 연 후 로그인 메시지 입력

```
#vi /etc/mail/sendmail.cf
 O Smtp GreetingMessage="경고 메시지 입력"
```

Step 5) DNS 배너 설정: vi 편집기로 "/etc/named.conf" 파일을 연 후 로그인 메시지 입력

```
#vi /etc/named.conf
 경고 메시지 입력
```

■ AIX

Step 1) 서버 로그온 메시지 설정: vi 편집기로 "/etc/motd" 파일을 연 후 로그온 메시지 입력

```
#vi /etc/motd
 경고 메시지 입력
```

Step 2) Telnet 배너 설정: vi 편집기로 "/etc/security/login.cfg" 파일을 연 후 로그온 메시지 입력

```
#vi /etc/security/lgoin.cfg
 default: 라인 끝부분에 herald=”경고 메시지” 설정 추가
```

Step 3) FTP 배너 설정

```
#dspcat -g /usr/lib/nls/msg/en_US/ftpd.cat > /tmp/ftpd.msg
#vi /tmp/ftpd.msg의 내용중 "(%s) FTP server (%s) ready." 삭제 후 경고 메시지
  입력
#gencat /tmp/ftpd.cat /tmp/ftpd.msg
#cp -p /tmp/ftpd.cat /usr/lib/nls/msg/en_US/ftpd.cat
```

Step 4) SMTP 배너 설정: vi 편집기로 "/etc/mail/sendmail.cf" 파일을 연 후 로그인 메시지 입력

```
#vi /etc/mail/sendmail.cf
#SMTP initial login message (old $e marco)
 O SmtpGreetingMessage="경고 메시지 입력"
```

Step 5) DNS 배너 설정: vi 편집기로 "/etc/named.conf" 파일을 연 후 로그인 메시지 입력

U-69 (하)	3. 서비스 관리 > 3.32 로그온 시 경고 메시지 제공

```
#vi /etc/named.conf
 경고 메시지 입력
```

■ **HP-UX**

Step 1) 서버 로그온 메시지 설정: vi 편집기로 "/etc/motd" 파일을 연 후 로그온 메시지 입력

```
#vi /etc/motd
 경고 메시지 입력
```

Step 2) Telnet 배너 설정: vi 편집기로 "/etc/inetd.conf" 파일을 연 후 telnet 부분에 로그인 파일 설정

```
#telnet stream tcp6 nowait root /usr/lbin/telnetd telnetd –b /etc/issue
```

(/etc/issue 파일은 banner가 작성되어 있는 파일)

(-b : 뒤에 따라오는 banner 파일을 사용하겠다는 옵션)

```
#vi /etc/issue
 경고 메시지 입력
```

Step 3) FTP 배너 설정: vi 편집기로 "/etc/inetd.conf" 파일을 연 후 다음 내용 추가

```
#vi /etc/inetd.conf
 ftp stream tcp nowait root /usr/lbin/ftpd ftpd -a /etc/ftpd/ftpaccess
```

(-a : 뒤에 따라오는 설정파일을 사용하겠다는 옵션)

※ hostname제거

<wu-ftpd v2.4 미만인 경우>

```
#vi /etc/ftpd/ftpaccess
 suppresshostname yes (hostname 숨김)
 suppressversion yes (version 정보 숨김)
banner /etc/ftpd/ftp_banner(ftp 배너가 작성된 파일)
```

<we-ftpd v2.4 이상인 경우>

```
#vi /etc/ftpd/ftpaccess
 greeting terse (hostname 및 version 정보 숨김)
```

</etc/ftpd/ftpaccess 파일이 없을 경우>

```
#cp /usr/newconfig/etc/ftpd/examples/ftpaccess /etc/ftpd/ftpaccess
```

Step 4) SMTP 배너 설정: vi 편집기로 "/etc/mail/sendmail.cf" 파일을 연 후 메시지 입력

```
#vi /etc/mail/sendmail.cf
 SMTP initial login message (old $e marco)
 O SmtpGreetingMessage="경고 메시지 입력"
```

Step 5) DNS 배너 설정: vi 편집기로 "/etc/named.conf" 파일을 연 후 메시지 입력

```
#vi /etc/named.conf
 경고 메시지 입력
```

조치 시 영향	일반적인 경우 영향 없음

UNIX 서버

U-70 (중)	3. 서비스 관리 > 3.33 NFS 설정파일 접근권한
취약점 개요	
점검내용	■ NFS 접근제어 설정파일에 대한 비인가자들의 수정 제한 여부 점검
점검목적	■ 비인가자에 의한 불법적인 외부 시스템 마운트를 차단하기 위해 NFS 접근 제어 파일의 소유자 및 파일 권한을 관리 해야 함
보안위협	■ NFS 접근제어 설정파일에 대한 권한 관리가 이루어지지 않을 시 인가되지 않은 사용자를 등록하고 파일시스템을 마운트하여 불법적인 변조를 시도할 수 있음
참고	※ **NFS(Network File System):** 원격 컴퓨터의 파일시스템을 로컬 시스템에 마운트하여 마치 로컬 파일시스템처럼 사용할 수 있는 프로그램 ※ 관련 점검 항목 : U-24(상), U-25(상)
점검대상 및 판단기준	
대상	■ SOLARIS, LINUX, AIX, HP-UX 등
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 소유자가 root 가 아니거나, 권한이 644 이하가 아닌 경우
점검 및 조치 사례	

OS별 점검 파일 위치 및 점검 방법	
SOLARIS	`#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	

■ SOLARIS

"/etc/dfs/dfstab" 파일의 소유자 및 권한 변경 (소유자 root, 권한 644)

```
#chown root /etc/dfs/dfstab
#chmod 644 /etc/dfs/dfstab
```

■ LINUX, AIX, HP-UX

"/etc/exports" 파일의 소유자 및 권한 변경 (소유자 root, 권한 644)

```
#chown root /etc/exports
#chmod 644 /etc/exports
```

조치 시 영향	일반적인 경우 영향 없음

U-71 (중)	3. 서비스 관리 > 3.34 expn, vrfy 명령어 제한
취약점 개요	
점검내용	■ SMTP 서비스 사용 시 vrfy, expn 명령어 사용 금지 설정 여부 점검
점검목적	■ SMTP 서비스의 expn, vrfy 명령을 통한 정보 유출을 막기 위하여 두 명령어를 사용하지 못하게 옵션을 설정해야함
보안위협	■ VRFY, EXPN 명령어를 통하여 특정 사용자 계정의 존재유무를 알 수 있고, 사용자의 정보를 외부로 유출 할 수 있음
참고	※ **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
점검대상 및 판단기준	
대상	■ SOLARIS, LINUX, AIX, HP-UX 등
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
점검 및 조치 사례	

OS별 점검 파일 위치 및 점검 방법	
SOLARIS, LINUX, HP-UX	noexpn, novrfy 옵션 설정 확인 `#vi /etc/mail/sendmail.cf` `O PrivacyOptions=authwarnings`
AIX	`#vi /etc/sendmail.cf` `O PrivacyOptions=authwarnings`

<서비스 필요 시>

■ SOLARIS, LINUX, AIX, HP-UX

Step 1) vi 편집기를 이용하여 "/etc/mail/sendmail.cf" 파일을 연 후 (단, AIX는 /etc/sendmail.cf)

`#vi /etc/mail/sendmail.cf`

Step 2) "/etc/mail/sendmail.cf" 파일에 noexpn, novrfy 옵션 추가

(수정 전) `O PrivacyOptions=authwarnings`

(수정 후) `O PrivacyOptions=authwarnings, noexpn, novrfy`

U-71 (중)	3. 서비스 관리 > 3.34 expn, vrfy 명령어 제한

Step 3) SMTP 서비스 재시작

< 서비스 불필요 시>

■ SOLARIS, LINUX, HP-UX

Step 1) 실행중인 서비스 중지

```
#ps –ef | grep sendmail
 root 441 1 0 Sep19 ? 00:00:00 sendmail: accepting connections
#kill -9 [PID]
```

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

■ **SOLARIS, 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
```

■ **SOLARIS 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

U-72 (중)	3. 서비스 관리 > 3.35 Apache 웹 서비스 정보 숨김
취약점 개요	
점검내용	■ 웹페이지에서 오류 발생 시 출력되는 메시지 내용 점검
점검목적	■ HTTP 헤더, 에러페이지에서 웹 서버 버전 및 종류, OS 정보 등 웹 서버와 관련된 불필요한 정보가 노출되지 않도록 하기 위함
보안위협	■ 불필요한 정보가 노출될 경우 해당 정보를 이용하여 시스템의 취약점을 수집할 수 있음
참고	-
점검대상 및 판단기준	
대상	■ SOLARIS, Linux, AIX, HP-UX 등
판단기준	**양호 :** ServerTokens Prod, ServerSignature Off로 설정되어있는 경우
	취약 : ServerTokens Prod, ServerSignature Off로 설정되어있지 않은 경우
조치방법	헤더에 최소한의 정보를 제한 후 전송 (ServerTokens 지시자에 Prod 옵션, ServerSignature 지시자에 Off 옵션 설정)
점검 및 조치 사례	

OS별 점검 파일 위치 및 점검 방법	
SOLARIS, LINUX, AIX, HP-UX	ServerTokens, ServerSignature 옵션 설정 여부 확인 `# vi /[Apache_Home]/conf/httpd.conf` `ServerTokens Prod` `ServerSignature off` "httpd.conf" 파일 내에 ServerTokens, ServerSignature 지시자가 위와 같이 설정되어 있지 않은 경우 아래의 보안설정방법에 따라 옵션 추가

■ SOLARIS, LINUX, AIX, HP-UX

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

```
#vi /[Apache_home]/conf/httpd.conf
```

Step 2) 설정된 모든 디렉터리의 ServerTokens 지시자에서 Prod 옵션 설정 및 ServerSignature Off 지시자에 Off 옵션 설정 (없으면 신규 삽입)

```
<Directory />
    Options Indexes FollowSymlinks
    ServerTokens Prod
    ServerSignature Off
    - 이하 생략-
</Directory>
```

U-72 (중)	3. 서비스 관리 > 3.35 Apache 웹 서비스 정보 숨김

ServerTokens 지시자 옵션		
키워드	**제공하는 정보**	**예문**
Prod	웹 서버 종류	Apache
Min	웹 서버 버전	Apache/2.2.3
OS	웹 서버 버전 + 운영체제	Apache/2.2.3 (CentOS) (기본값)
Full	웹 서버의 모든 정보	Apache/2.2.3 (CentOS) DAV/2 PHP/5.16

조치 시 영향	일반적인 경우 영향 없음

U-73 (하)	5. 로그 관리 > 5.2 정책에 따른 시스템 로깅 설정
취약점 개요	
점검내용	■ 내부 정책에 따른 시스템 로깅 설정 적용 여부 점검
점검목적	■ 보안 사고 발생 시 원인 파악 및 각종 침해 사실에 대한 확인을 하기 위함
보안위협	■ 로깅 설정이 되어 있지 않을 경우 원인 규명이 어려우며, 법적 대응을 위한 충분한 증거로 사용할 수 없음
참고	■ 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 ※ 관련 점검 항목 : A-20(상), A-85(상)
점검대상 및 판단기준	
대상	■ SOLARIS, Linux, AIX, HP-UX 등
판단기준	**양호 :** 로그 기록 정책이 정책에 따라 설정되어 수립되어 있으며 보안정책에 따라 로그를 남기고 있을 경우
	취약 : 로그 기록 정책 미수립 또는, 정책에 따라 설정되어 있지 않거나 보안정책에 따라 로그를 남기고 있지 않을 경우
조치방법	로그 기록 정책을 수립하고, 정책에 따라 syslog.conf 파일을 설정
점검 및 조치 사례	

■ **SOLARIS**

Step 1) vi 편집기를 이용하여 "/etc/syslog.conf" 파일 열기

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

Step 2) 아래와 같이 수정 또는, 신규 삽입

```
mail.debug                      /var/log/mail.log
*.info                          /var/log/syslog.log
*.alert                         /var/log/syslog.log
*.alert                         /dev/console
*.alert                         root
*.emerg                         *
```

Step 3) 위와 같이 설정 후 SYSLOG 데몬 재시작

< SOLARIS 9 이하 버전 >

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

U-73 (하)	5. 로그 관리 > 5.2 정책에 따른 시스템 로깅 설정

< SOLARIS 10 이상 버전 >

```
#svcs -a | grep system-log
 online 16:23:03 svc:/system/system-log:default
#svcadm disable svc:/system/system-log:default
#svcadm enable svc:/system/system-log:default
```

■ LINUX

Step 1) vi 편집기를 이용하여 "/etc/syslog.conf" 파일 열기

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

※ CentOS 6.x 이상 버전의 로그파일명: rsyslog.conf

Step 2) 아래와 같이 수정 또는, 신규 삽입

```
*.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                                    *
```

Step 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

Step 1) vi 편집기를 이용하여 "/etc/syslog.conf" 파일 열기

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

Step 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
```

U-73 (하)	5. 로그 관리 > 5.2 정책에 따른 시스템 로깅 설정

Step 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**

Step 1) vi 편집기를 이용하여 "/etc/syslog.conf" 파일 열기

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

Step 2) 아래와 같이 수정 또는, 신규 삽입

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

Step 3) 위와 같이 설정 후 SYSLOG 데몬 재시작

```
#/sbin/init.d/syslogd start 또는,
#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

UNIX 서버

U-73 (하)	5. 로그 관리 > 5.2 정책에 따른 시스템 로깅 설정

메시지 우선순위	
메시지	**설명**
alert	즉각적으로 조치를 취해야 할 상황
crit	급한 상황은 아니지만, 치명적인 시스템 문제 발생 시
debug	프로그램 실행 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 로그를 설정할 경우, 시스템 퍼포먼스와 로그 저장에 따른 서버 용량 부족 문제가 발생할 수 있으므로 시스템 운영환경과 특성을 고려하여 적용

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

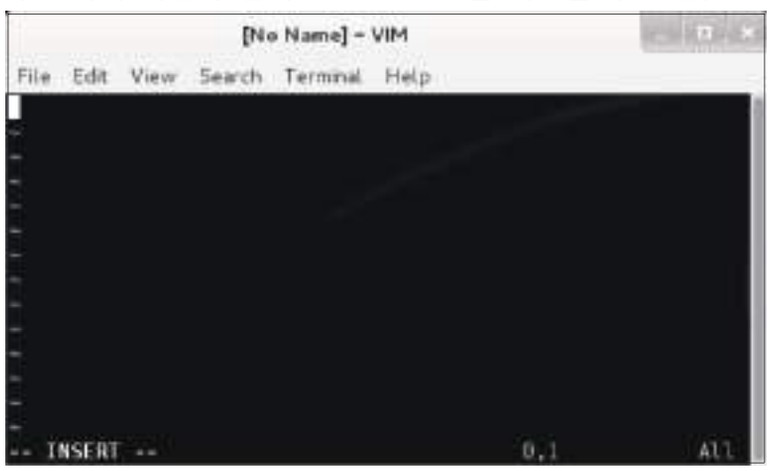
| more	많은 내용 출력 시 사용하는 옵션 "Enter"를 누르면 한 줄씩, "SpaceBar"를 누르면 한 화면씩 더 보여줌
| grep [Word]	특정 단어가 포함된 줄만 출력하는 명령어 [Word]에 특정 단어를 입력하여 호출
| nl	파일의 내용이 총 몇 줄인지 출력하는 명령어
| head	파일의 앞부분 10줄만 출력하는 명령어
| tail	파일의 뒷부분 10줄만 출력하는 명령어

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

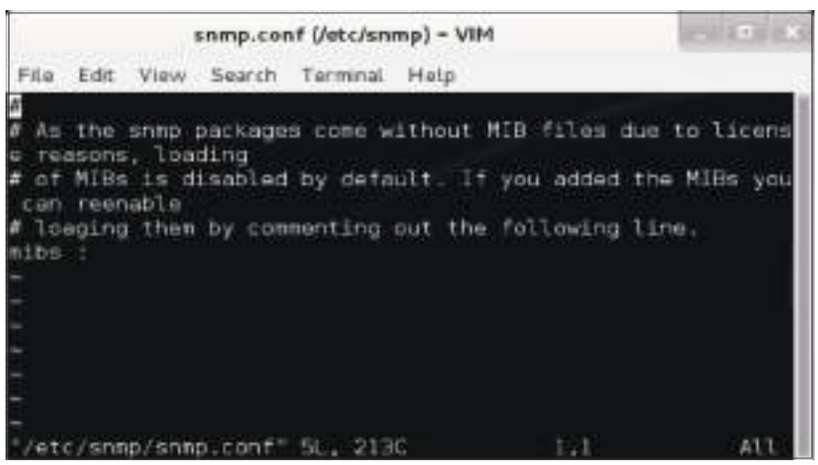
#vi <파일 경로/파일명>

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)



부 록

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

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

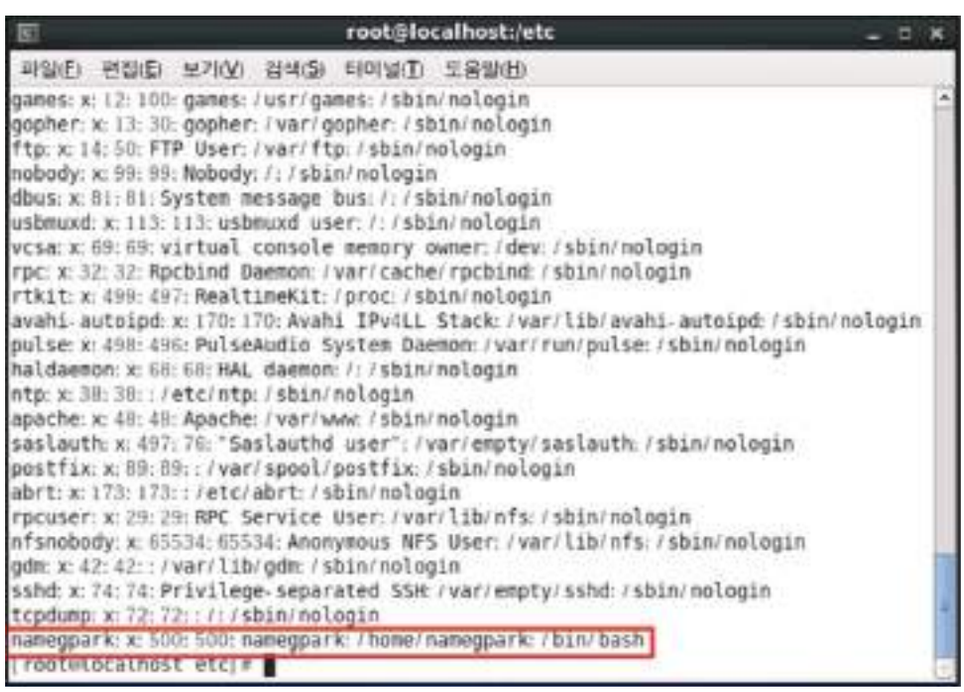
부 록

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 있은 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)

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

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

■ **/etc/passwd**



부 록

namegpark	x	500	500	namegpark	/home/namegpark	/bin/bash
계정명①	패스워드②	UID③	GID④	계정설명⑤	홈 디렉터리⑥	Shell 정보⑦

① 사용자 이름(대부분 ID라고함)
② 사용자 비밀번호(X로 되어 있는 것은 /etc/shadow 에 암호화된 형태로 저장되어 있음)
③ 사용자 UID(Unix의 모든 정보는 수치값으로 저장되어 있음 (root -> 0(GID))
④ 사용자 소속 그룹 GID(리눅스의 모든 정보는 수치값으로 저장 되어 있음 root -> 0(GID))
⑤ 사용자 정보(이름이나 연락처등 기타 정보 입력)
⑥ 사용자 계정 디렉터리(계정 홈 디렉터리)
⑦ 사용자 로그인 쉘 (Linux : bash Shell, Unix : Korn Shell 등)

■ /etc/shadow

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

ex)Root : 1Fz4q1GjE$G/EskZPyPdMo9.cNhRKSY.:14806: 0 : 99999 : 7 : : :
① ② ③ ④ ⑤ ⑥ ⑦ ⑧ ⑨

각 필드의 구분자는 콜론(:)이며, 각 필드는 아래의 의미를 가지고 있다.
① Login Name : 사용자 계정
② Encrypted : 패스워드를 암호화시킨 값
③ Last Changed : 1970년부터 1월 1일부터 패스워드가 수정된 날짜의 일수를 계산
④ Minimum : 패스워드가 변경되기 전 최소사용기간(일수)
⑤ Maximum : 패스워드 변경 전 최대사용기간(일수)
⑥ Warn : 패스워드 사용 만기일 전에 경고 메시지를 제공하는 일수
⑦ Inactive : 로그인 접속차단 일 수

부 록

⑧ Expire : 로그인 사용을 금지하는 일 수 (월/일/연도)+A1:A44
⑨ Reserved : 사용되지 않음

■ /etc/group

namegpark	x	500	-
그룹명	패스워드	GID	그룹구성원

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

부 록

• 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 쉘 계정
• pcap:x:77:77::/var/arpwatch:/sbin/nologin = 패킷 캡쳐 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
※ UID 100이하 또는 60000이상의 계정들은 시스템 계정으로 로그인이 필요없음

06. 불필요한 SUID/SGID 목록 설명

SOLARIS	
/usr/bin/admintool	System Administration Tools
/usr/bin/at	지정된 시간에 실행할 작업을 입력하고, 대기 목록을 확인하고, 제거하는 명령어
/usr/bin/atq	Daemons 현재 대기중인 작업 목록 확인
/usr/bin/atrm	Daemons 현재 대기중인 작업제거
/usr/bin/lpset	프린터와 관련된 장치, 디렉터리를 접근하는 명령어로 EGID 를 변경
/usr/bin/newgrp	현재 세션의 사용자 그룹 변경 (지정한 그룹의 쉘로 환경이 바로 변경)
/usr/bin/nispasswd	RPC DAEMON NIS+passwd 테이블 패스워드 변경
/usr/bin/rdist	원격 서버로 동기화, 복사, 백업 수행
/usr/bin/yppasswd	

부 록	
/usr/dt/bin/dtappgather	사용자 세션을 시작하는 것과 연관된 명령어로 사용 가능한 응용프로그램 모으는 명령어
/usr/dt/bin/dtprintinfo	데스크탑에 프린터 추가할 때 사용하는 명령어
/usr/dt/bin/sdtcm_convert	캘린더 도구로서 데이터 형식을 변환하거나 캘린더의 불필요한 부분을 제거하는데 사용
/usr/lib/fs/ufs/ufsdump	Backup/Restore
/usr/lib/fs/ufs/ufsrestore	Backup/Restore
/usr/lib/lp/bin/netpr	lpsched 데몬, LP 프린트 서비스와 PostScript 필터들에 의해 사용되는 바이너리 파일들, 기본 프린터 인터페이스 프로그램들과 연관
/usr/openwin/bin/ff.core	
/usr/openwin/bin/kcms_calibrate	/tmp 디렉터리에 kp_kcms_sys.sem 이라는 임시 파일을 /tmp에 존재하는지 검사하지 않고 무조건 생성하는 프로그램
/usr/openwin/bin/kcms_configure	
/usr/openwin/bin/xlock	X 터미널을 잠그기 위한 프로그램
/usr/platform/sun4u/sbin/prtdiag	시스템 하드웨어 사항과 시스템의 하드웨어적 실패 부분 조회
/usr/sbin/arp	네트워크 관련 명령어
/usr/sbin/lpmove	다른 프린터와 print request 를 이동할 수 있는 명령어
/usr/sbin/prtconf	현재 시스템의 메모리 양, 시스템에서 인식한 장치 목록을 장치 트리를 사용해서 보여주는 명령어
/usr/sbin/sysdef	유닉스 기반의 시스템에서 정의된 내용을 출력하는 명령어
/usr/sbin/sparcv7/prtconf	현재 시스템의 메모리 양, 시스템에서 인식한 장치 목록을 장치 트리를 사용해서 보여주는 명령어
/usr/sbin/sparcv7/sysdef	유닉스 기반의 시스템에서 정의된 내용을 출력하는 명령어
/usr/sbin/sparcv9/prtconf	현재 시스템의 메모리 양, 시스템에서 인식한 장치 목록을 장치 트리를 사용해서 보여주는 명령어
/usr/sbin/sparcv9/sysdef	유닉스 기반의 시스템에서 정의된 내용을 출력하는 명령어
LINUX	
/sbin/dump	Backup/Restore
/sbin/restore	Backup/Restore
/sbin/unix_chkpwd	사용자의 암호가 읽을 수 없는 장소에 보관되는 경우 사용자의 암호를 검사해주는 프로그램. 이 프로그램을 호출한 사용자의 암호를 검사해주는 역할만 함

부 록

/usr/bin/at	지정된 시간에 실행할 작업을 입력하고, 대기 목록을 확인하고, 제거하는 명령어
/usr/bin/lpq	라인프린터 작업 큐 조회 명령어
/usr/bin/lpq-lpd	DAEMON
/usr/bin/lpr	콘솔환경에서 명시된 파일을 인쇄할 때 사용
/usr/bin/lpr-lpd	DAEMON
/usr/bin/lprm	lpq 명령어로 볼 수 있는 작업 큐를 살펴보고 해당하는 작업을 취소하거나 작업 번호를 지정하여 작업 번호에 해당하는 큐를 삭제.
/usr/bin/lprm-lpd	DAEMON
/usr/bin/newgrp	현재 세션의 사용자 그룹 변경(지정한 그룹의 쉘로 환경이 바로 변경)
/usr/sbin/lpc	커맨드 기반의 프린터 제어
/usr/sbin/lpc-lpd	DAEMON
/usr/sbin/traceroute	네트워크 경로 출력
AIX	
/usr/dt/bin/dtaction	지정된 인수로 CDE 작업을 호출
/usr/sbin/mount	파일시스템을 지정된 위치에서 사용 가능하도록 연결
/usr/dt/bin/dtterm	데스크탑 기본 터미널 에뮬레이터
/usr/sbin/lchangelv	논리적 볼륨과 연관되는 명령어
/usr/bin/X11/xlock	X 터미널을 잠그기 위한 프로그램
HP-UX	
/opt/perf/bin/glance	성능 모니터링 툴(CUI)
/opt/perf/bin/gpm	성능 모니터링 툴(GUI)
/opt/video/lbin/camServer	
/usr/bin/at	Daemons 지정된 시간에 실행할 작업을 입력하고, 대기 목록을 확인하고, 제거하는 명령어
/usr/bin/lpalt	프린터 및 인쇄 요청의 우선 순위 변경
/usr/bin/mediainit	디스크 포맷 명령어로 읽기, 쓰기 테스트를 수행하여 디스크 무결성을 검증하고 손상된 블럭이 발견될 경우 수정
/usr/bin/newgrp	현재 세션의 사용자 그룹 변경(지정한 그룹의 쉘로 환경이 바로

부 록

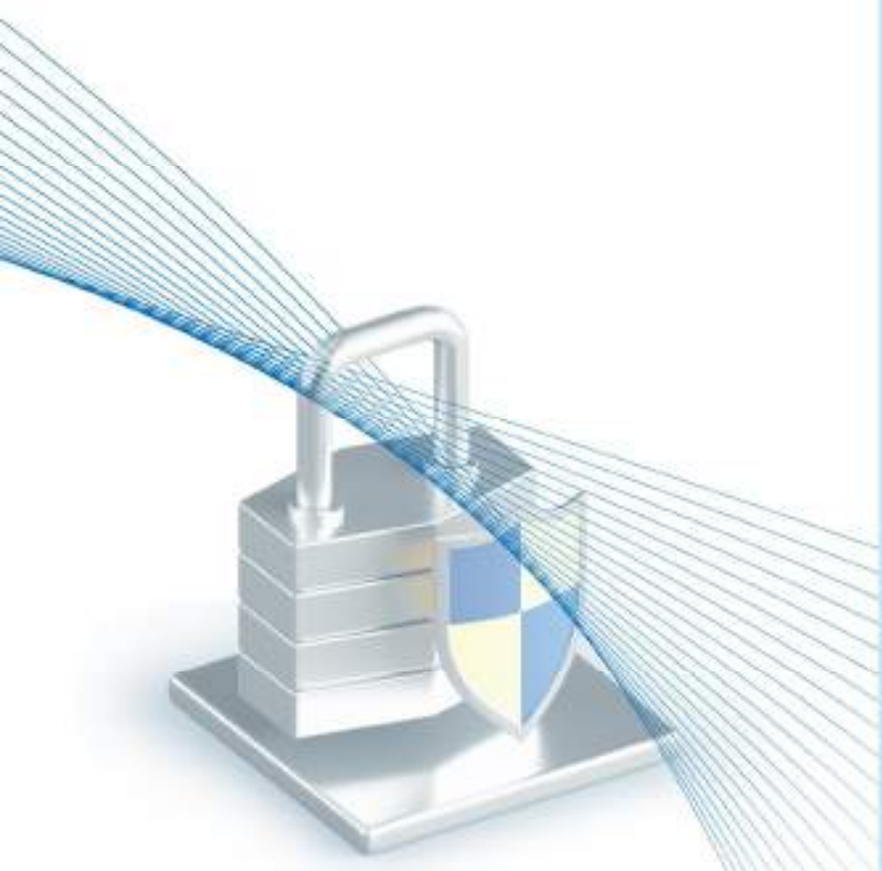
	변경)
/usr/bin/rdist	원격 서버로 동기화, 복사, 백업 수행
/usr/dt/bin/dtprintinfo	데스크탑에 프린터 추가할 때 사용하는 명령어
/usr/sbin/arp	네트워크 관련 명령어
/usr/sbin/lanadmin	네트워크 관련 명령어
/usr/sbin/landiag	네트워크 하드웨어 이상을 진단하는 명령어
/usr/sbin/lpsched	LP 요청 스케줄러의 데이터를 표시
/usr/sbin/swacl	소프트웨어 생산품 접근 통제 명령어
/usr/sbin/swconfig	시스템에 설치된 소프트웨어를 configure 하는 명령어
/usr/sbin/swinstall	시스템에 소프트웨어를 설치하거나 업데이트 하는 명령어
/usr/sbin/swreg	특정 서버에 등록하는 명령어
/usr/sbin/swremove	시스템에 설치되어 있는 소프트웨어를 제거
/usr/contrib/bin/traceroute	네트워크 경로 출력
/usr/dt/bin/dtappgather	사용자 세션을 시작하는 것과 연관된 명령어로 사용 가능한 응용프로그램 모으는 명령어
/usr/sbin/swmodify	소프트웨어 패키지 내역 변경 명령어
/usr/sbin/swpackage	소프트웨어 패키지 시 사용하는 명령어

07. RPC 서비스 종류

- rpc.statd : 시스템 장애 시 NFS에서 파일 복구를 위해 제공하는 lockd 프로그램을 지원하는 도구로 클라이언트와 서버의 상태를 모니터링 하는 데몬
- rpc.ttdbserverd : ToolTalk 애플리케이션간의 통신을 관리하는 데몬
- sadmind : 원격에서 시스템을 관리하거나 모니터링하기 쉽게 도와주는 데몬
- rpc.ypupdated : nis process 변경된 정보를 변경해주는 데몬
- rusersd : 현재 네트워크에 있는 사용자 리스트를 리턴해주는 데몬
- walld : 메시지를 네트워크의 모든 사용자에게 전송하는 요청을 처리하는 데몬
- sprayd : 지정된 수의 패킷을 호스트에 전송하고 성능 통계를 보고하는 데몬
- rstatd : CPU와 가상메모리 사용통계, 네트워크 가동시간, 하드디스크에 대한 정보를 제공하는 데몬
- rpc.nisd : NIS+의 서비스를 제공하는 데몬
- rexd : 원격 사용자가 서버에서 명령어를 실행하도록 하는 데몬
- rpc.pcnfsd : PC-NFS(개인용 컴퓨터 네트워크 파일 시스템) 클라이언트에서의 서비스 요청을 처리하는 데몬
- rpc.cmsd : 데이터베이스 관리 데몬으로 open Windows의 Calender Manager와 CDE의 Calender에서 사용
- rpc.rquotad : 원격 쿼터 데몬으로 NFS 서버의 파일 시스템을 마운트한 로컬 유저의 쿼터를 넘겨줌
- kcms_server : 데스크탑 컴퓨터 및 관련 주변 기기에 디지털 컬러 이미지의 색상 성능을 제어 할 수 있는 코닥 색상 관리 시스템을 원격에서 접근할 수 있게 해주는 데몬
- cachefsd : 캐시 파일 시스템 데몬. nfs나 cdrom 같은 저속의 장치를 디스크로부터 캐싱하여 성능을 증가시킴

Ⅱ

윈도우즈 서버



윈도우즈 서버 취약점 분석·평가 항목

분류	점검항목	항목 중요도	항목코드
1. 계정 관리	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 해제	상	W-05
	관리자 그룹에 최소한의 사용자 포함	상	W-06
	Everyone 사용권한을 익명 사용자에 적용 해제	중	W-46
	계정 잠금 기간 설정	중	W-47
	패스워드 복잡성 설정	중	W-48
	패스워드 최소 암호 길이	중	W-49
	패스워드 최대 사용 기간	중	W-50
	패스워드 최소 사용 기간	중	W-51
	마지막 사용자 이름 표시 안함	중	W-52
	로컬 로그온 허용	중	W-53
	익명 SID/이름 변환 허용 해제	중	W-54
	최근 암호 기억	중	W-55
	콘솔 로그온 시 로컬 계정에서 빈 암호 사용 제한	중	W-56
	원격터미널 접속 가능한 사용자 그룹 제한	중	W-57
2. 서비스 관리	공유 권한 및 사용자 그룹 설정	상	W-07
	하드디스크 기본 공유 제거	상	W-08
	불필요한 서비스 제거	상	W-09
	IIS 서비스 구동 점검	상	W-10
	IIS 디렉토리 리스팅 제거	상	W-11
	IIS CGI 실행 제한	상	W-12
	IIS 상위 디렉토리 접근 금지	상	W-13

	IIS 불필요한 파일 제거	상	W-14
	IIS 웹프로세스 권한 제한	상	W-15
	IIS 링크 사용 금지	상	W-16
	IIS 파일 업로드 및 다운로드 제한	상	W-17
	IIS DB 연결 취약점 점검	상	W-18
	IIS 가상 디렉토리 삭제	상	W-19
	IIS 데이터파일 ACL 적용	상	W-20
	IIS 미사용 스크립트 매핑 제거	상	W-21
	IIS Exec 명령어 쉘 호출 진단	상	W-22
	IIS WebDAV 비활성화	상	W-23
	NetBIOS 바인딩 서비스 구동 점검	상	W-24
	FTP 서비스 구동 점검	상	W-25
	FTP 디렉토리 접근 권한 설정	상	W-26
	Anonymous FTP 금지	상	W-27
	FTP 접근 제어 설정	상	W-28
	DNS Zone Transfer 설정	상	W-29
	RDS(Remonte Data Services) 제거	상	W-30
	최신 서비스팩 적용	상	W-31
	터미널 서비스 암호화 수준 설정	중	W-58
	IIS 웹 서비스 정보 숨김	중	W-59
	SNMP 서비스 구동 점검	중	W-60
	SNMP 서비스 커뮤니티스트링의 복잡성 설정	중	W-61
	SNMP Access control 설정	중	W-62
	DNS 서비스 구동 점검	중	W-63
	HTTP/FTP/SMTP 배너 차단	하	W-64
	Telnet 보안 설정	중	W-65
	불필요한 ODBC/OLE-DB 데이터소스와 드라이브 제거	중	W-66
	원격터미널 접속 타임아웃 설정	중	W-67
	예약된 작업에 의심스러운 명령이 등록되어 있는지 점검	중	W-68

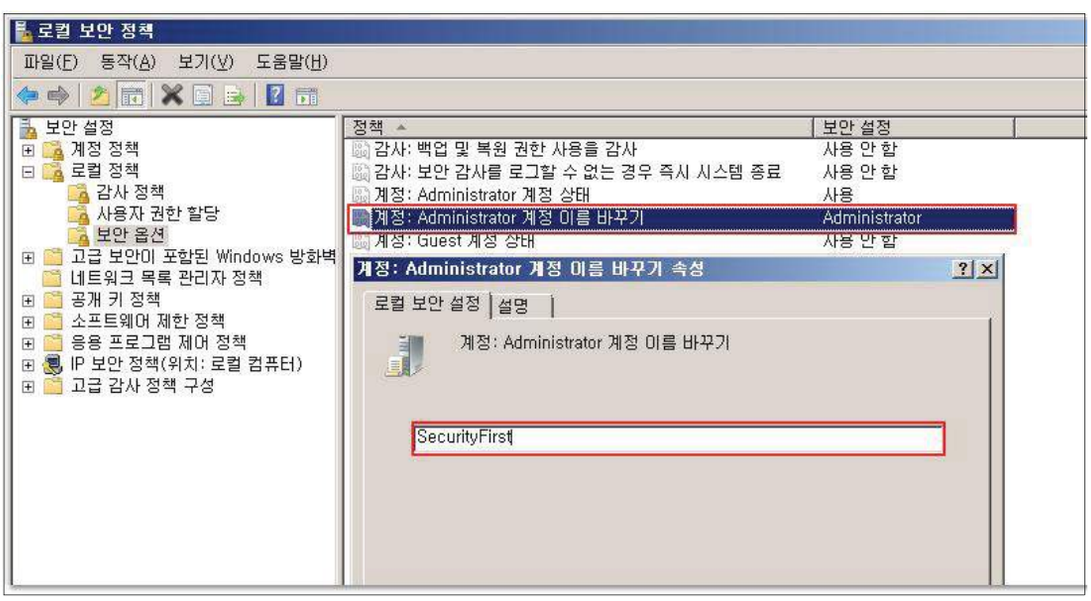
3. 패치 관리	최신 HOT FIX 적용	상	W-32
	백신 프로그램 업데이트	상	W-33
	정책에 따른 시스템 로깅설정	중	W-69
4. 로그 관리	로그의 정기적 검토 및 보고	상	W-34
	원격으로 액세스 할 수 있는 레지스트리 경로	상	W-35
	이벤트 로그 관리 설정	하	W-70
	원격에서 이벤트 로그파일 접근 차단	중	W-71
5. 보안 관리	백신 프로그램 설치	상	W-36
	SAM 파일 접근 통제 설정	상	W-37
	화면보호기 설정	상	W-38
	로그온 하지 않고 시스템 종료 허용 해제	상	W-39
	원격 시스템에서 강제로 시스템 종료	상	W-40
	보안감사를 로그할 수 없는 경우 즉시 시스템 종료 해제	상	W-41
	SAM 계정과 공유의 익명 열거 허용 안함	상	W-42
	Autologin 기능 제어	상	W-43
	이동식 미디어 포맷 및 꺼내기 허용	상	W-44
	디스크 볼륨 암호화 설정	상	W-45
	Dos 공격 방어 레지스트리 설정	중	W-72
	사용자가 프린터 드라이버를 설치할 수 없게 함	중	W-73
	세션 연결을 중단하기 전에 필요한 유휴시간	중	W-74
	경고 메시지 설정	하	W-75
	사용자별 홈 디렉토리 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
	시작 프로그램 목록 분석	중	W-81
6. DB 관리	Windows 인증 모드 사용	중	W-82

W-01 (상)	1. 계정관리 > 1.1 Administrator 계정 이름 바꾸기
취약점 개요	
점검내용	■ 윈도우즈 최상위 관리자 계정인 Administrator의 계정명 변경 여부 점검
점검목적	■ 윈도우즈 기본 관리자 계정인 Administrator의 이름을 변경하여, 잘 알려진 계정을 통한 악의적인 패스워드 추측 공격을 차단하고자 함
보안위협	■ 일반적으로 관리자 계정으로 잘 알려진 Administrator를 변경하지 않은 경우 악의적인 사용자의 패스워드 추측 공격을 통해 사용 권한 상승의 위험이 있으며, 관리자를 유인하여 침입자의 액세스를 허용하는 악성코드를 실행할 우려가 있음 ■ 윈도우즈 최상위 관리자 계정인 Administrator는 기본적으로 삭제하거나 잠글 수 없어 악의적인 사용자의 목표가 됨
참고	※ 윈도우즈 서버는 Administrator 계정을 비활성화 할 수 있으나 안전 모드로 컴퓨터를 시작할 경우 본 계정은 자동으로 활성화 됨
점검대상 및 판단기준	
대상	■ Windows NT, 2000, 2003, 2008, 2012
판단기준	**양호 :** Administrator Default 계정 이름을 변경한 경우
	취약 : Administrator Default 계정 이름을 변경하지 않은 경우
조치방법	Administrator Default 계정 이름 변경
점검 및 조치 사례	

■ **Window NT, 2000, 2003, 2008, 2012**

Step 1) 시작> 프로그램> 제어판> 관리도구> 로컬 보안 정책> 로컬 정책> 보안옵션

Step 2) "계정: Administrator 계정 이름 바꾸기"를 유추하기 어려운 계정 이름으로 변경



조치 시 영향	일반적인 경우 영향 없음

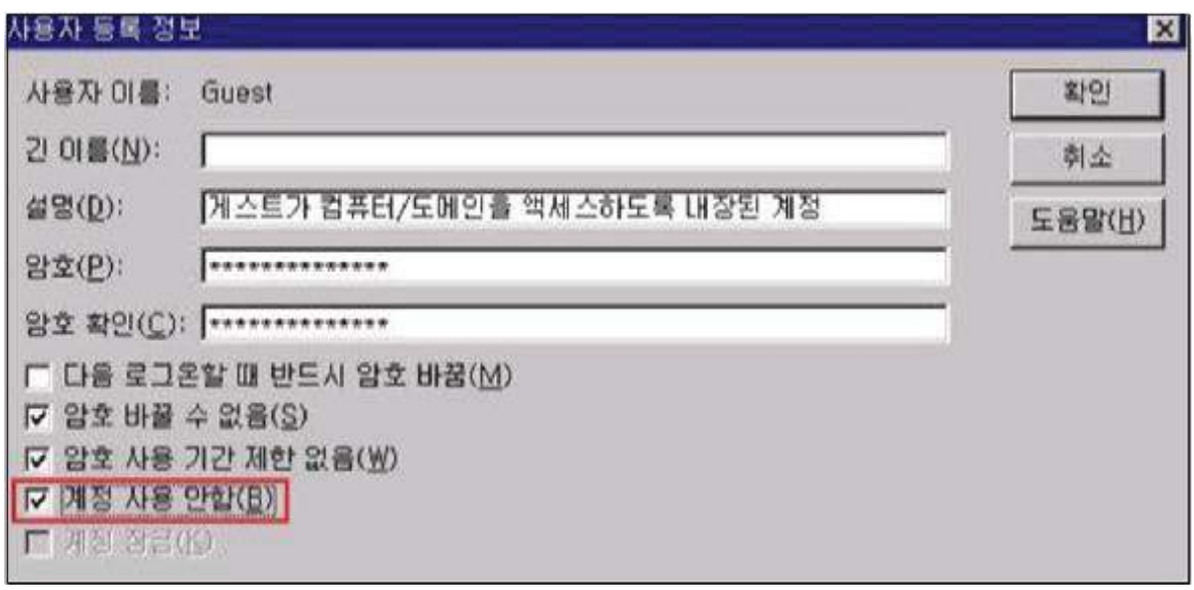
Windows 서버

W-02 (상)	1. 계정관리 > 1.2 Guest 계정 상태
취약점 개요	
점검내용	■ Guest 계정 비활성화 여부 점검
점검목적	■ Guest 계정을 비활성화 하여 불특정 다수의 임시적인 시스템 접근을 차단하기 위함
보안위협	■ Guest 계정은 시스템에 임시로 액세스해야 하는 사용자용 계정으로, 이 계정을 사용하여 권한 없는 사용자가 시스템에 익명으로 액세스할 수 있으므로 비인가자 접근, 정보 유출 등 보안 위험이 따를 수 있음
참고	※ 윈도우즈 Guest 계정은 삭제가 불가능한 built-in 계정으로 보안 강화 목적으로 반드시 비활성화 처리 하여야 함
점검대상 및 판단기준	
대상	■ Windows NT, 2000, 2003, 2008, 2012
판단기준	**양호 :** Guest 계정이 비활성화 되어 있는 경우
	취약 : Guest 계정이 활성화 되어 있는 경우
조치방법	Guest 계정 비활성화
점검 및 조치 사례	

■ **Window NT**

Step 1) 시작> 프로그램> 관리도구> 도메일 사용자 관리> Guest 계정 선택> 등록정보

Step 2) "계정 사용 안함"에 체크

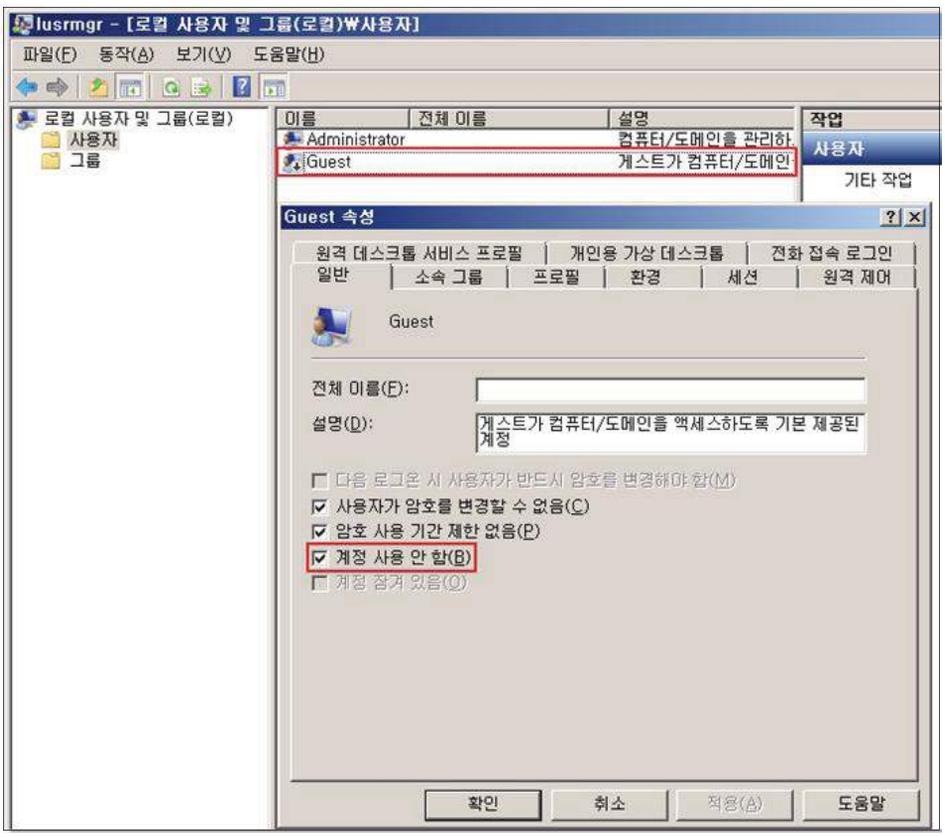


W-02 (상)	1. 계정관리 > 1.2 Guest 계정 상태

■ **Windows 2000, 2003, 2008, 2012**

Step 1) 시작> 실행> LUSRMGR.MSC> 사용자> GUEST> 속성

Step 2) "계정 사용 안 함"에 체크



조치 시 영향	일반적인 경우 영향 없음

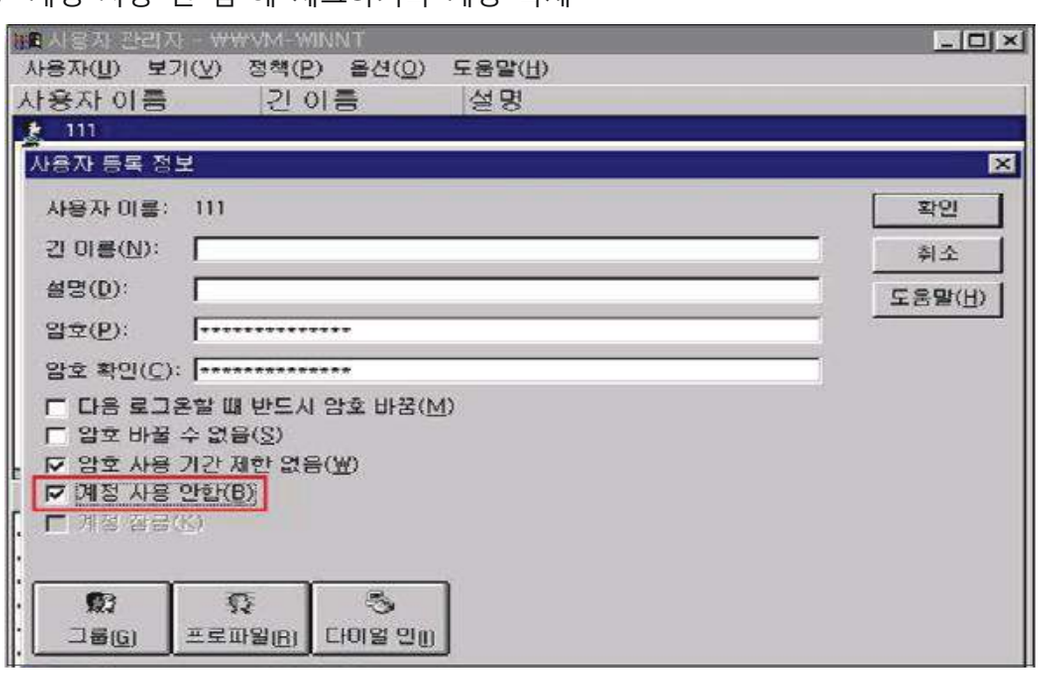
Windows 서버

W-03 (상)	1. 계정관리 > 1.3 불필요한 계정 제거
취약점 개요	
점검내용	■ 시스템 내 불필요한 계정 및 의심스러운 계정의 존재 여부를 점검
점검목적	■ 퇴직, 전직, 휴직 등의 이유로 더 이상 사용하지 않는 계정, 불필요한 계정 및 의심스러운 계정을 삭제하여, 일반적으로 로그인이 필요치 않은 해당 계정들을 통한 로그인을 차단하고, 계정의 패스워드 추측 공격 시도를 차단하고자 함
보안위협	■ 관리되지 않은 불필요한 계정은 장기간 패스워드가 변경되지 않아 무작위 대입 공격(Brute Force Attack)이나 패스워드 추측 공격 (Password Guessing Attack)의 가능성이 존재하며, 또한 이런 공격에 의해 계정 정보가 유출되어도 유출 사실을 인지하기 어려움
참고	※ **무작위 대입 공격(Brute Force Attack):** 컴퓨터로 암호를 해독하기 위해 조합 가능한 모든 경우의 수를 다 대입해보는 것을 말함
점검대상 및 판단기준	
대상	■ Windows NT, 2000, 2003, 2008, 2012
판단기준	**양호 :** 불필요한 계정이 존재하지 않는 경우
	취약 : 불필요한 계정이 존재하는 경우
조치방법	현재 계정 현황 확인 후 불필요한 계정 삭제
점검 및 조치 사례	

■ **Window NT**

Step 1) 시작> 프로그램> 관리도구> 도메인 사용자 관리> 계정 선택> 등록 정보

Step 2) "계정 사용 안 함"에 체크하거나 계정 삭제

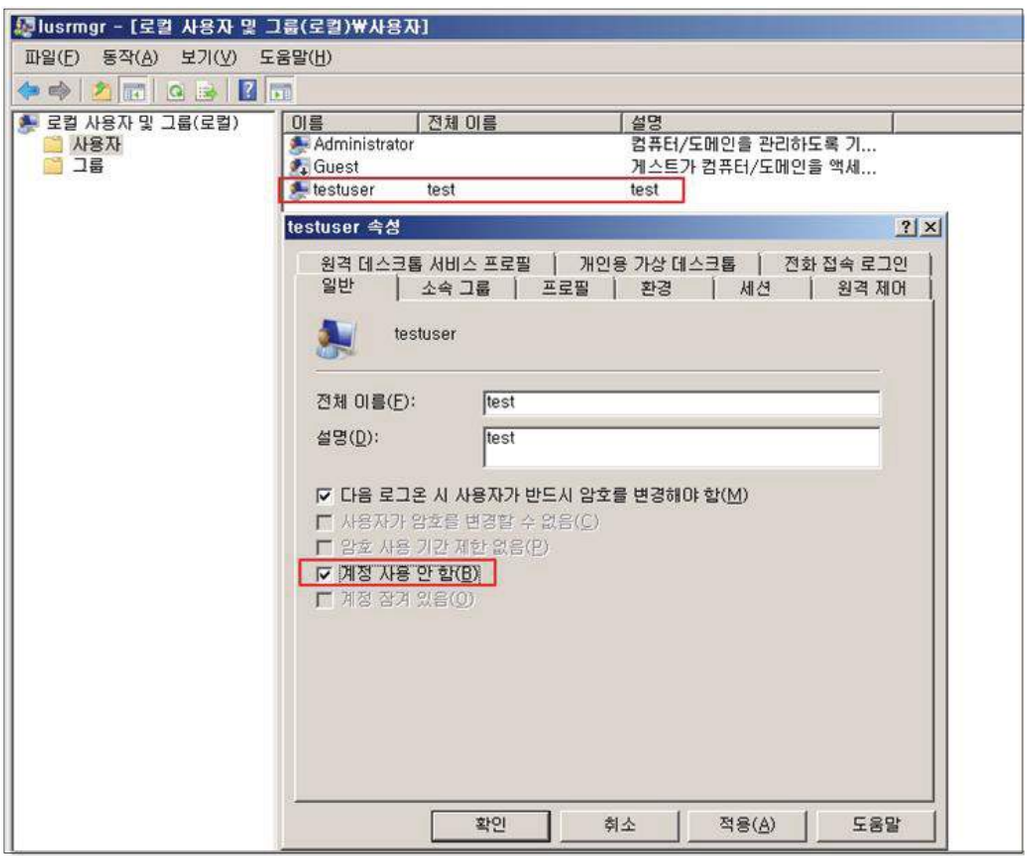


W-03 (상)	1. 계정관리 > 1.3 불필요한 계정 제거

■ **Windows 2000, 2003, 2008, 2012**

Step 1) 시작> 실행> LUSRMGR.MSC> 사용자

Step 2) 등록된 계정 중 불필요한 사용자 선택> 속성> "계정 사용 안 함"에 체크하거나 계정 삭제



조치 시 영향	명확하게 파악되지 않은 계정을 삭제하는 경우 해당 계정과 관련한 업무에 장애발생 가능성이 존재함

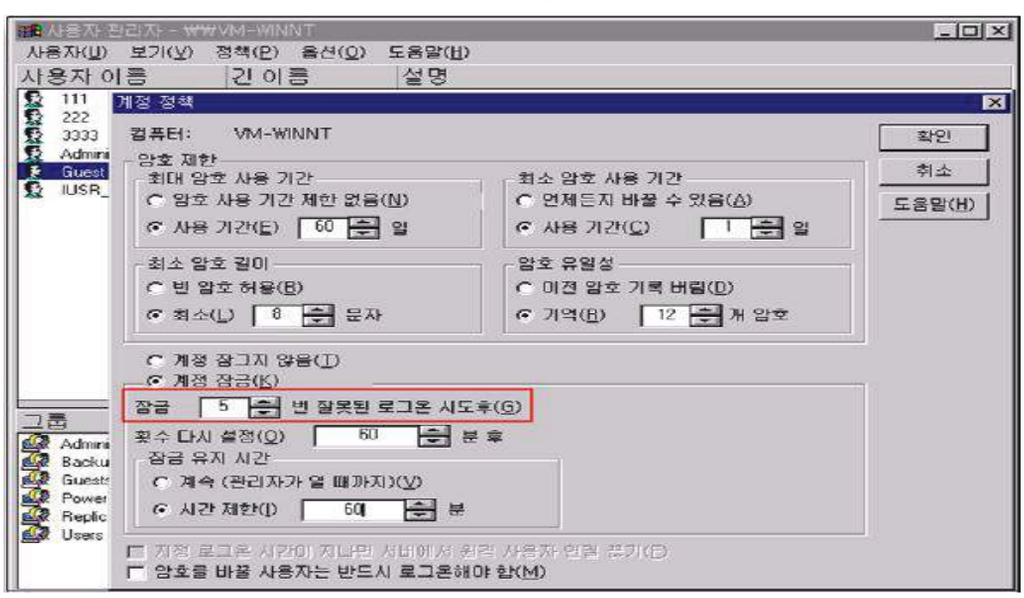
Windows 서버

W-04 (상)	1. 계정관리 > 1.4 계정 잠금 임계값 설정
취약점 개요	
점검내용	■ 계정 잠금 임계값의 설정 여부 점검
점검목적	■ 계정 잠금 임계값을 설정하여 공격자의 자유로운 자동화 암호 유추 공격을 차단하기 위함
보안위협	■ 공격자는 시스템의 계정 잠금 임계값이 설정되지 않은 경우 자동화된 방법을 이용하여 모든 사용자 계정에 대해 암호조합 공격을 자유롭게 시도할 수 있으므로 사용자 계정 정보의 노출 위험이 있음
참고	※ 계정 잠금 임계값 설정은 사용자 계정이 잠기는 로그온 실패 횟수를 결정하며 잠긴 계정은 관리자가 재설정하거나 해당 계정의 잠금 유지 시간이 만료되어야 사용할 수 있음 ※ **계정 잠금 정책:** 해당 계정이 시스템으로부터 잠기는 환경과 시간을 결정하는 정책으로 '계정 잠금 기간', '계정 잠금 임계값', '다음 시간 후 계정 잠금 수를 원래대로 설정'의 세가지 하위 정책을 가짐 ※ 관련 점검 항목 : W-47(중)
점검대상 및 판단기준	
대상	■ Windows NT, 2000, 2003, 2008, 2012
판단기준	**양호 :** 계정 잠금 임계값이 5 이하의 값으로 설정되어 있는 경우
	취약 : 계정 잠금 임계값이 6 이상의 값으로 설정되어 있는 경우
조치방법	계정 잠금 임계값을 5번 이하의 값으로 설정
점검 및 조치 사례	

■ **Window NT**

Step 1) 시작> 프로그램> 관리도구> 도메인 사용자 관리자> 정책> 계정 정책

Step 2) "계정 잠금" 선택 후 "잠금"에 "5"이하의 값 설정

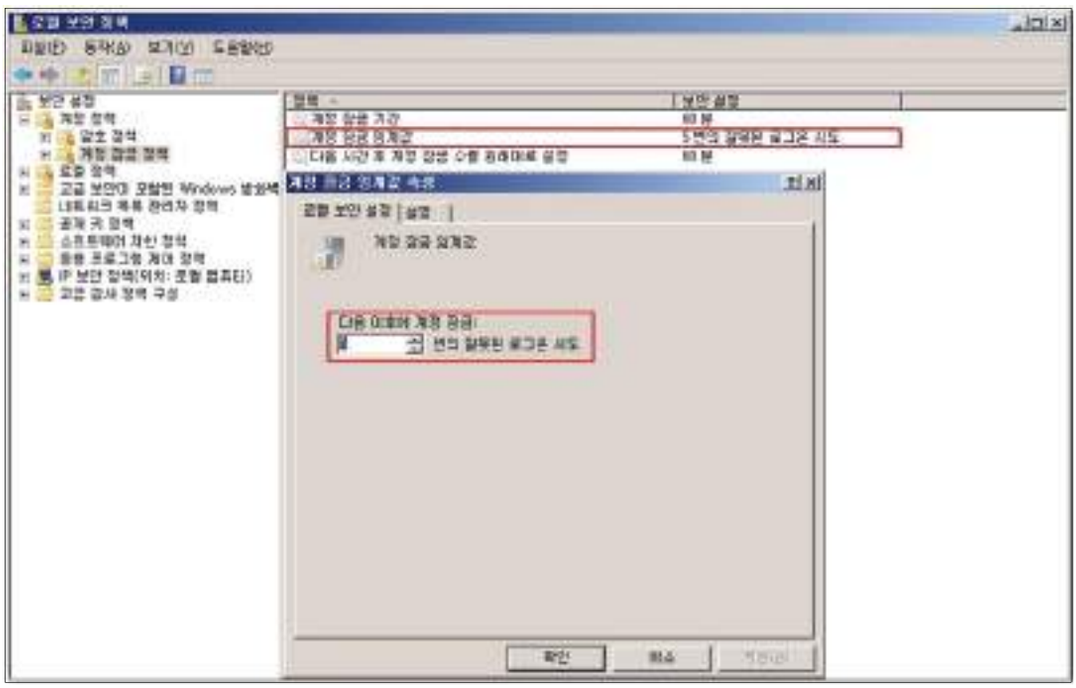


W-04 (상)	1. 계정관리 > 1.4 계정 잠금 임계값 설정

■ **Windows 2000, 2003, 2008, 2012**

Step 1) 시작> 실행> SECPOL.MSC> 계정 정책> 계정 잠금 정책

Step 2) "계정 잠금 임계값"을 "5"이하의 값으로 설정



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

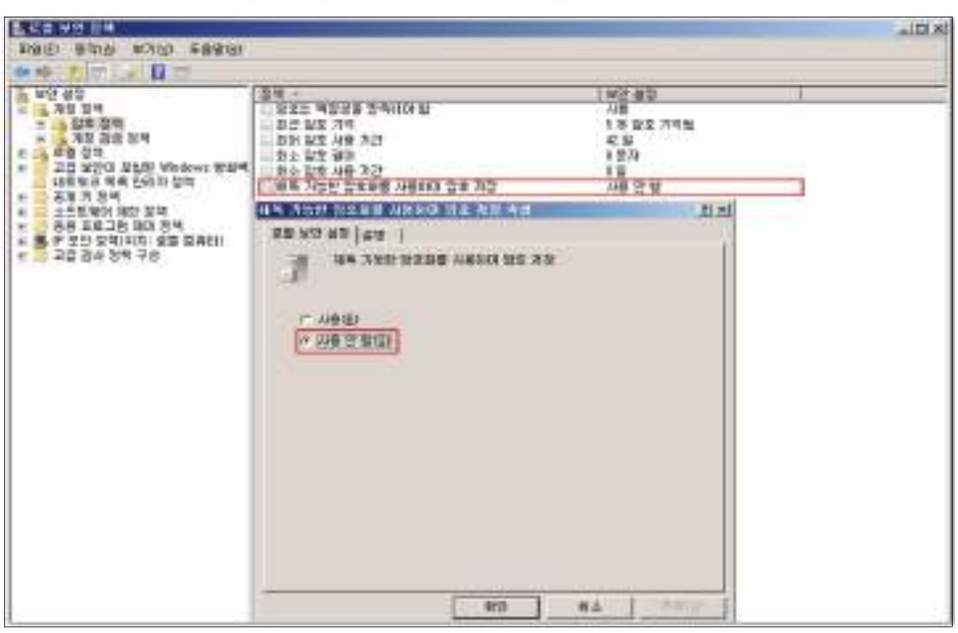
Windows 서버

W-05 (상)	1. 계정관리 > 1.5 해독 가능한 암호화를 사용하여 암호 저장 해제
취약점 개요	
점검내용	■ 해독 가능한 암호화 사용 여부 점검
점검목적	■ '해독 가능한 암호화를 사용하여 암호 저장' 정책이 설정되어 사용자 계정 비밀번호가 해독 가능한 텍스트 형태로 저장 되는 것을 차단하기 위함
보안위협	■ 위 정책이 설정된 경우 OS에서 사용자 ID, PW를 입력받아 인증을 진행하는 응용프로그램 프로토콜 지원 시 OS 는 사용자의 PW 를 해독 가능한 방식으로 암호를 저장하기 때문에, 노출된 계정에 대해 공격자가 암호 복호화 공격으로 PW를 획득하여 네트워크 리소스에 접근할 수 있음
참고	※ '해독 가능한 암호화를 사용하여 암호 저장' 정책은 암호를 암호화 하지 않은 상태로 저장하여 일반 텍스트 버전의 암호를 저장하는 것과 같으나 시스템에서 기본적으로 동작하지는 않음
점검대상 및 판단기준	
대상	■ Windows NT, 2000, 2003, 2008, 2012
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
점검 및 조치 사례	

■ Window NT, 2000, 2003, 2008, 2012

Step 1) 시작> 실행> SECPOL.MSC> 계정 정책> 암호 정책

Step 2) "해독 가능한 암호화를 사용하여 암호 저장"을 "사용 안 함"으로 설정



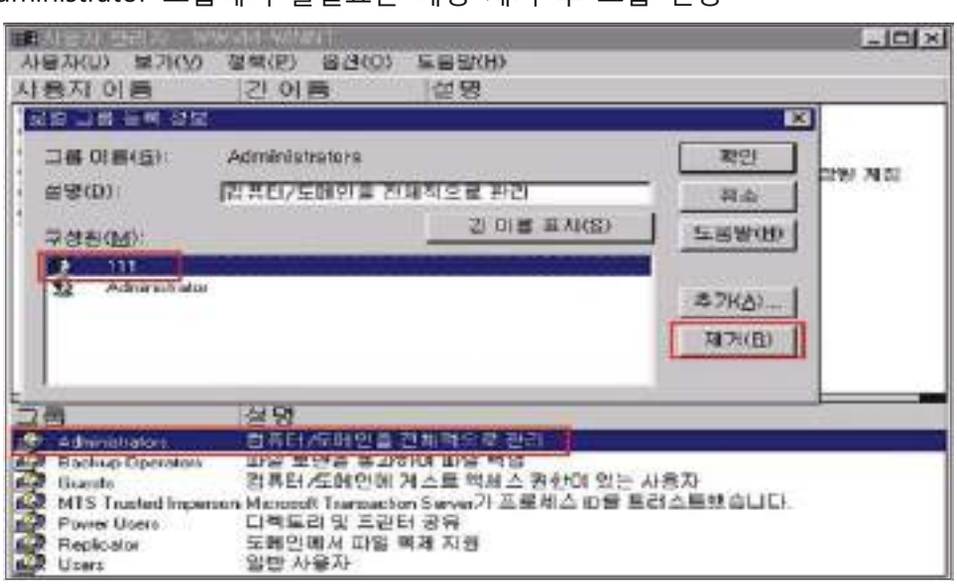
조치 시 영향	일반적인 경우 영향 없음

W-06 (상)	1. 계정관리 > 1.6 관리자 그룹에 최소한의 사용자 포함
취약점 개요	
점검내용	■ 관리자 그룹에 불필요한 사용자의 포함 여부 점검
점검목적	■ 관리자 그룹 구성원에 불필요한 사용자의 포함 여부를 점검하여, 관리 권한자를 최소화 하고자 함
보안위협	■ Administrators와 같은 관리자 그룹에 속한 구성원은 컴퓨터 시스템에 대한 완전하고 제한 없는 액세스 권한을 가지므로, 사용자를 관리자 그룹에 포함 시킬 경우 비인가 사용자에 대한 과도한 관리 권한이 부여될 수 있음
참고	※ 관리 권한의 오남용으로 인한 시스템 피해를 줄이기 위해서 관리 업무를 위한 계정과 일반 업무를 위한 계정을 분리하여 사용하는 것이 바람직함 ※ 시스템 관리를 위해서 관리권한 계정과 일반권한 계정을 분리하여 운영하는 것을 권고 ※ 시스템 관리자는 원칙적으로 1명 이하로 유지하고, 부득이하게 2명 이상의 관리 권한자를 유지하여야 하는 경우에는 관리자 그룹에는 최소한의 사용자만 포함하도록 하여야 함
점검대상 및 판단기준	
대상	■ Windows NT, 2000, 2003, 2008, 2012
판단기준	**양호 :** Administrators 그룹의 구성원을 1명 이하로 유지하거나, 불필요한 관리자 계정이 존재하지 않는 경우
	취약 : Administrators 그룹에 불필요한 관리자 계정이 존재하는 경우
조치방법	Administrators 그룹에 포함된 불필요한 계정 제거
점검 및 조치 사례	

■ **Window NT**

Step 1) 시작> 프로그램> 관리도구> 도메인 사용자 관리> Administrators 그룹> 등록 정보

Step 2) Administrator 그룹에서 불필요한 계정 제거 후 그룹 변경



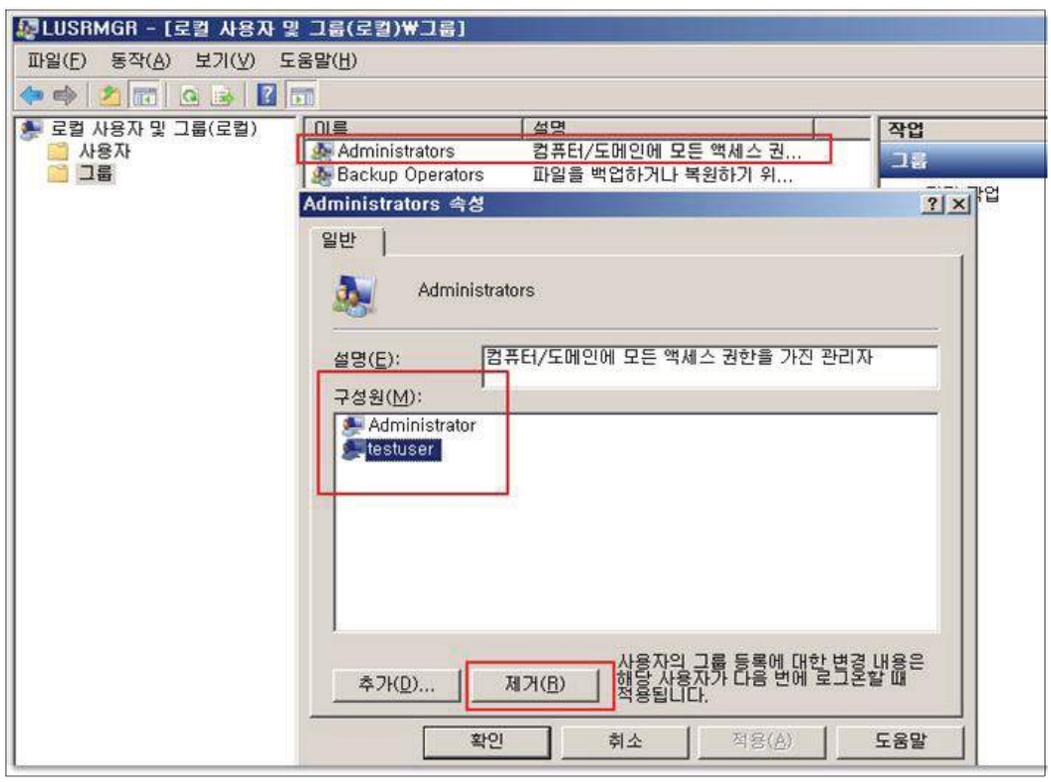
Windows 서버

W-06 (상)	1. 계정관리 > 1.6 관리자 그룹에 최소한의 사용자 포함

■ **Windows 2000, 2003, 2008, 2012**

Step 1) 시작> 실행> LUSRMGR.MSC> 그룹> Administrators> 속성

Step 2) Administrators 그룹에서 불필요한 계정 제거 후 그룹 변경

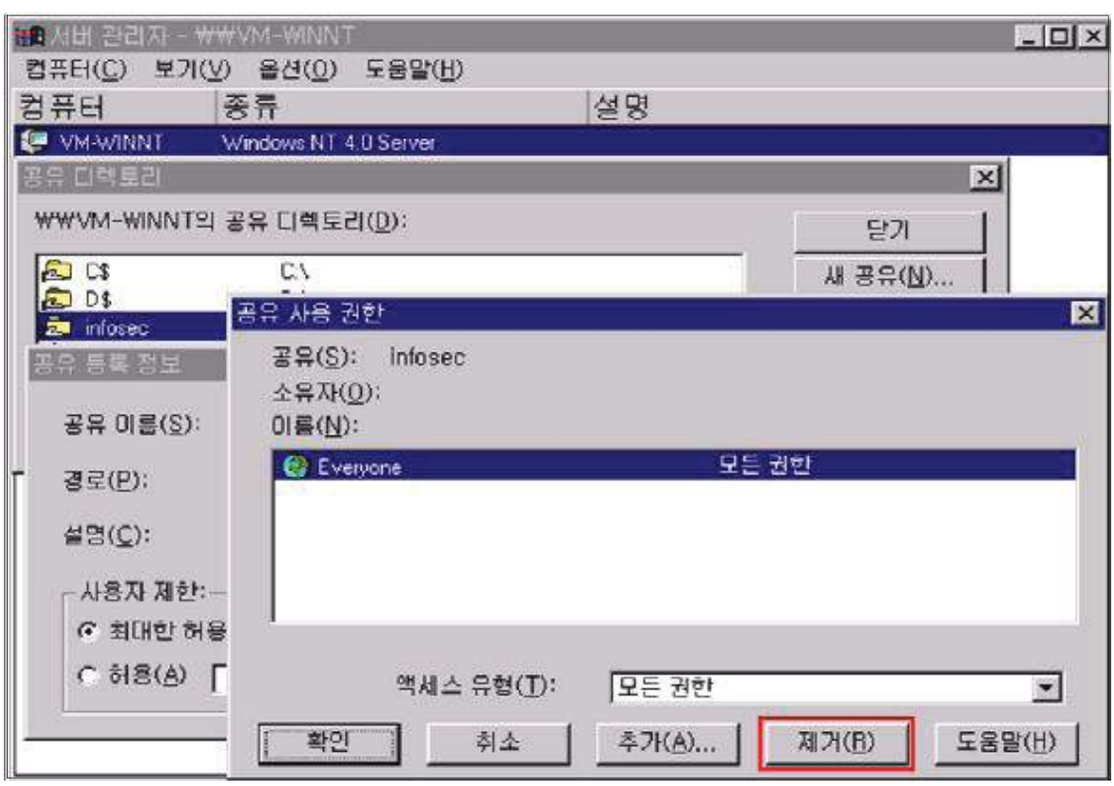


조치 시 영향	Administrator 그룹에 있는 계정을 잘못 삭제하는 경우 해당 업무에 장애 발생 가능성이 있음

W-7 (상)	2. 서비스 관리 > 2.1 공유 권한 및 사용자 그룹 설정
취약점 개요	
점검내용	■ 공유 디렉토리 내 Everyone 권한 존재 여부 점검
점검목적	■ 디폴트 공유인 C$, D$, Admin$, IPC$ 등을 제외한 공유 폴더에 Everyone 그룹으로 공유되는 것을 금지하여 익명 사용자의 접근을 차단하기 위함
보안위협	■ Everyone이 공유계정에 포함되어 있으면 익명 사용자의 접근이 가능하여 내부 정보 유출 및 악성코드의 감염 우려가 있음
참고	-
점검대상 및 판단기준	
대상	■ Windows NT, 2000, 2003, 2008, 2012
판단기준	**양호 :** 일반 공유 디렉토리가 없거나 공유 디렉토리 접근 권한에 Everyone 권한이 없는 경우
	취약 : 일반 공유 디렉토리의 접근 권한에 Everyone 권한이 있는 경우
조치방법	공유 디렉토리 접근 권한에서 Everyone 권한 제거 후 필요한 계정 추가
점검 및 조치 사례	

■ **Windows NT**

Step 1) 프로그램> 관리도구> 서버 관리자> 컴퓨터> 공유 디렉토리> 등록정보> 사용 권한에서 Everyone 으로 된 공유를 제거하고 접근이 필요한 계정의 적절한 권한 추가



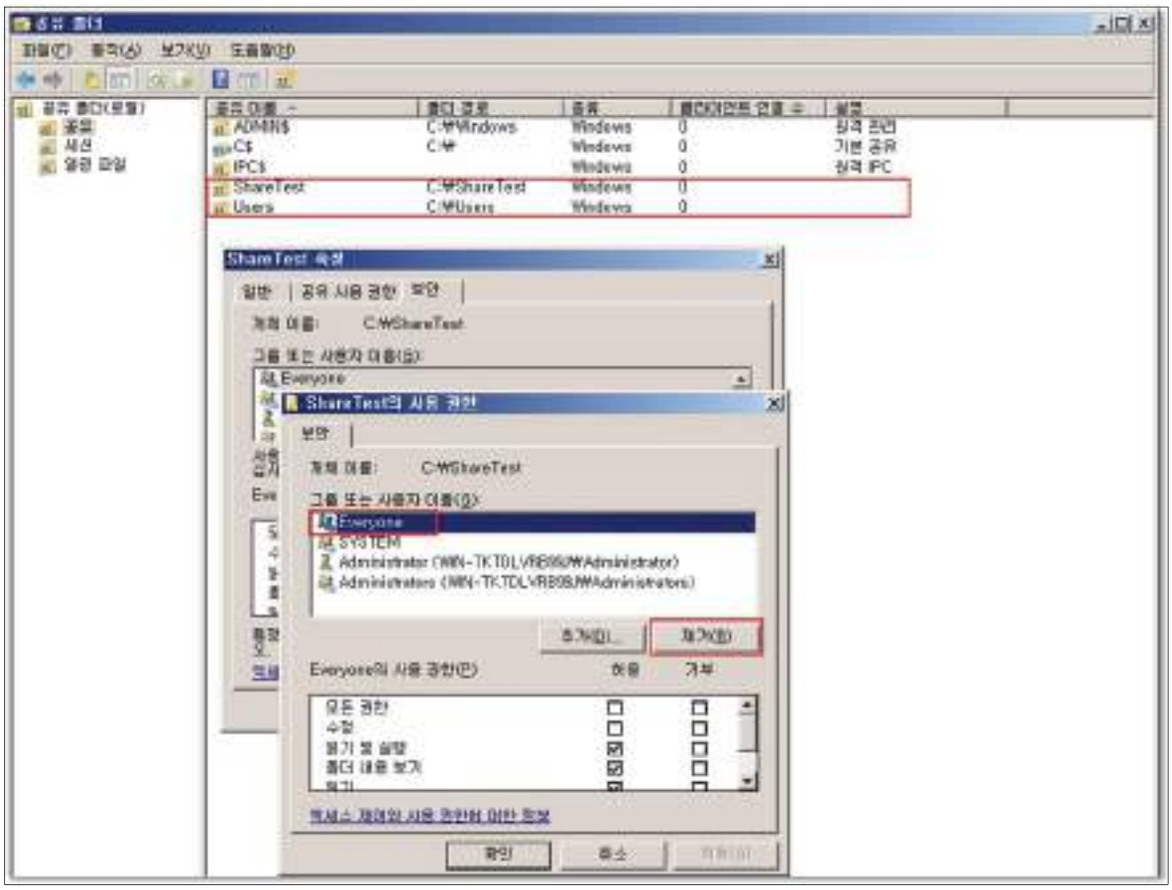
Windows 서버

W-7 (상)	2. 서비스 관리 > 2.1 공유 권한 및 사용자 그룹 설정

■ **Windows 2000, 2003, 2008, 2012**

Step 1) 시작> 실행> FSMGMT.MSC> 공유

Step 2) 사용 권한에서 Everyone 으로 된 공유를 제거하고 접근이 필요한 계정의 적절한 권한 추가

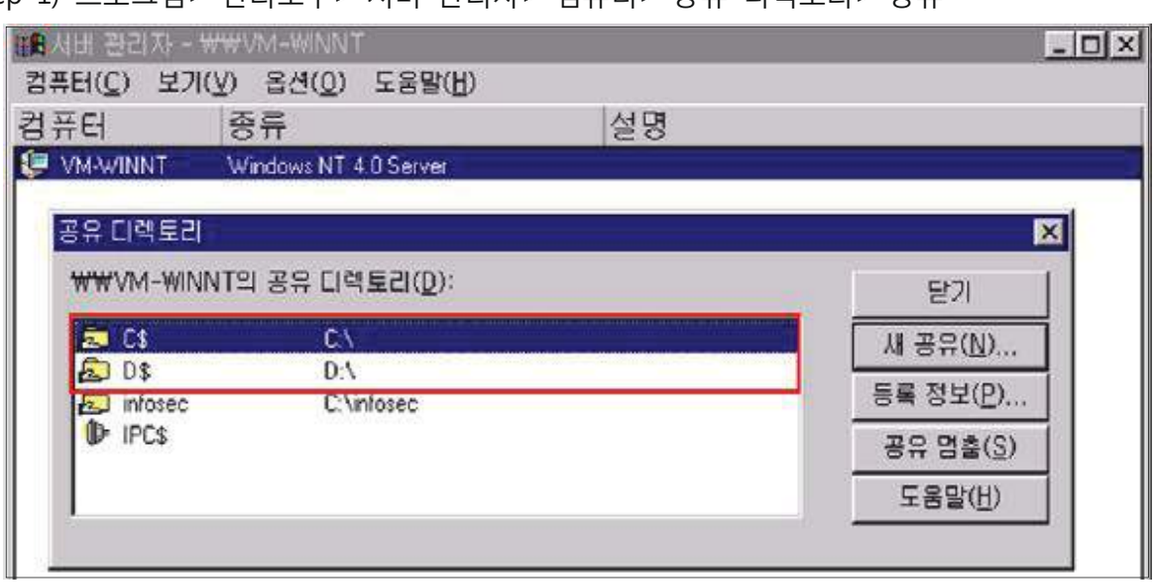


조치 시 영향	애플리케이션이나 Backup 용도로 Everyone 공유를 사용하는 경우 해당 작업에 영향 가능

W-8 (상)	2. 서비스 관리 > 2.2 하드디스크 기본 공유 제거
취약점 개요	
점검내용	■ 하드디스크 기본 공유 제거 여부 점검
점검목적	■ 하드디스크 기본 공유를 제거하여 시스템 정보 노출을 차단하고자 함
보안위협	■ 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
참고	※ **기본 공유:** 관리목적으로 자동 생성되는 공유 드라이브(Administrative share). 이러한 드라이브들은 C$, D$, E$ 등과 같이 이름 뒤에 $가 붙어서 숨겨진 공유로 처리되며, Windows 2000, XP에서는 관리자 ID와 Password를 알고 있으면 네트워크를 통해 이러한 공유 드라이브들에 자유롭게 접근할 수 있음. 그러나 이후 버전 Windows에서는 보안상의 이유로 로컬시스템의 관리자가 네트워크를 통해 시스템을 관리하지 못하도록 기본적으로 차단됨
점검대상 및 판단기준	
대상	■ Windows NT, 2000, 2003, 2008, 2012
판단기준	**양호 :** 레지스트리의 AutoShareServer (WinNT: AutoShareWks)가 0이며 기본 공유가 존재하지 않는 경우
	취약 : 레지스트리의AutoShareServer (WinNT: AutoShareWks)가 1이거나 기본 공유가 존재하는 경우
조치방법	기본 공유 중지 후 레지스트리 값 설정(IPC$, 일반 공유 제외)
점검 및 조치 사례	

■ **Windows NT**

Step 1) 프로그램> 관리도구> 서버 관리자> 컴퓨터> 공유 디렉토리> 공유

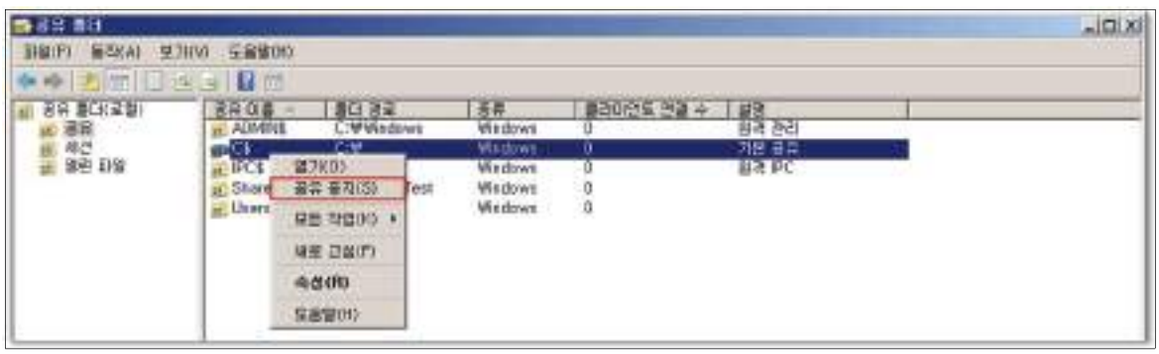


Windows 서버

W-8 (상)	2. 서비스 관리 > 2.2 하드디스크 기본 공유 제거

■ **Windows 2000, 2003, 2008, 2012**

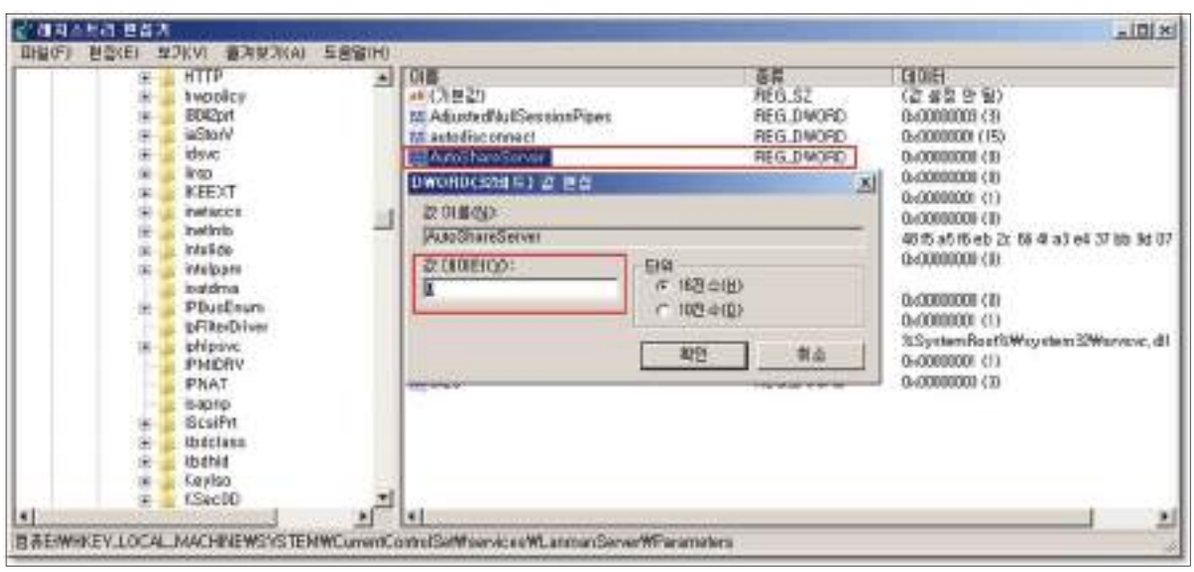
Step 1) 시작> 실행> FSMGMT.MSC> 공유> 기본 공유 선택> 마우스 우클릭> 공유 중지



Step 2) 시작> 실행> REGEDIT

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

"HKLM₩SYSTEM₩CurrentControlSet₩Services₩lanmanserver₩parameters₩AutoShareServer"(Windows NT일 경우: AutoShareWks)



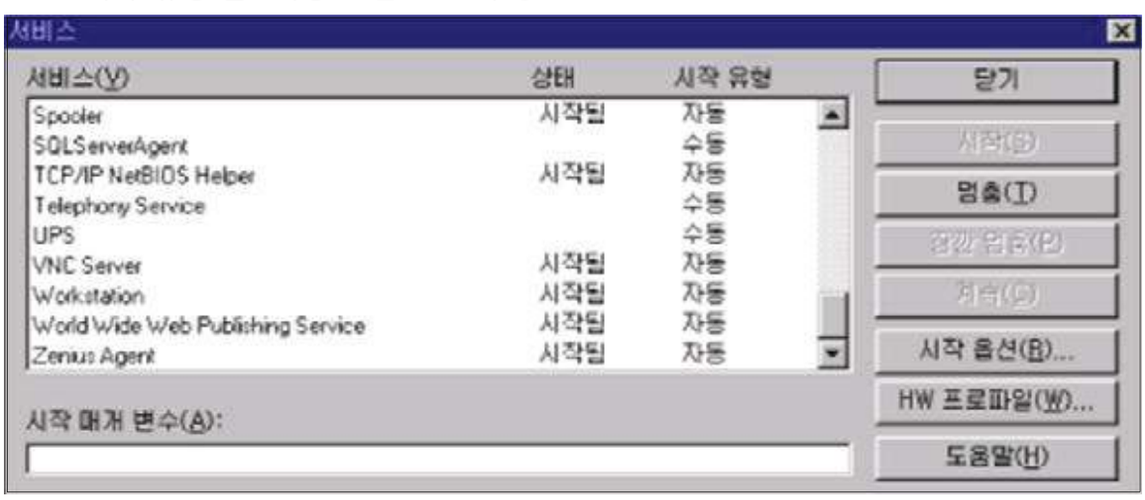
※ 방화벽과 라우터에서 135~139(TCP/UDP)포트를 차단하여 외부로부터의 위험을 제거함으로써 보안성을 높일 수 있음 (Windows 2008 제외)

조치 시 영향	Active Directory, Clustered system에서는 적용 시 영향 있음 ※ **Active Directory:** 중앙 집중화된 자원 관리를 위한 계층적 디렉토리 서비스 ※ **Clustered system:** 여러 개의 시스템을 결합하여 사용함

W-9 (상)	2. 서비스 관리 > 2.3 불필요한 서비스 제거
취약점 개요	
점검내용	■ 불필요한 서비스 가동 여부 점검
점검목적	■ 사용자 환경에 필요하지 않은 서비스 및 실행 파일을 제거하거나 비활성화 처리하여 이를 통한 악의적인 공격을 차단하기 위함
보안위협	■ 시스템에 기본적으로 설치되는 불필요한 취약 서비스들이 제거되지 않은 경우, 해당 서비스의 취약점으로 인한 공격이 가능하며, 네트워크 서비스의 경우 열린 포트를 통한 외부 침입의 가능성이 존재함
참고	※ OS 버전에 따라 '일반적으로 불필요한 서비스' 목록에 나열된 서비스가 제공되지 않을 수 있음
점검대상 및 판단기준	
대상	■ Windows NT, 2000, 2003, 2008, 2012
판단기준	**양호 :** 일반적으로 불필요한 서비스(아래 목록 참조)가 중지되어 있는 경우
	취약 : 일반적으로 불필요한 서비스(아래 목록 참조)가 구동 중인 경우
조치방법	서비스 중지 후 "사용 안 함" 설정
점검 및 조치 사례	

■ **Windows NT**

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



Step 2) 해당 서비스를 선택하고 오른쪽 메뉴에서 "시작 옵션"을 클릭하면 시스템이 시작할 때에 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

Windows 서버

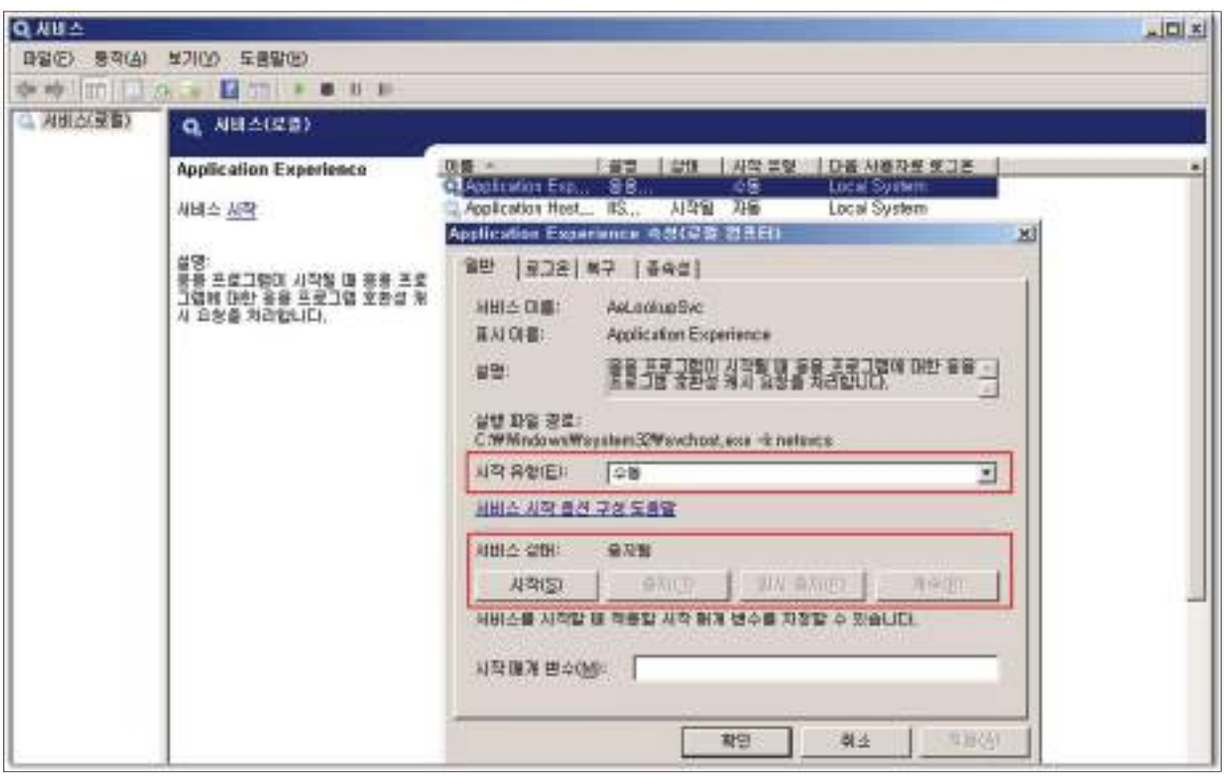
W-9 (상)	2. 서비스 관리 > 2.3 불필요한 서비스 제거

■ **Windows 2000, 2003, 2008, 2012**

Step 1) 시작> 실행> SERVICES.MSC> "해당 서비스" 선택> 속성

Step 2) 시작 유형 -> 사용 안 함

Step 3) 서비스 상태 -> 중지 설정



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

W-9 (상)	2. 서비스 관리 > 2.3 불필요한 서비스 제거

각 서비스마다 옵션을 설정할 수 있으며 해당 서비스를 선택하고 더블 클릭하게 되면 시작 유형을 선택할 수 있으며 시작 시 로그온 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

※ 일반적으로 불필요한 서비스

서비스명	기능 및 설명
Alerter	네트워크상에서 사용자와 컴퓨터에 관리용 경고메시지를 전송하는 기능
Automatic Updates	중요한 윈도우 업데이트를 다운로드하고 설치할 수 있도록 하는 애플리케이션. 수동패치를 적용하거나, MS패치 관리 서버로 패치를 일괄적으로 관리하는 경우 불필요한 서비스
Clipbook	서버 내 Clipbook을 다른 클라이언트와 공유
Computer Browser	네트워크에 있는 모든 컴퓨터의 목록을 업데이트 하고 관리하는 기능
Cryptographic Services	윈도우 파일의 서명을 확인하는 카탈로그 데이터베이스 서비스를 총괄
DHCP Client	IP 주소와 DNS 이름을 DHCP 서버에 등록하거나 DHCP 서버로부터 동적으로 IP주소를 가져오는 기능을 수행. 단독으로 시스템을 수행하며 고정IP를 사용하는 경우 불필요한 서비스
Distributed Link Tracking Client, Server	네트워크 도메인의 여러 컴퓨터나 일반컴퓨터에서 NTFS 파일간의 연결을 관리하는 도구. Active Directory가 구성되어 있지 않은 서버에서는 불필요한 서비스.
DNS Client	컴퓨터에 대한 도메인 이름 시스템(DNS)이름을 확인하고 캐시에 보관하는기능. DNS 서버가 아닌 시스템에서는 유명무실하나, IPSEC을 사용하는 경우 필요한 경우 있음
Error reporting Service	프로그램 오류가 시 응용프로그램의 오류를 MS에 보고한다는 내용을 표시하는 기능
Human Interface Device Access	키보드 또는 기타 멀티미디어 장치에 사전 정의된 버튼들을 사용하는 HID장치들을 위한 서비스
IMAPI CD-Burning COM Service	서버에 CD-RW 또는 DVD-RW가 장착되어 보조백업장치 역할을 하기 위해서 자체 레코딩 백업을 할 수 있음
Messenger	클라이언트와 서버 사이에 netsend 및 경고서비스 메시지를 전송하는 기능
NetMeeting Remote Desktop Sharing	윈도우9X 운영체제부터 인증된 사용자가 넷미팅을 사용해서 원격으로 컴퓨터에 접근할 수 있도록 하는 기능
Portable Media Serial Number	컴퓨터에 연결된 이동성 음악연주기(미디기기)의 등록번호를 복원하는 기능
Print Spooler	인쇄 과정에 있는 스풀링을 관리하는 서비스. 프린터가 있는 경우 필수 서비스이나, 프린터가 연결되지 않은 시스템에서는 불필요함
Remote Registry	원격 사용자가 이 컴퓨터에서 레지스트리 설정을 수정할 수 있도록 설정하는 애플리케이션
Simple TCP/IP Services	Echo, Discard, Character Generator, Daytime, Quote of the Day 지원
Wireless Zero Configuration	802.11 어댑터에 대해 자동 구성을 공급하는 기본적인 도구

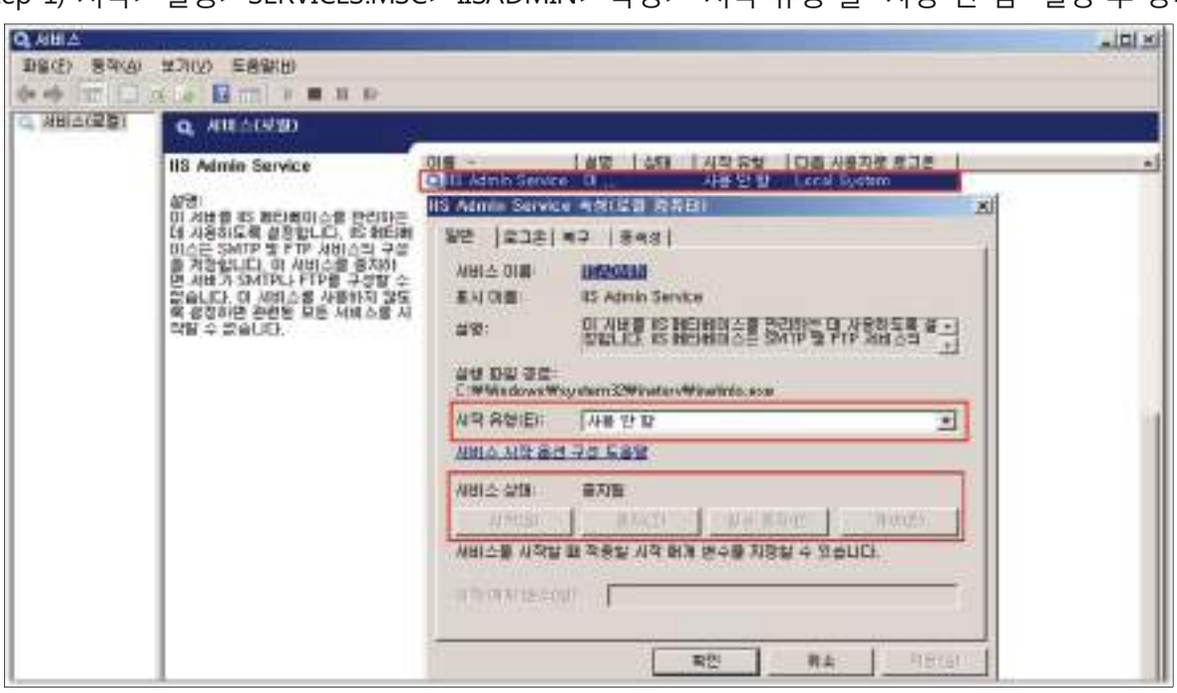
Windows 서버

W-9 (상)	2. 서비스 관리 > 2.3 불필요한 서비스 제거
운영중인 시스템에서 필수 서비스를 정의하는 것은 매우 복잡한 과정으로 서비스 사용 여부는 시스템의 영향성을 고려하여 신중하게 평가되어야 하므로 Microsoft에서 권고하는 가이드에 따라 전략적으로 적용하여야 함 ※ https://technet.microsoft.com/ko-kr/library/dd547941.aspx (서비스 및 서비스 계정 보안 계획 가이드) 참고 윈도우 시스템 설치 시 기본적으로 설치되는 서비스에 대한 상세 설명은 아래 주소 참조 https://technet.microsoft.com/ko-kr/library/dd547949.aspx	
조치 시 영향	일반적으로 영향 없음

W-10 (상)	2. 서비스 관리 > 2.4 IIS 서비스 구동 점검
취약점 개요	
점검내용	■ 불필요한 IIS 서비스 구동 여부 점검
점검목적	■ 불필요한 IIS 서비스가 구동 상태인지를 점검하여 제거하고, 해당 서비스가 취약점이 제거되지 않은 상태로 외부 위협에 노출되지 않도록 하기 위함
보안위협	■ IIS 서비스는 WEB, FTP 등의 서비스를 제공해주는 유용한 서비스이나 프로파일링, 서비스 거부, 불법적인 접근, 임의의 코드실행, 정보 공개, 바이러스, 웜, 트로이목마 등의 위협에 노출될 수 있어 서비스 불필요 시 삭제하여야 함
참고	※ 일반적으로 불필요한 서비스가 시스템 내 구동되고 있는 경우에는 관리되지 않은 상태로 방치되는 경우가 많아 보안 취약점이 그대로 노출되어 악의적인 공격의 대상이 될 수 있음
점검대상 및 판단기준	
대상	■ Windows NT, 2000, 2003, 2008, 2012
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
점검 및 조치 사례	

■ **Windows NT, 2000, 2003, 2008, 2012**

Step 1) 시작> 실행> SERVICES.MSC> IISADMIN> 속성> "시작 유형"을 "사용 안 함" 설정 후 중지



※ IIS 가 설치되어 있지 않을 경우 SERVICES.MSC 에서 보이지 않음

조치 시 영향	일반적인 경우 영향 없음

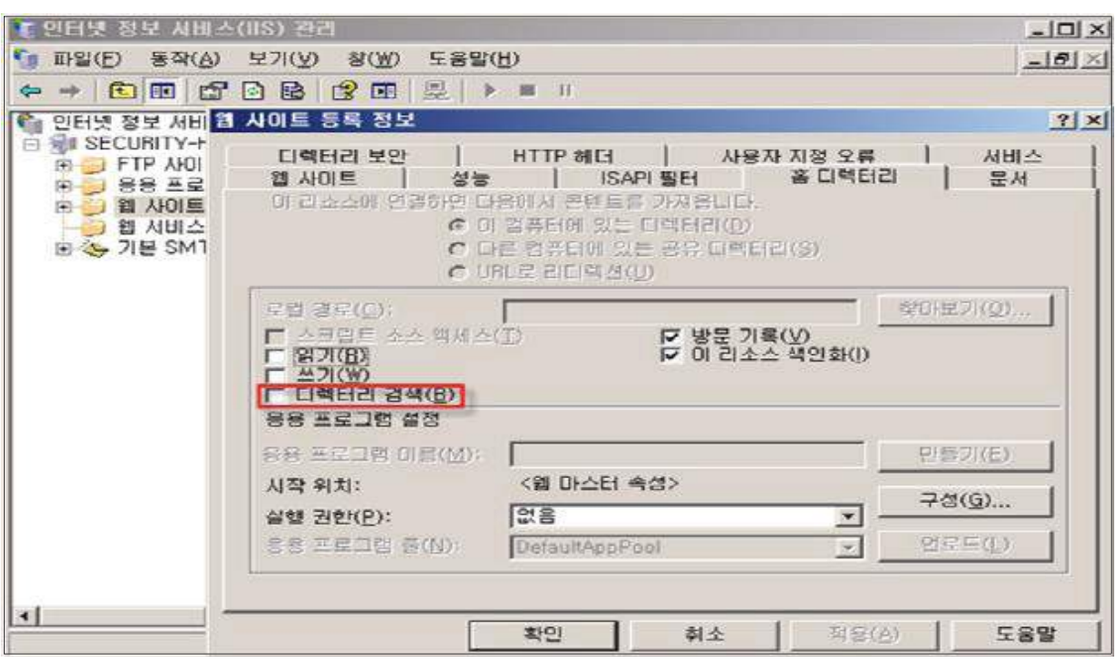
Windows 서버

W-11 (상)	2. 서비스 관리 > 2.5 디렉토리 리스팅 제거
취약점 개요	
점검내용	■ 웹서버 디렉토리 리스팅 차단 설정 여부 점검
점검목적	■ 웹서버 특정 폴더에 대한 디렉토리 리스팅 취약점을 제거하여, 불필요한 파일 정보 노출을 차단하기 위함
보안위협	■ 웹서버에 디렉토리 리스팅이 제거되지 않은 경우 외부에서 디렉토리 내에 보유하고 있는 모든 파일 목록 확인 및 파일에 대한 접근이 가능하여 주요 정보의 유출의 가능성이 있음
참고	※ **디렉토리 리스팅 취약점:** 디렉토리에 대한 요청 시 기본 페이지가 호출되어 사용자에게 전송하지만, 기본 페이지가 존재하지 않는 경우 디렉토리 내에 존재하는 모든 파일의 목록을 보여주는 취약점
점검대상 및 판단기준	
대상	■ Windows 2000, 2003, 2008, 2012
판단기준	**양호 :** "디렉토리 검색" 체크하지 않음
	취약 : "디렉토리 검색" 체크함 ※ 조치 시 마스터 속성과 모든 사이트에 적용함
조치방법	사용하지 않는 경우 IIS 서비스 중지, 사용할 경우 디렉토리 검색 체크 해제
점검 및 조치 사례	

■ **Windows 2000(IIS 5.0), 2003(IIS 6.0)**

Step 1) 시작> 실행> INETMGR> 웹 사이트> 속성> 홈 디렉토리

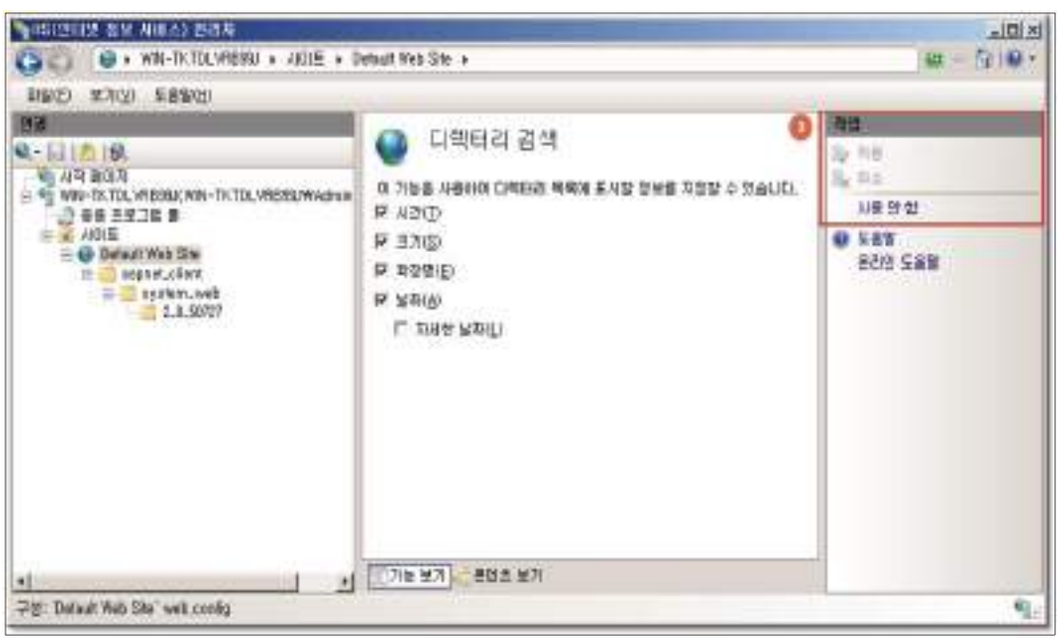
Step 2) "디렉토리 검색" 체크 해제



W-11 (상)	2. 서비스 관리 > 2.5 디렉토리 리스팅 제거

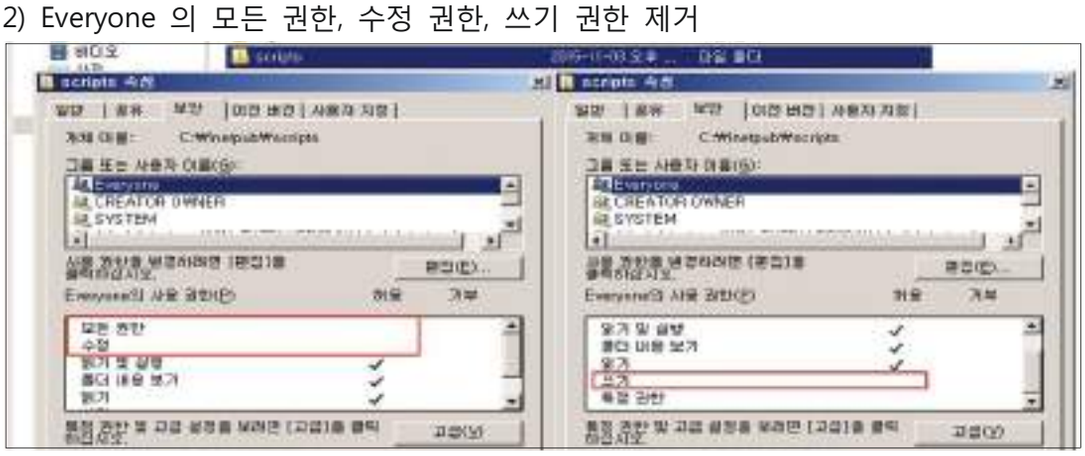
■ **Windows 2008(IIS 7.0), 2012(IIS 8.0)**

Step 1) 제어판> 관리도구> 인터넷 정보 서비스(IIS) 관리> 해당 웹 사이트> IIS> "디렉토리 검색" 선택 후 "사용 안 함" 선택



조치 시 영향	일반적인 경우 영향 없음

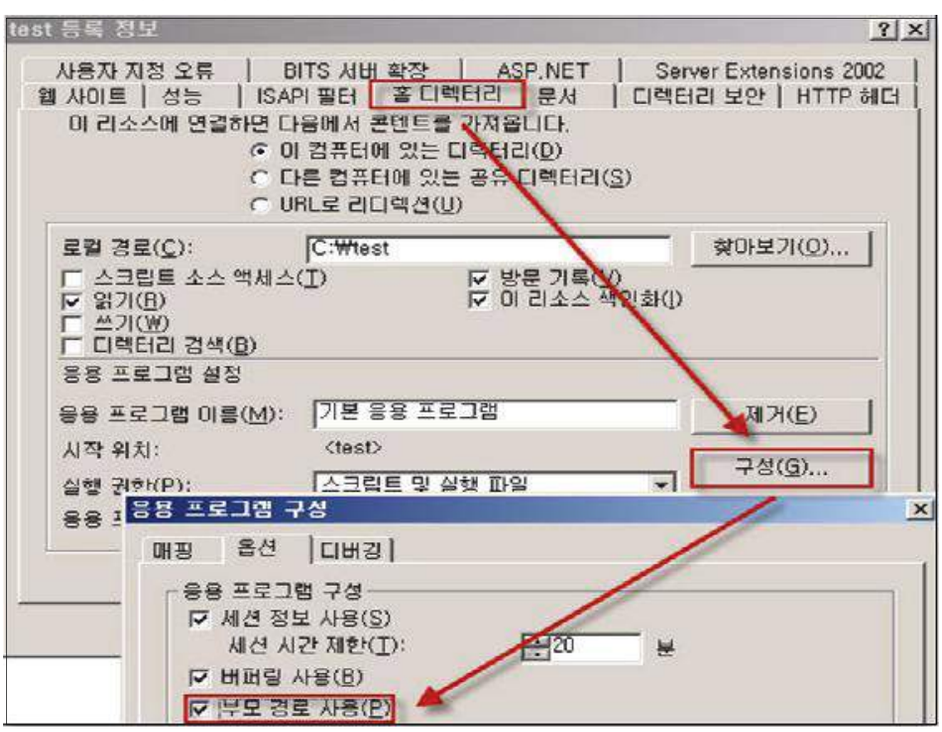
Windows 서버

W-12 (상)	2. 서비스 관리 > 2.6 IIS CGI 실행 제한
취약점 개요	
점검내용	■ IIS CGI 실행 제한 설정 여부 점검
점검목적	■ CGI 스크립트를 정해진 디렉토리에서만 실행되도록 하여 악의적인 파일의 업로드 및 실행을 방지하기 위함
보안위협	■ 게시판이나 자료실과 같이 업로드 되는 파일이 저장되는 디렉토리에 CGI 스크립트가 실행 가능한 경우 악의적인 파일을 업로드하고 이를 실행하여 시스템의 중요 정보가 노출될 수 있으며 침해사고의 경로로 이용될 수 있음.
참고	※ **CGI(Common Gateway Interface):** 사용자가 서버로 보낸 데이터를 서버에서 작동중인 데이터처리프로그램에 전달하고, 여기에서 처리된 데이터를 다시 서버로 되돌려 보내는 등의 일을 하는 프로그램 ※ 일반적으로 기본 CGI 디렉토리(C:₩inetpub₩scripts)는 사용하지 않음
점검대상 및 판단기준	
대상	■ Windows 2000, 2003, 2008, 2012
판단기준	**양호 :** 해당 디렉토리 Everyone에 모든 권한, 수정 권한, 쓰기 권한이 부여되지 않은 경우
	취약 : 해당 디렉토리 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)
점검 및 조치 사례	
■ **Windows 2000(IIS 5.0), 2003(IIS 6.0), 2008(IIS 7.0), 2012(IIS 8.0)** Step 1) 탐색기> 해당 디렉토리> 속성> 보안 (기본 CGI 디렉토리 위치 C:₩inetpub₩scripts) Step 2) Everyone 의 모든 권한, 수정 권한, 쓰기 권한 제거  ※ IIS 초기 구축시에는 scripts 폴더가 생성되지 않을 수 있음	
조치 시 영향	해당 디렉토리 확인 후 추가적인 파일이 없다면 영향 없음

W-13 (상)	2. 서비스 관리 > 2.7 IIS 상위 디렉토리 접근 금지
취약점 개요	
점검내용	■ IIS 상위 디렉토리 접근 금지 설정 적용 여부 점검
점검목적	■ ".." 와 같은 웹서버 상에서 상위 경로를 사용하지 못하도록 설정하여 Unicode 버그 및 서비스 거부 공격에 이용당하지 않도록 하기 위함
보안위협	■ 이용자가 상위경로로 이동하는 것이 가능할 경우 하위경로에서 상위로 접근하며 정보 탐색이 가능하여 중요 정보가 노출될 가능성이 존재함
참고	※ ".."는 unicode 버그, 서비스 거부와 같은 공격에 쉽게 이용되므로 허용하지 않는 것을 권장함
점검대상 및 판단기준	
대상	■ Windows 2000, 2003, 2008, 2012
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)
점검 및 조치 사례	

■ **Windows 2000(IIS 5.0), 2003(IIS 6.0)**

Step 1) 인터넷 정보 서비스(IIS) 관리> 해당 웹사이트> 속성> 홈디렉토리> 구성> [옵션] 탭에서 "부모 경로 사용" 의 체크박스 해제 확인

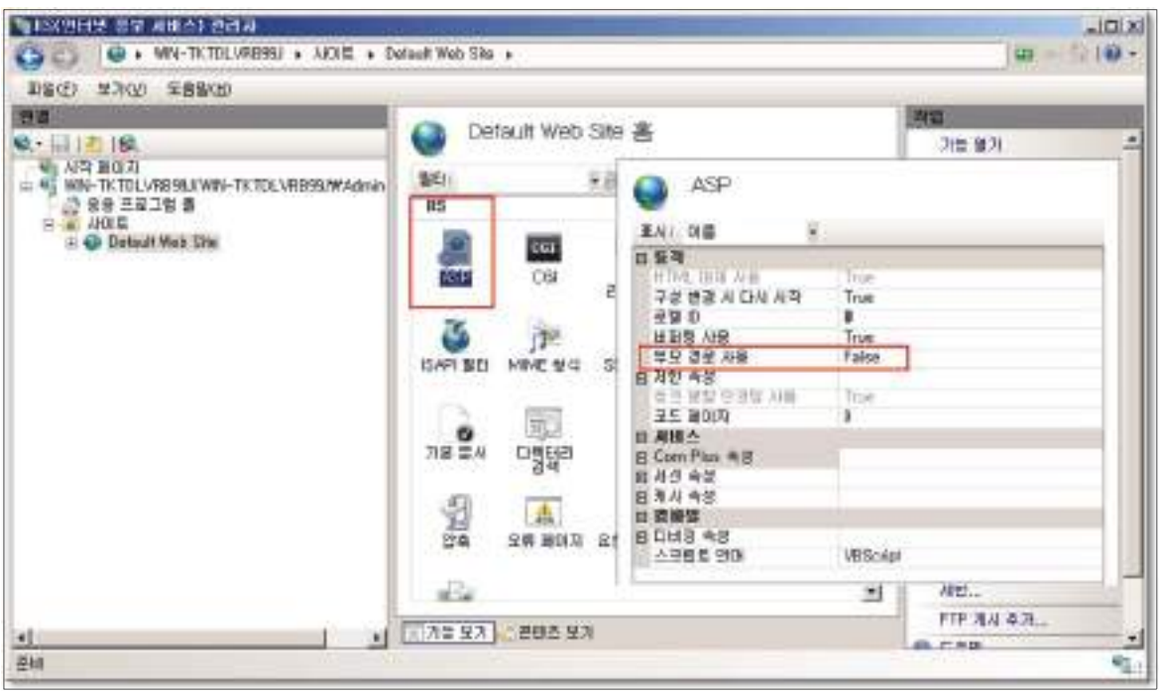


Windows 서버

W-13 (상)	2. 서비스 관리 > 2.7 IIS 상위 디렉토리 접근 금지

■ **Windows 2008(IIS 7.0), 2012(IIS 8.0)**

Step 1) 제어판> 관리도구> 인터넷 정보 서비스(IIS) 관리자> 해당 웹사이트> IIS> ASP 선택, "부모 경로 사용" 항목 "False" 설정 확인



조치 시 영향	"../" 와 같이 상대경로를 사용하도록 하드 코딩되어 있는 애플리케이션의 경우 영향 있음

W-14 (상)	2. 서비스 관리 > 2.8 IIS 불필요한 파일 제거
취약점 개요	
점검내용	■ IIS 설치 시 기본적으로 제공되는 불필요한 파일 제거 여부 점검
점검목적	■ IIS 서비스 설치 시 기본으로 설치되는 예제 스크립트, 설명서, 샘플 애플리케이션, 디렉토리 등 서비스에 불필요한 IIS 모듈을 제거하여 불필요한 공격 대상으로 이용되는 것을 방지하기 위함
보안위협	■ IIS 서비스 설치 시 기본적으로 제공 되는 파일 및 디렉토리를 제거하지 않을 경우, 해당 파일들로 인해 공격 대상으로 이용되거나 백도어가 심어질 위험이 존재함
참고	-
점검대상 및 판단기준	
대상	■ Windows 2000, 2003
판단기준	**양호 :** 해당 웹 사이트에 IISSamples, IISHelp 가상 디렉토리가 존재하지 않는 경우
	취약 : 해당 웹 사이트에 IISSamples, IISHelp 가상 디렉토리가 존재하는 경우 ※ 조치 시 마스터 속성과 모든 사이트에 적용함
조치방법	사용하지 않는 경우 IIS 서비스 중지, 사용할 경우 가상 디렉토리 삭제
점검 및 조치 사례	
■ **Windows 2000(IIS 5.0), 2003(IIS 6.0)** Step 1) Sample 디렉토리 확인 후 삭제함 c:₩inetpub₩iissamples c:₩winnt₩help₩iishelp (IIS 설명서) c:₩program files₩common files₩system₩msadc₩sample (데이터 액세스) %SystemRoot%₩System32₩Inetsrv₩IISADMPWD ※ IIS 7.0(Windows 2008) 이상 버전 해당 사항 없음	
조치 시 영향	일반적인 경우 영향 없음

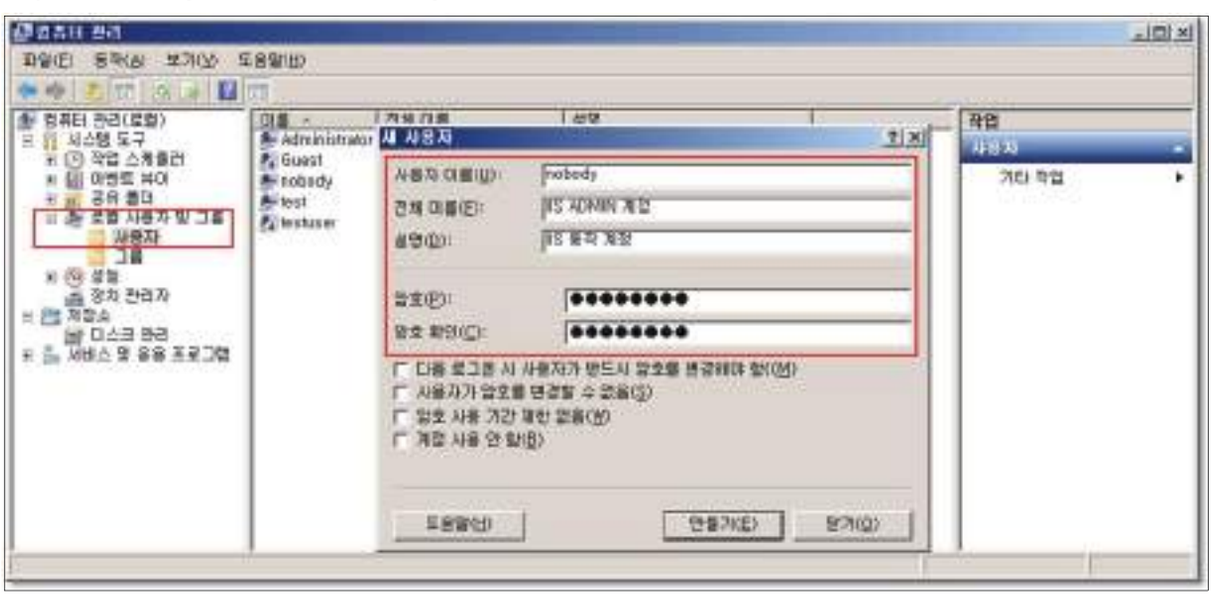
Windows 서버

W-15 (상)	2. 서비스 관리 > 2.9 웹 프로세스 권한 제한
취약점 개요	
점검내용	■ 웹 프로세스 권한 제한 설정 여부 점검
점검목적	■ 웹 프로세스가 웹 서비스 운영에 필요한 최소한의 권한만을 갖도록 제한하여 웹사이트 방문자가 웹 서비스의 취약점을 이용해 시스템에 대한 어떤 권한도 획득할 수 없도록 하기 위함
보안위협	■ 웹 프로세스 권한을 제한하지 않은 경우 웹 사이트 방문자가 웹 서비스의 취약점을 이용하여 시스템 권한을 획득할 수 있으며, 웹 취약점을 통해 접속 권한을 획득한 경우에는 관리자 권한을 획득하여 서버에 접속 후 정보의 변경, 훼손 및 유출 할 우려가 있음
참고	※ 참고로 최소 권한의 계정으로 IIS를 구동 시키는 것 이외에 '웹 사이트 등록정보' > '홈 디렉토리' > 응용프로그램 보호(IIS 프로세스 권한 설정)에서도 프로세스 권한을 설정할 수 있음 (점검 및 조치 사례 하단 참조)
점검대상 및 판단기준	
대상	■ Windows NT, 2000, 2003, 2008, 2012
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
점검 및 조치 사례	

■ Windows NT, 2000, 2003, 2008, 2012

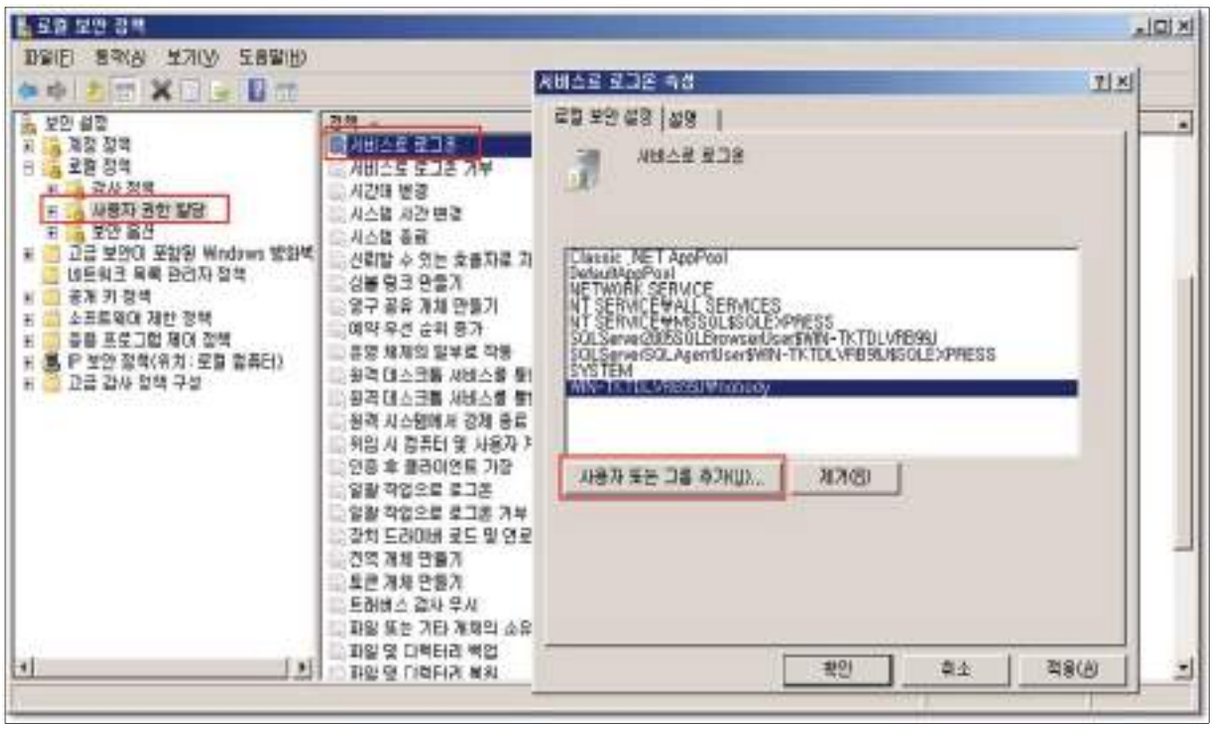
Step 1) 시작> 제어판> 관리도구> 컴퓨터 관리> 로컬 사용자 및 그룹> 사용자 선택

Step 2) nobody 계정 추가(nobody 계정의 소속 그룹에 정해진 User가 있으면 제거)

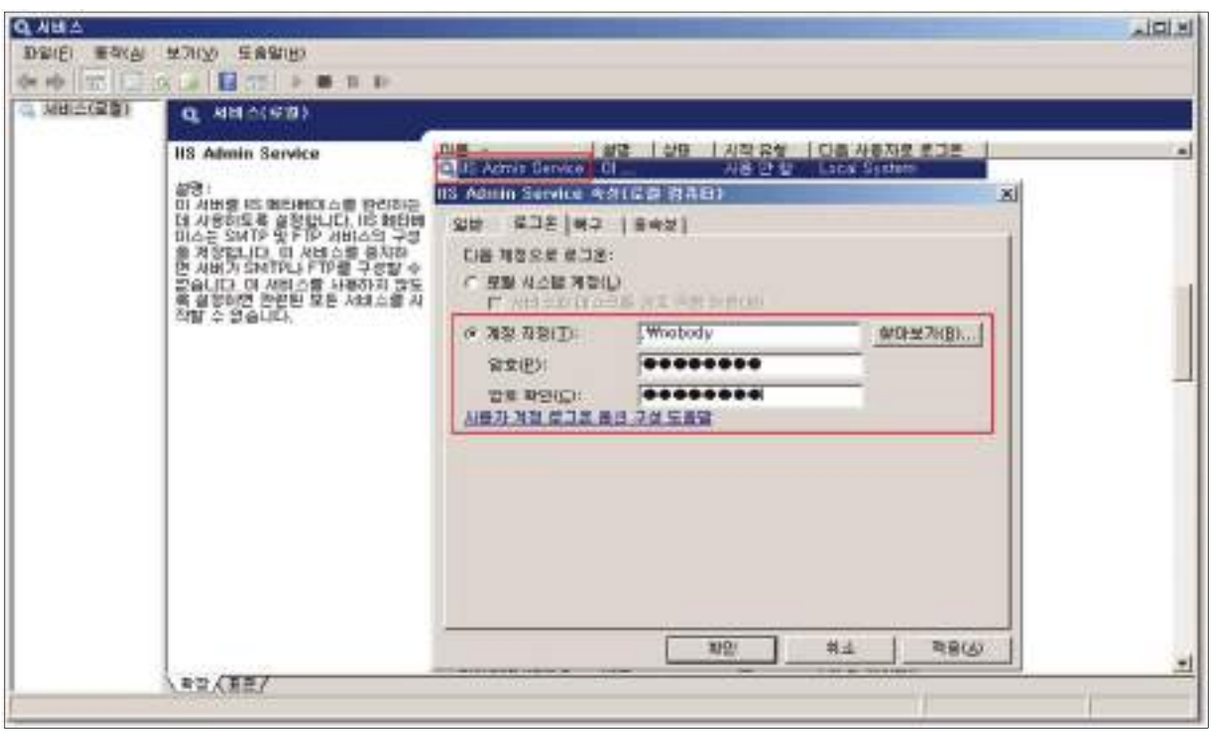


W-15 (상)	2. 서비스 관리 > 2.9 웹 프로세스 권한 제한

Step 3) 시작> 제어판> 관리도구> 로컬 보안 정책> 로컬 정책> 사용자 권한 할당 선택, "서비스 로그온"에 "nobody" 계정 추가



Step 4) 시작> 실행> SERVICES.MSC> IIS Admin Service> 속성> [로그온] 탭의 계정 지정에 nobody 계정 및 패스워드 입력



Windows 서버

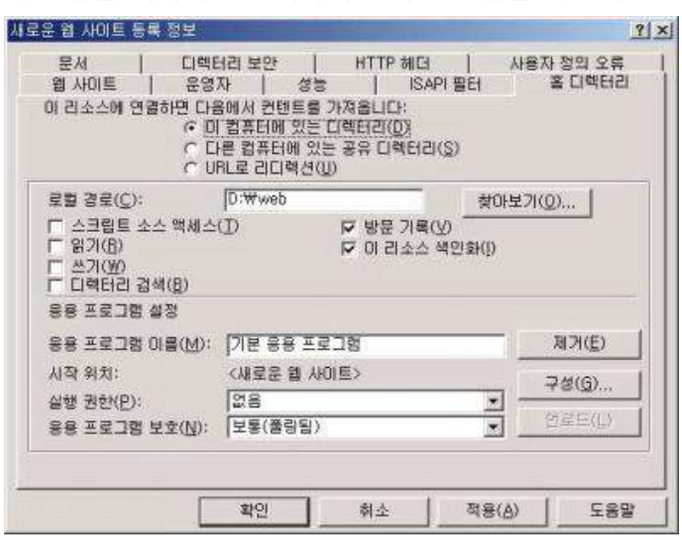
W-15 (상)	2. 서비스 관리 > 2.9 웹 프로세스 권한 제한

Step 5) 시작> 프로그램> 윈도우 탐색기> IIS 가 설치된 폴더 속성> [보안] 탭에서 nobody 계정을 추가하고 모든 권한 체크

※ '웹 사이트 등록정보' > '홈 디렉토리 > 응용프로그램 보호(IIS 프로세스 권한 설정)

- **낮음(IIS 프로세스)**: IIS 프로세스는 시스템 권한을 가짐
- **보통(풀링됨)**: IIS 프로세스를 실행과 동시에 일반 권한의 계정으로 권한 강하(falling)
- **높음(격리됨)**: IIS 프로세스를 Guest 권한에 준하는 권한으로 실행시킴

세 가지 권한 중 '낮음'으로 되어 있는 경우, IIS 프로세스는 시스템 권한을 가지게 되므로 해커가 IIS 프로세스의 권한을 획득하면 관리자에 준하는 권한을 가질 수 있으므로 주의 해야 함

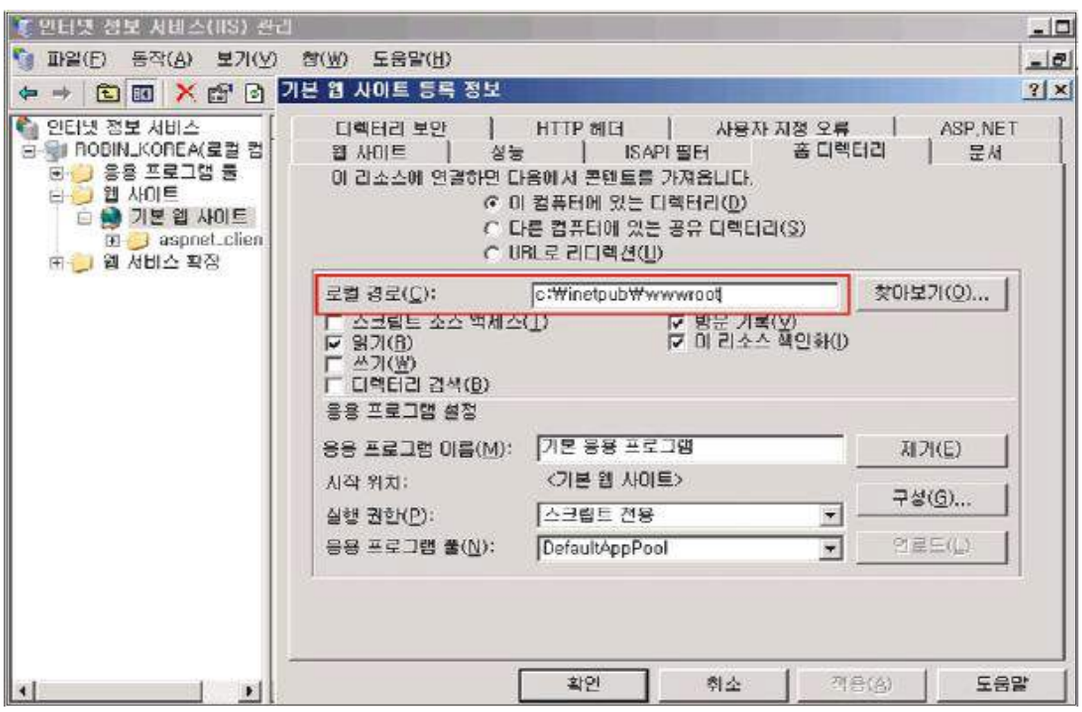


조치 시 영향	일반적인 경우 영향 없음

W-16 (상)	2. 서비스 관리 > 2.10 IIS 링크 사용금지
취약점 개요	
점검내용	■ IIS 링크 사용금지 설정 여부 점검
점검목적	■ 웹 컨텐츠 디렉토리에서 다른 디렉토리나 파일들에 접근할 수 있는 심볼릭 링크, 별칭(aliases), 바로가기 등을 제거하여 허용하지 않은 경로의 접근을 차단하기 위함
보안위협	■ 접근을 허용한 웹 콘텐츠 디렉토리 내에 서버의 다른 디렉토리나 파일들에 접근할 수 있는 심볼릭 링크, aliases, 바로가기 등이 존재하는 경우 해당 링크를 통해 허용하지 않은 다른 디렉토리에 액세스 할 수 있는 위험성 존재
참고	-
점검대상 및 판단기준	
대상	■ Windows 2000, 2003, 2008, 2012
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 디렉토리에 있는 심볼릭 링크, aliases, 바로가기 파일 삭제
점검 및 조치 사례	

■ **Windows 2000(IIS 5.0), 2003(IIS 6.0)**

Step 1) 인터넷 정보 서비스(IIS) 관리> 해당 웹사이트> 속성> [홈 디렉토리] 탭 선택> "로컬 경로"에서 홈 디렉토리 위치 확인



Windows 서버

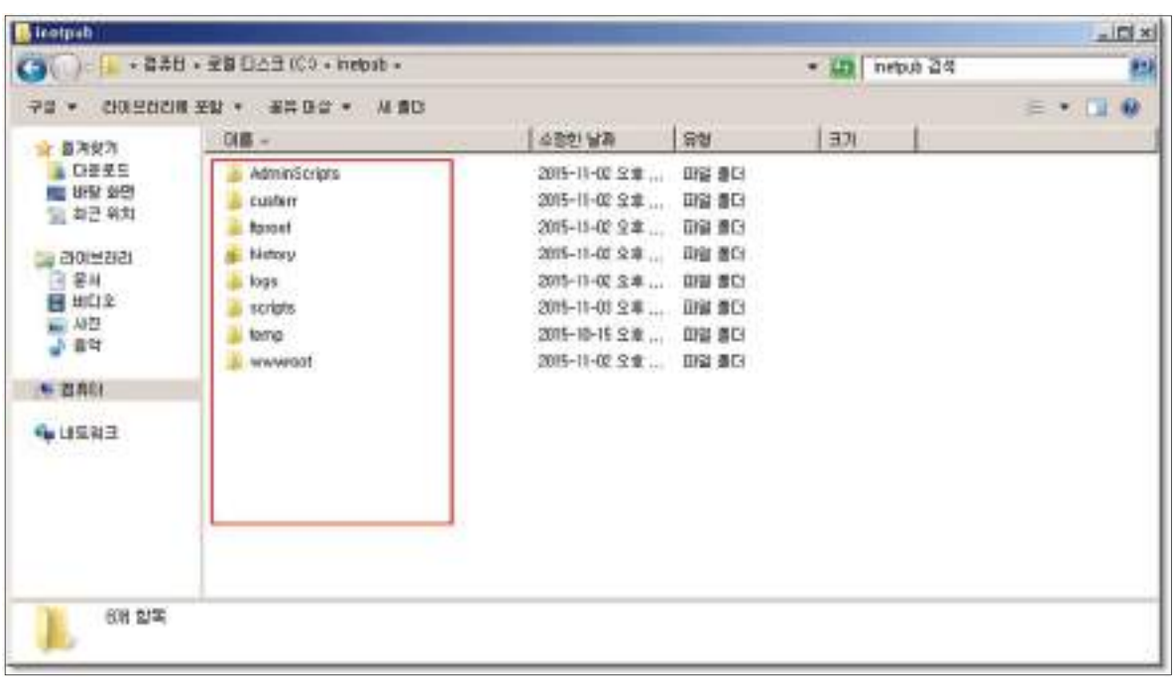
W-16 (상)	2. 서비스 관리 > 2.10 IIS 링크 사용금지

Step 2) 로컬 경로에 입력된 홈 디렉토리로 이동하여 바로가기 파일 삭제

■ **Windows 2008(IIS 7.0), 2012(IIS 8.0)**

Step 1) 제어판> 관리도구> 인터넷 정보 서비스(IIS) 관리자> 해당 웹사이트> 기본 설정> "실제 경로"에서 홈 디렉토리 위치 확인

Step 2) 실제 경로에 입력된 홈 디렉토리로 이동하여 바로가기 파일 삭제



조치 시 영향	일반적인 경우 영향 없음

W-17 (상)	2. 서비스 관리 > 2.11 IIS 파일 업로드 및 다운로드 제한
취약점 개요	
점검내용	■ IIS 파일 업로드 및 다운로드 제한 설정 여부 점검
점검목적	■ 기반시설 시스템은 파일의 업로드 및 다운로드를 원칙적으로 금지하나, 부득이 파일의 업로드 및 다운로드 기능을 활용해야 하는 경우, 파일의 용량 제한을 설정하여 보안성 유지 및 안정적인 웹서버 자원관리를 할 수 있도록 하기 위함
보안위협	■ 대용량 파일 업로드 및 다운로드가 가능한 경우 서버 리소스에 영향을 주어 서비스 장애가 발생할 수 있음
참고	※ IIS에서는 파일의 업로드 및 다운로드 기능을 직접적으로 차단하는 기능이 없어, 웹사이트 내 파일의 업로드 및 다운로드 기능의 구현 여부의 병행 점검이 필요
점검대상 및 판단기준	
대상	■ Windows NT, 2000, 2003, 2008, 2012
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
점검 및 조치 사례	

■ **Windows NT, 2000, 2003**

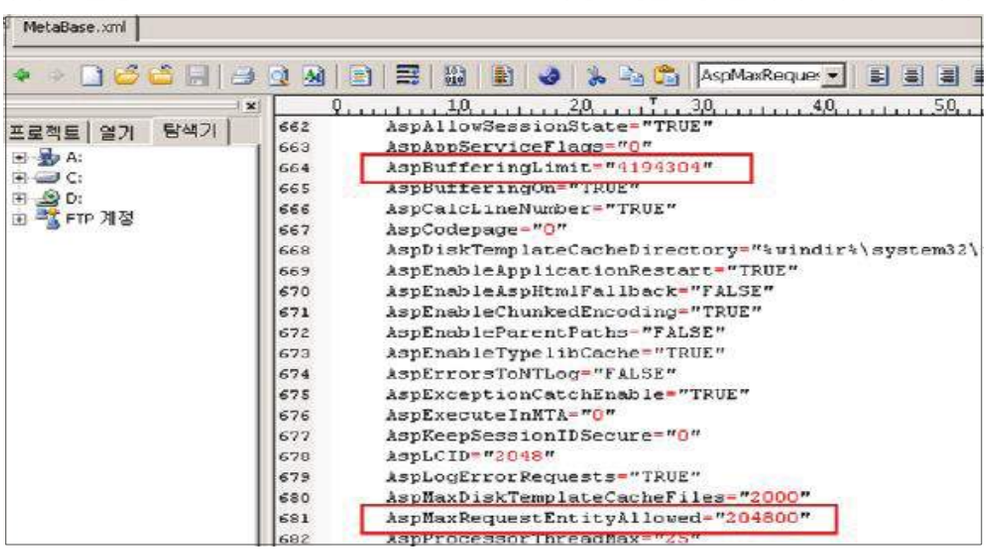
Step 1) 시작> 실행> SERVICES.MSC> IISADMIN> 속성> [일반] 탭에서 서비스 중지

Step 2) %systemroot%₩system32₩inetsrv₩MetaBase.xml 파일을 찾아 편집기로 OPEN

Step 3) AspMaxRequestEntityAllowed 값을 찾아 파일 업로드 용량을 최소 범위로 제한

Step 4) AspBufferingLimit 값을 찾아 파일 다운로드 용량을 최소 범위로 제한

Step 5) 시작> 실행> SERVICES.MSC> IISADMIN> 속성> [일반] 탭에서 서비스 시작



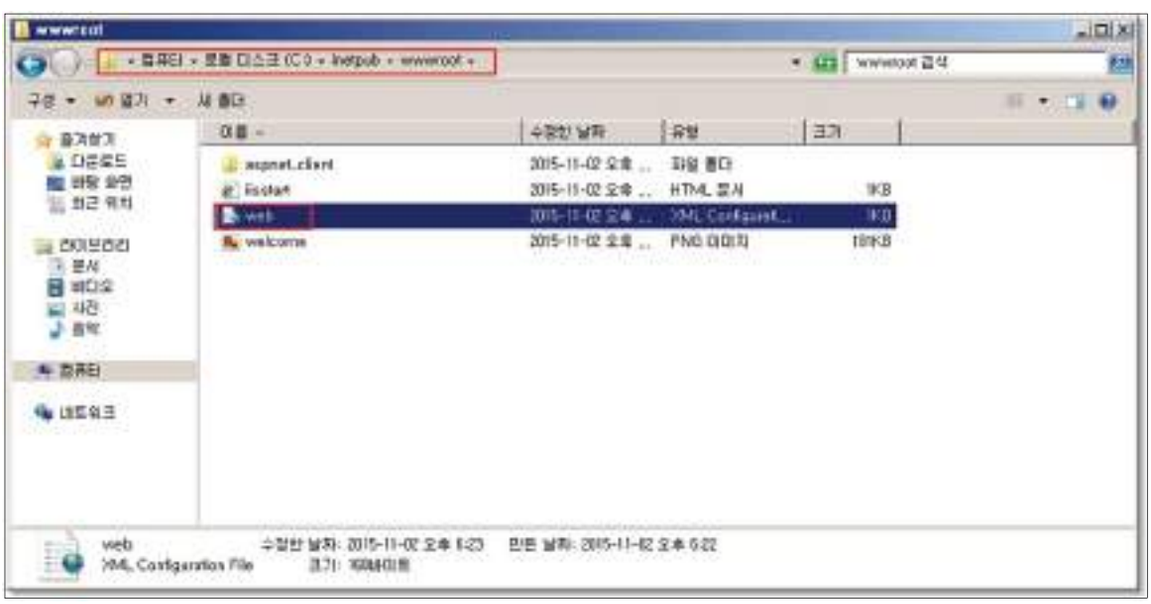
Windows 서버

W-17 (상)	2. 서비스 관리 > 2.11 IIS 파일 업로드 및 다운로드 제한

■ **Windows 2008, 2012**

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

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

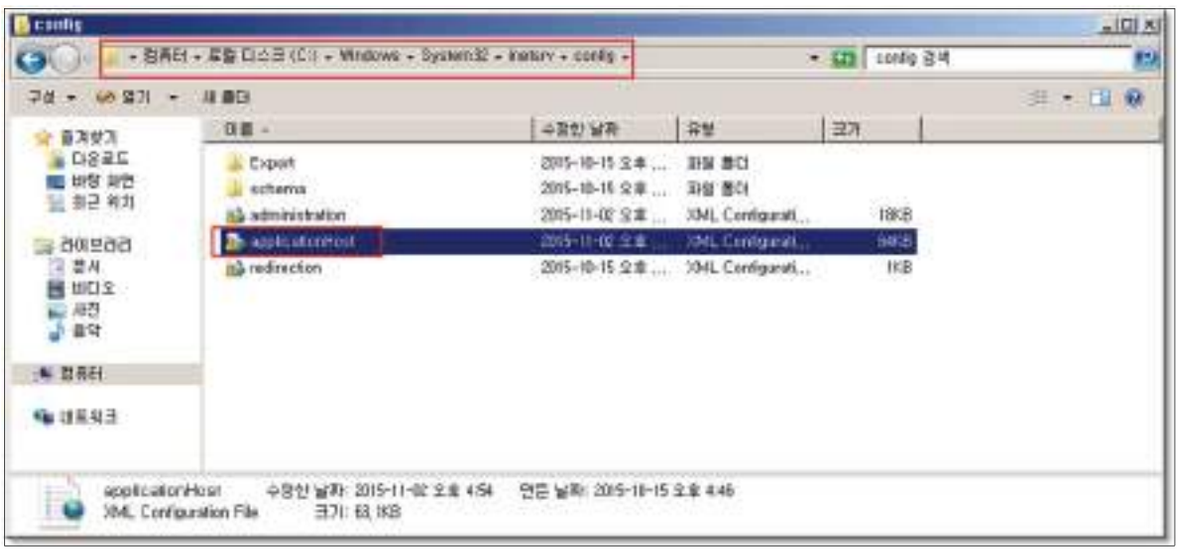


[upload 및 download 용량 제한 - web.config 파일 편집]

Step 2) %systemroot% ₩system32 ₩inetsrv ₩config ₩applicationHost.config 파일 내 아래 항목 추가

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

W-17 (상)	2. 서비스 관리 > 2.11 IIS 파일 업로드 및 다운로드 제한



[upload 및 download 용량 제한 - applicationHost.config 파일 편집]

※ Default 설정 값

(1) maxAllowedContentLength (콘텐츠 용량) => Default: 30MB

(2) MaxRequestEntityAllowed (파일 업로드 용량) => Default: 200000 byte

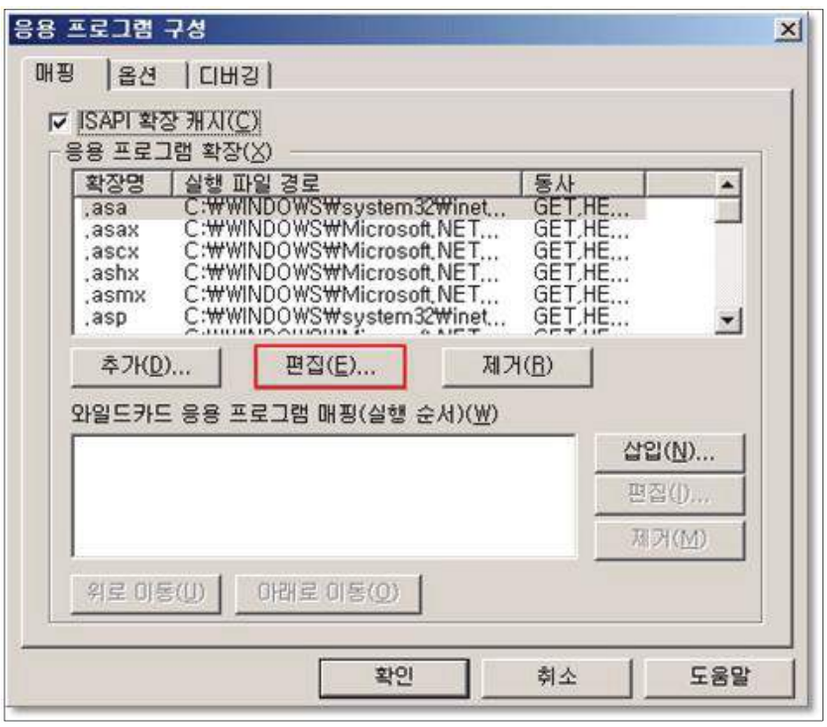
(3) bufferingLimit (파일 다운로드 용량)=> Default: 4MB(4194304 byte)

조치 시 영향	일반적인 경우 영향 없음

Windows 서버

W-18 (상)	2. 서비스 관리 > 2.12 IIS DB 연결 취약점 점검
취약점 개요	
점검내용	■ Global.asa 또는 별도의 DB 컨넥션을 하는 파일에 대한 취약점 점검
점검목적	■ DB 컨넥션 파일(global.asa)에 대한 접근을 제한하여 SQL 서버의 사용자명과 패스워드와 같은 중요 정보의 노출을 차단하기 위함
보안위협	■ 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
참고	※ **global.asa 파일:** 각각의 ASP(Active Server Pages) 프로그램을 위해 IIS 서버상에서 관리되는 파일. IIS 서버는 IIS 프로그램이 시작하고 정지할 때, 혹은 웹 클라이언트가 ASP 프로그램의 웹 페이지들을 액세스하는 브라우저 세션들을 시작하고 정지할 때 자동적으로 global.asa 파일을 처리함
점검대상 및 판단기준	
대상	■ Windows 2000, 2003, 2008, 2012
판단기준	**양호 :** .asa 매핑 시 특정 동작만 가능하도록 제한하여 설정한 경우 또는 매핑이 없을 경우
	취약 : .asa 매핑 시 모든 동작이 가능하도록 설정한 경우
조치방법	사용하지 않는 경우 IIS 서비스 중지, 사용할 경우 .asa 매핑을 아래 그림과 같이 특정 동작만 가능하도록 추가(IIS 6.0) / asa 설정을 false 함(7.0, 8.0)
점검 및 조치 사례	
■ **Windows 2000(IIS 5.0), 2003(IIS 6.0)** Step 1) asa 매핑 등록 확인 인터넷 정보 서비스(IIS) 관리자> 웹 사이트> 해당 웹 사이트> 속성> [홈 디렉토리] 탭에서 구성> [매핑] 탭 선택 후 .asa 매핑이 등록되어 있는지 확인	

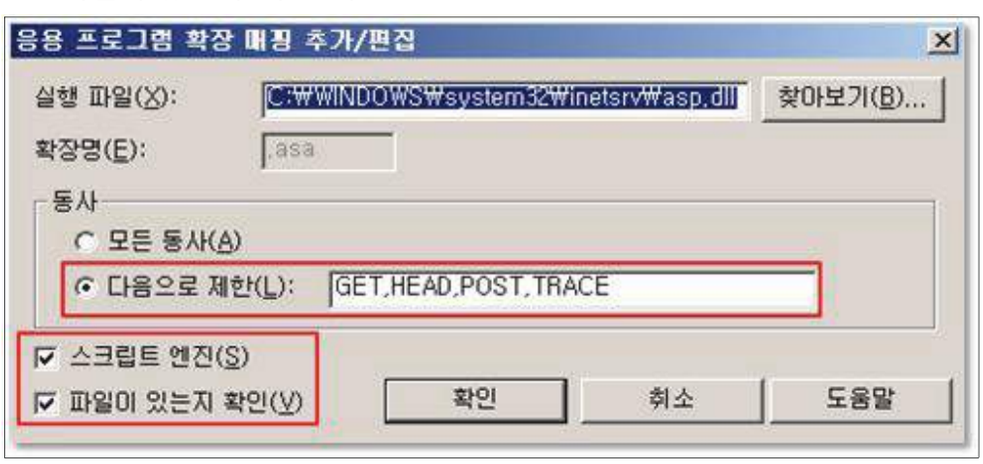
W-18 (상)	2. 서비스 관리 > 2.12 IIS DB 연결 취약점 점검



Step 2) asa 매핑 등록되어 있다면 특정 동작만 가능하도록 설정되어 있는지 확인

[매핑] 탭에서 [편집] 내용이 다음과 동일하게 설정되어 있는지 확인

- 동사> 다음으로 제한> GET, HEAD, POST, TRACE 입력
- 스크립트 엔진 체크
- 파일이 있는지 확인 체크



■ **Windows 2008(IIS 7.0), 2012(IIS 8.0)**

총 2가지 항목에서 확인 필요

2가지 항목이 모두 아래의 방법과 같이 설정되어 있을 경우 취약하다고 볼 수 있으며, 한 가지 경우라도 설정이 되어 있지 않거나 해당 설정이 없을 시 양호하다고 판단함

Windows 서버

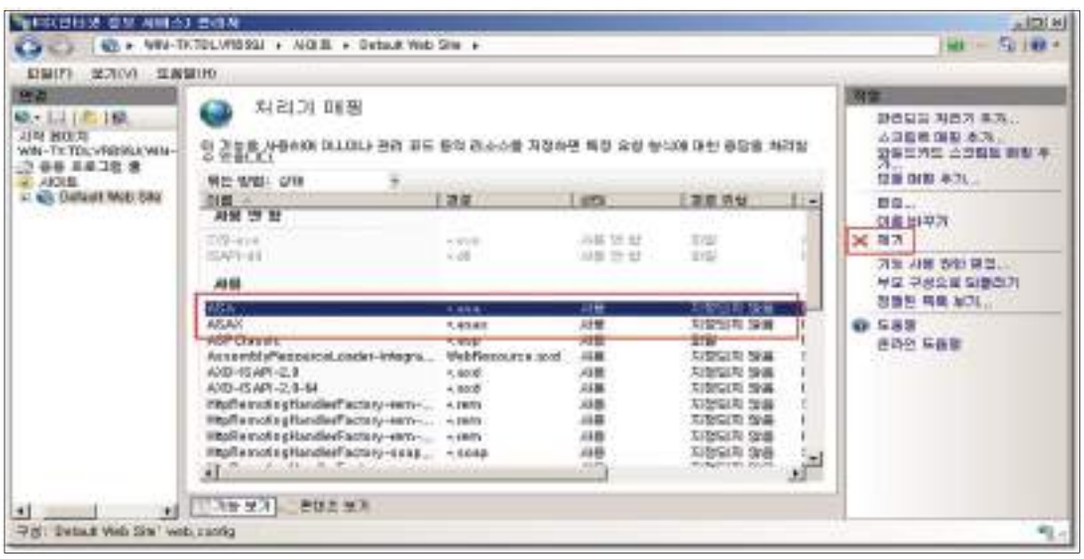
W-18 (상)	2. 서비스 관리 > 2.12 IIS DB 연결 취약점 점검

1. asa / asax 스크립트 매핑 확인

Step 1) 매핑이 없을 경우 양호

인터넷 정보 서비스(IIS) 관리자> 해당 웹 사이트> IIS> "처리기 매핑" 선택, 사용 항목에 *.asa / *.asax 등록되지 않을 경우 양호

※ 아래 이미지처럼 등록되어 있을 경우 삭제 시 양호

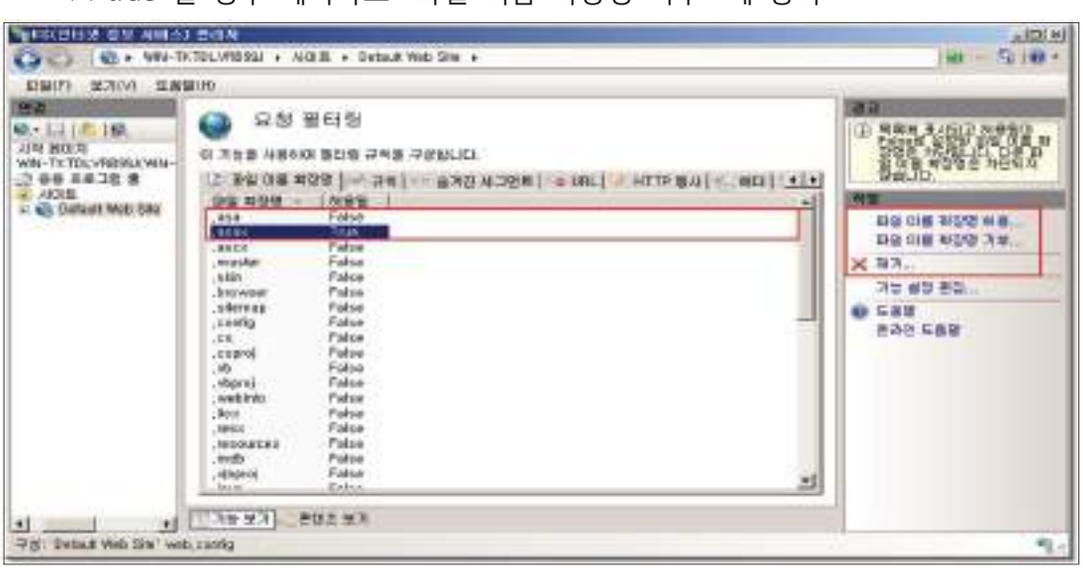


2. asa / asax 파일 필터링 확인

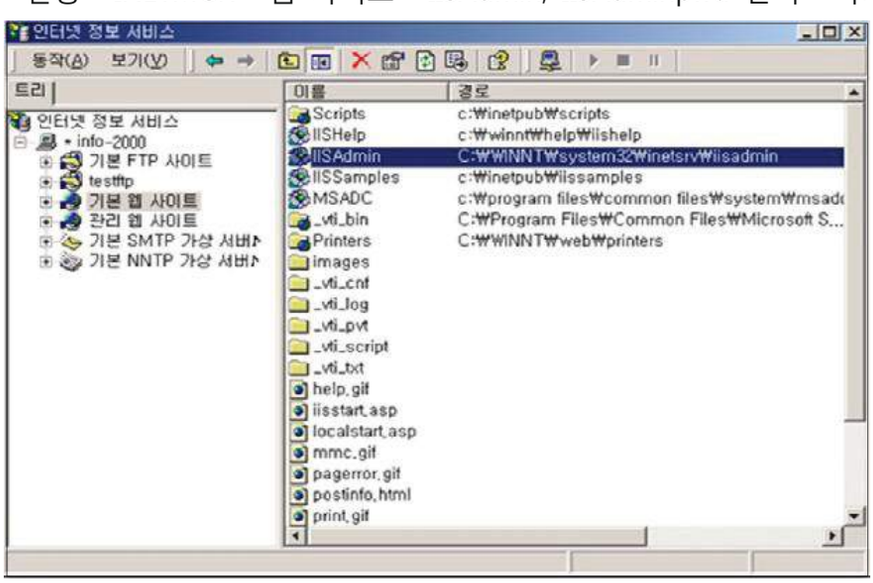
Step 1) false 일 경우 양호

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

※ true 일 경우 제거하고 "파일 이름 확장명 거부" 에 등록



조치 시 영향	일반적인 경우 영향 없음

W-19 (상)	2. 서비스 관리 > 2.13 IIS 가상 디렉토리 삭제
취약점 개요	
점검내용	■ 불필요한 IIS 가상 디렉토리 삭제 여부 점검
점검목적	■ IIS 를 설치 시 가상 디렉토리 내에 제공되는 취약한 샘플 어플리케이션을 제거하여 잠재적인 위험을 제거하기 위함
보안위협	■ 기본 가상 디렉토리가 삭제되지 않은 경우 ADSI 스크립트를 이용한 기본 웹 사이트 설정을 변경 및 MSADC 가상 디렉토리를 통한 서버 자원 접근이 가능하여 악의적인 공격의 대상이 될 수 있음
참고	※ /issadmpwd 파일을 제거하고 이 외 존재하는 가상 디렉토리 취약점을 줄이기 위해서 IIS Admin에 관계되는 모든 파일 및 디렉토리를 삭제하여야 함 ※ IIS 4.0, 5.0 설치 시 기본적으로 /issadmpwd라는 가상 디렉토리를 생성하는데, 이 디렉토리에는 웹 서버를 통하여 패스워드를 변경시켜주는 기능 등을 하는 .HTR 파일이 존재함
점검대상 및 판단기준	
대상	■ Windows NT, 2000, 2003, 2008, 2012
판단기준	**양호 :** 해당 웹 사이트에 IIS Admin, IIS Adminpwd 가상 디렉토리가 존재하지 않는 경우
	취약 : 해당 웹 사이트에 IIS Admin, IIS Adminpwd 가상 디렉토리가 존재하는 경우 ※ 조치 시 마스터 속성과 모든 사이트에 적용함
조치방법	사용하지 않는 경우 IIS 서비스 중지, 사용할 경우 IIS Admin, IIS Adminpwd 삭제
점검 및 조치 사례	
■ **Windows 2000(IIS 5.0)** Step 1) 시작> 실행> INETMGR> 웹 사이트> IISAdmin, IISAdminpwd 선택> 삭제  ※ Windows 2003(6.0) 이상 버전 해당 사항 없음	
조치 시 영향	일반적으로 IIS 관리용 페이지를 사용하지 않으므로 영향 없음

Windows 서버

W-20 (상)	2. 서비스 관리 > 2.14 IIS 데이터 파일 ACL 적용
취약점 개요	
점검내용	■ IIS 데이터 파일 ACL 적용 여부 점검
점검목적	■ 웹 데이터 파일에 ACL을 부여함으로써 권한 없는 사용자로부터의 실행 및 읽기를 방지하고자 함
보안위협	■ 웹 데이터 파일에 ACL을 부여되지 않은 경우 권한 없는 사용자로부터의 읽기 및 실행이 가능
참고	※ 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 저장 2. 홈 디렉토리(기본: c:₩inetpub₩wwwroot)내에 적절한 ACL 권한 부여. ※ ACL(Access Control List): 접근이 허가된 주체들과 허가받은 접근 종류들이 기록된 목록
점검대상 및 판단기준	
대상	■ Windows 2000, 2003, 2008, 2012
판단기준	**양호 :** 홈 디렉토리 내에 있는 하위 파일들에 대해 Everyone 권한이 존재하지 않는 경우(정적 콘텐츠 파일은 Read 권한만)
	취약 : 홈 디렉토리 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 디렉토리에 Administrators, System 권한만 설정 후, 하위 디렉토리에 존재하는 모든 Everyone 권한 제거(정적 콘텐츠 파일에 경우 Read 권한 허용)
점검 및 조치 사례	

■ **Windows 2000(IIS 5.0), 2003(IIS 6.0)**

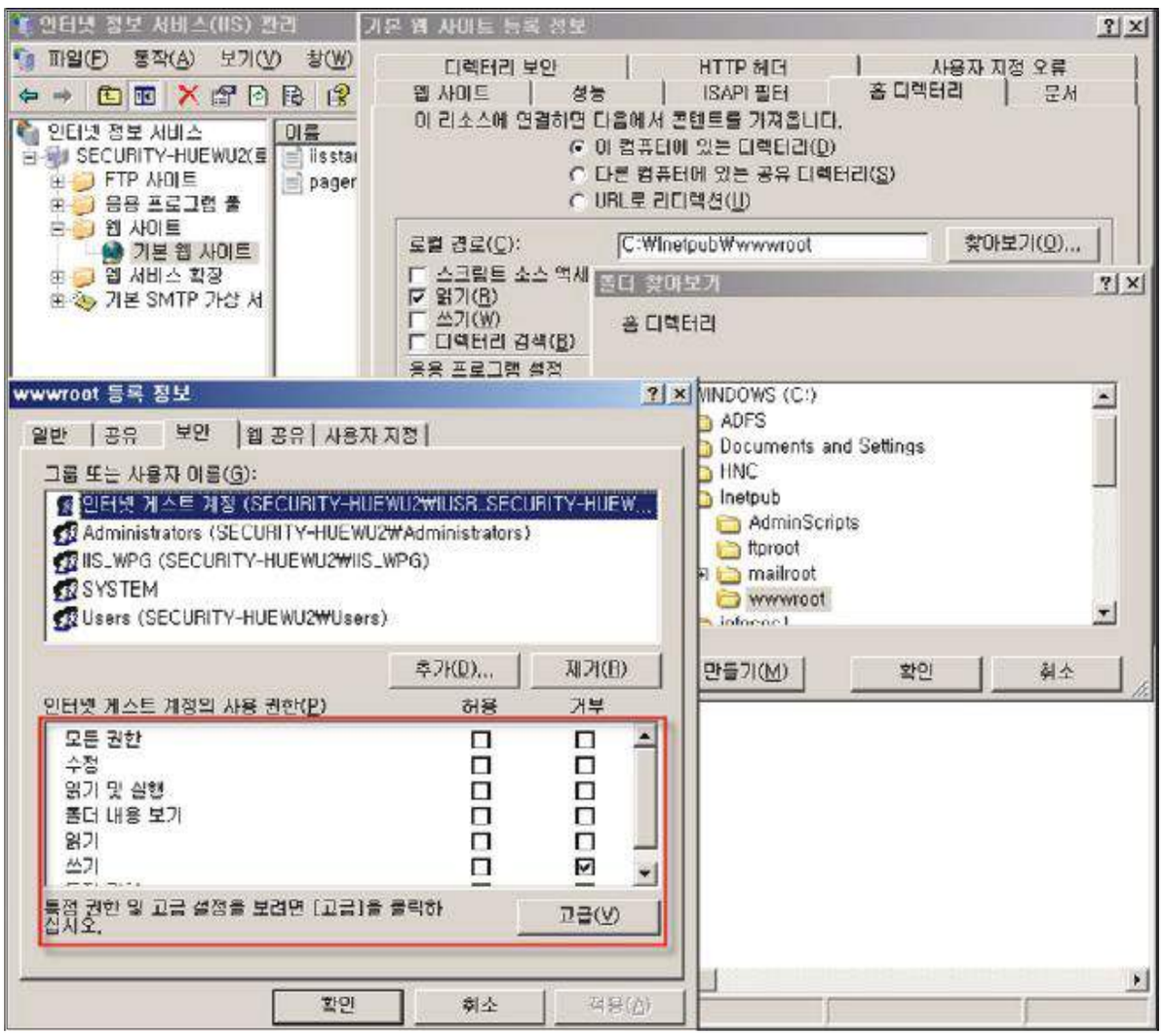
Step 1) 시작> 실행> INETMGR> 웹 사이트> 해당 웹사이트> 속성> 홈 디렉토리 경로 확인

Step 2) 탐색기를 이용하여 홈 디렉토리의 등록정보> [보안] 탭에서 Everyone 권한 확인

Step 3) 아래와 같은 파일들에 대한 불필요한 Everyone 권한 제거

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)

W-20 (상)	2. 서비스 관리 > 2.14 IIS 데이터 파일 ACL 적용



■ Windows 2008(IIS 7.0), 2012(IIS 8.0)

Step 1) 시작> 실행> INETMGR> 사이트> 해당 웹사이트> 기본 설정> 홈 디렉토리 실제 경로 확인

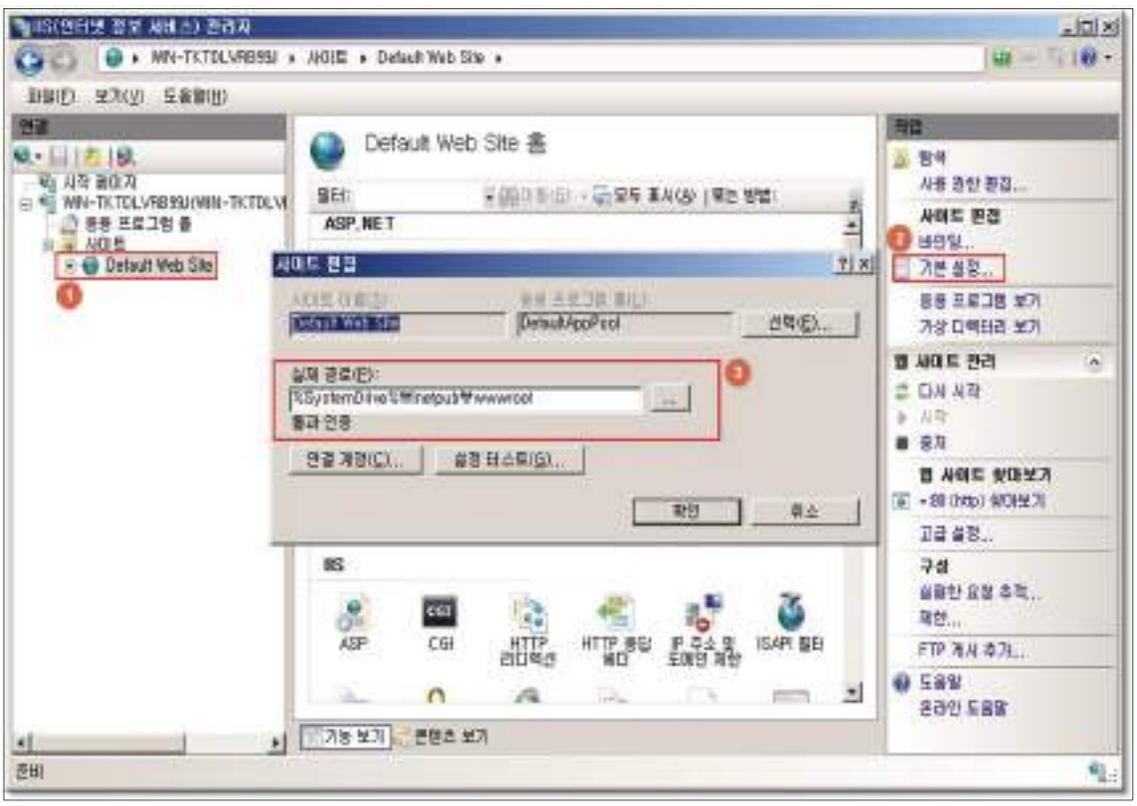
Step 2) 탐색기를 이용하여 홈 디렉토리의 등록 정보> [보안] 탭에서 Everyone권한 확인

Step 3) 아래와 같은 파일들에 대한 불필요한 Everyone 권한 제거

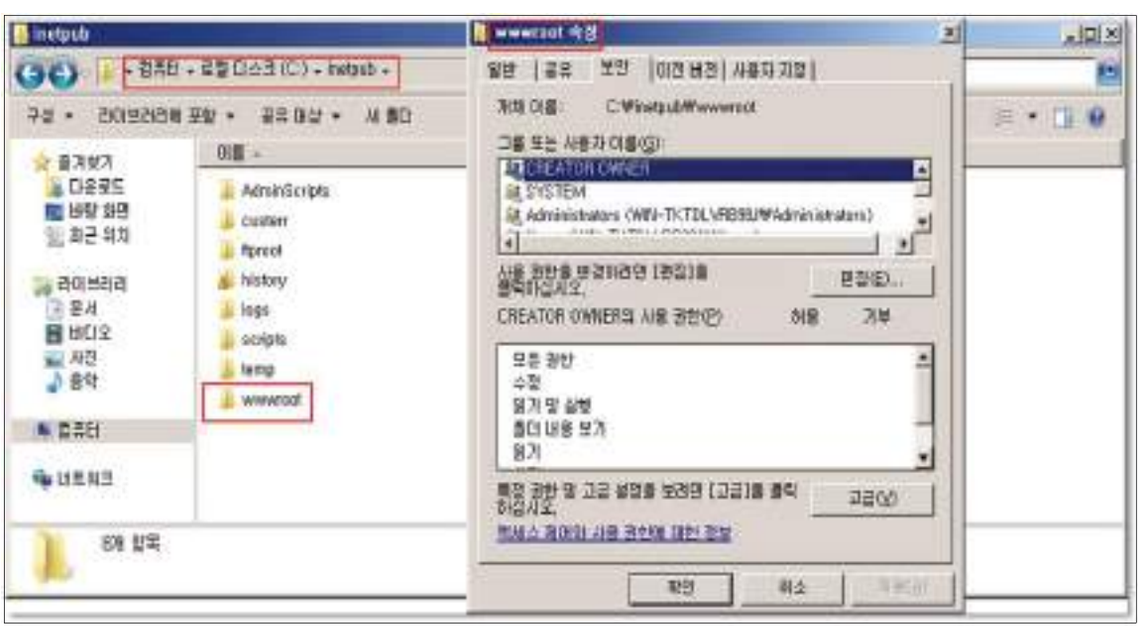
파일 형식	액세스 제어 목록
CGI (.exe, .dll, .cmd, .pl)	모든 사람(X), 관리자/시스템(전체 제어)
스크립트 파일(.asp)	모든 사람(X), 관리자/시스템(전체 제어)

Windows 서버

W-20 (상)	2. 서비스 관리 > 2.14 IIS 데이터 파일 ACL 적용



[웹사이트 실제 경로 확인]



[웹사이트 홈디렉토리 내 everyone 권한 확인]

조치 시 영향	IIS에서 홈 디렉토리 내에 있는 데이터 파일 권한 조치에 따른 검증 필요

W-21 (상)	2. 서비스 관리 > 2.15 IIS 미사용 스크립트 매핑 제거
취약점 개요	
점검내용	■ IIS 미사용 스크립트 매핑 제거 여부 점검
점검목적	■ 사용하지 않은 확장자 매핑을 제거하여 추가 공격의 위험을 제거하기 위함
보안위협	■ 미사용 확장자 매핑을 제거하지 않은 .htr .idc .stm .shtm .shtml .printer .htw .ida .idq 확장자는 버퍼 오버플로우(Buffer Overflow) 공격 위험이 존재함
참고	※ 사용하지 않는 스크립트 매핑은 보안에 위협이 될 수 있으므로 개발자와 협의하여 불필요한 매핑인지 확인한 후 제거해야 함 ※ .asp나 .shtm 과 같은 확장자들은 특정 DLL 파일과 매핑 되어 있어, 이러한 파일들에 대한 요청이 들어오면 해당 DLL에 의해 처리됨 ※ **스크립트 매핑:** IIS는 클라이언트가 요청한 자원의 파일 확장자에 따라서 이를 처리할 ISAPI 확장 핸들러를 지정하게 되어 있는데 이를 스크립트 매핑이라고 함 ※ **버퍼 오버플로우(Buffer Overflow):** 메모리에 할당된 버퍼의 양을 초과하는 데이터를 입력하여 프로그램의 복귀 주소를 조작, 궁극적으로 해커가 원하는 코드를 실행하는 것
점검대상 및 판단기준	
대상	■ Windows 2000, 2003, 2008, 2012
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)
점검 및 조치 사례	

■ **Windows 2000(IIS 5.0), 2003(IIS 6.0)**

Step 1) 시작> 실행> INETMGR> 웹 사이트> 해당 웹 사이트> 속성> [홈 디렉토리] 탭에서 [구성] 버튼 선택

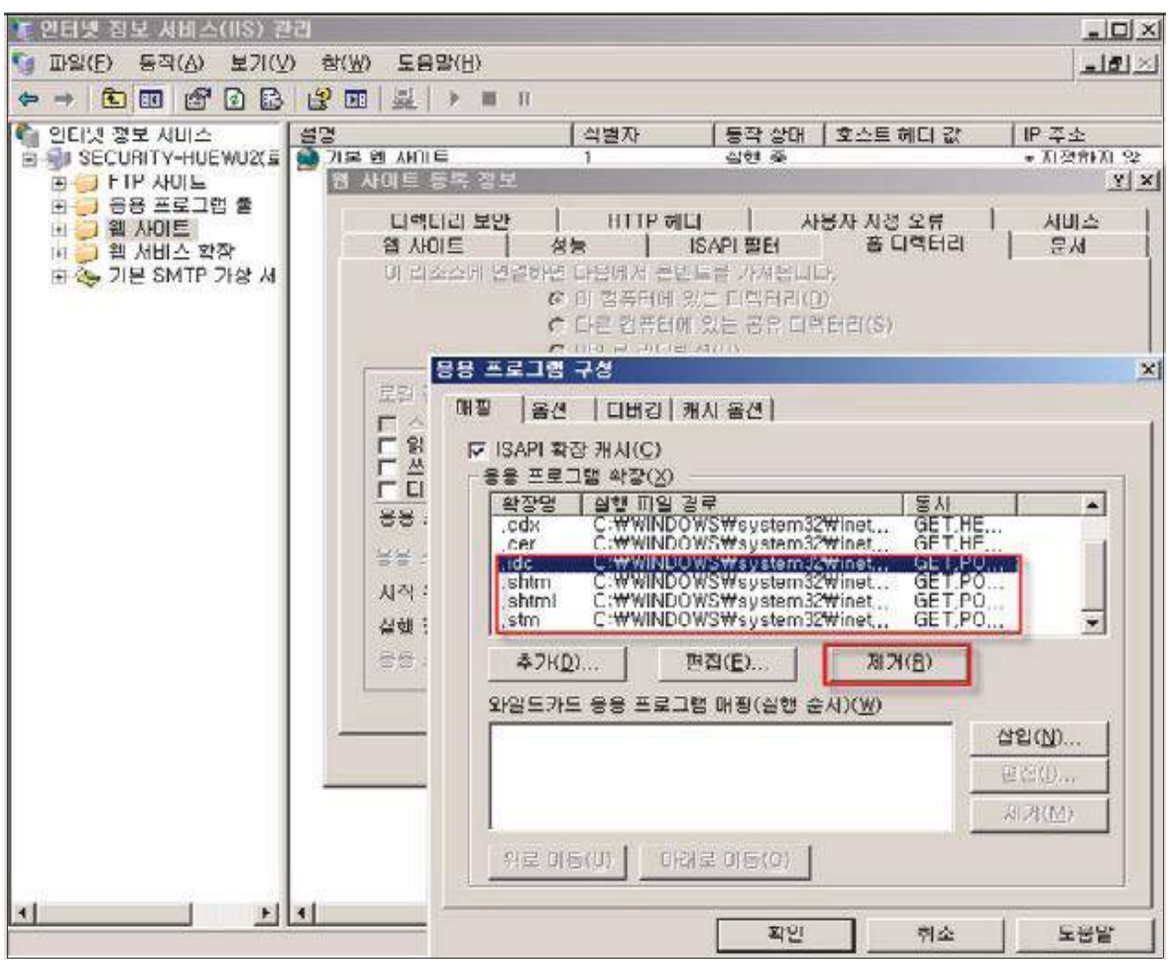
Step 2) [매핑] 탭에서 아래와 같은 취약한 매핑 제거

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

Windows 서버

W-21 (상)	2. 서비스 관리 > 2.15 IIS 미사용 스크립트 매핑 제거

idc	Internet Database Connector: SQL 서버에 연결하기 위한 정보 등을 관리함. asp를 통해 같은 작업을 수행 가능	Web 디렉토리 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

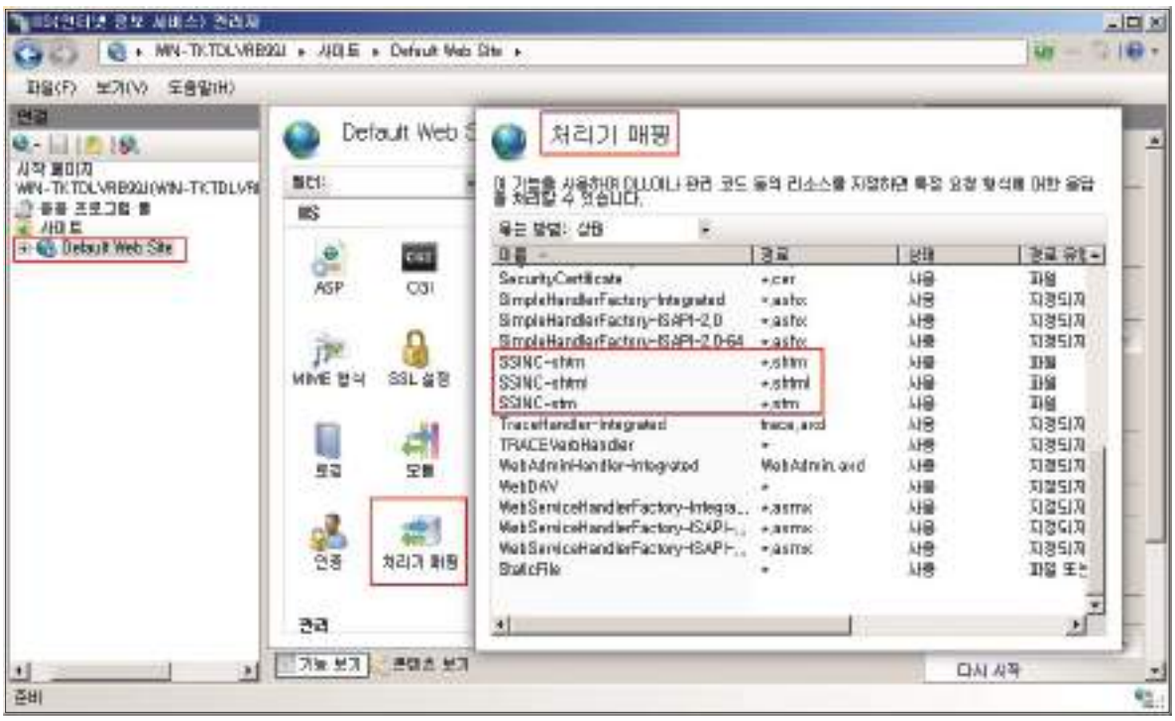


W-21 (상)	2. 서비스 관리 > 2.15 IIS 미사용 스크립트 매핑 제거

■ **Windows 2008(IIS 7.0), 2012(IIS 8.0)**

Step 1) 시작> 실행> INETMGR> 웹 사이트> 해당 웹 사이트> 처리기 매핑 선택

Step 2) 취약한 매핑 제거(.htr, .idc, .stm, .shtm, .shtml, .printer, .htw, .ida, .idq)



조치 시 영향	일반적인 경우 영향 없음

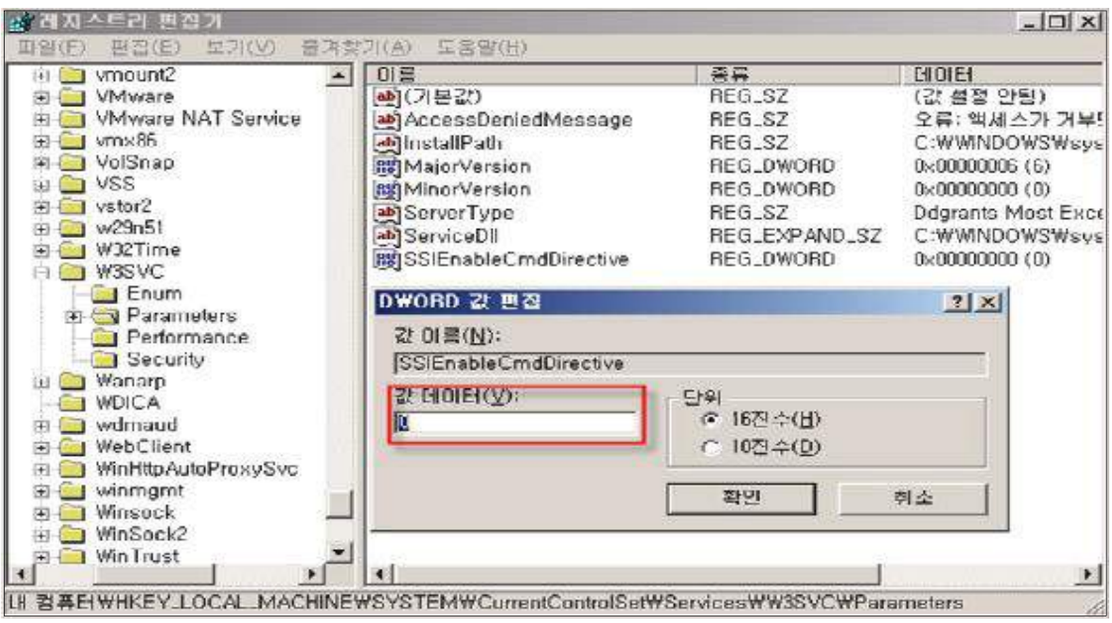
Windows 서버

W-22 (상)	2. 서비스 관리 > 2.16 IIS Exec 명령어 쉘 호출 진단
취약점 개요	
점검내용	■ IIS Exec 명령어 쉘 호출 여부 진단
점검목적	■ 웹 서버에서 임의 명령어 호출을 제한하여 허가되지 않은 명령어 실행을 차단하기 위함
보안위협	■ 웹 서버에서 # exec 명령어를 통한 명령어 실행이 차단되지 않은 경우, 웹 서버에서 임의의 시스템 명령이 호출 가능하여 허가되지 않은 파일의 실행 위험 존재
참고	-
점검대상 및 판단기준	
대상	■ Windows NT, 2000
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
점검 및 조치 사례	

■ **Windows NT(IIS 4.0), 2000(IIS 5.0)**

Step 1) 시작> 실행> REGEDIT> HKLM₩SYSTEM₩CurrentControlSet₩Services₩W3SVC ₩Parameters 검색

Step 2) DWORD> SSIEnableCmdDirective 값을 찾아 값을 "0"으로 입력



※ IIS 6.0 이상 버전(windows 2003 이상) 해당 사항 없음

조치 시 영향	일반적인 경우 영향 없음

W-23 (상)	2. 서비스 관리 > 2.17 IIS WebDAV 비활성화
취약점 개요	
점검내용	■ IIS WebDAV 비활성화 여부 점검
점검목적	■ WebDAV 서비스를 비활성화 하여, IIS WebDAV에서 발견되는 다수의 인증 우회 취약점을 제거하고자 함
보안위협	■ WebDAV가 활성화 되어 있는 경우 IIS에 악의적으로 작성된 HTTP 요청을 이용하여 인증을 우회함으로써 패스워드로 보호된 WebDAV의 자원에 접근(디렉토리 열람, 파일 다운로드 등)이 가능 ■ WebDAV에 의해 호출된 일부 구성 요소에 매개 변수를 정확하게 점검하지 않는 결함이 존재하여, 이로 인해 버퍼 오버런이 발생 가능
참고	※ **WebDAV(Web Distributed Authoring and Versioning):** 사용자가 원격 World Wide Web 서버를 이용하여 파일을 수정하거나 처리할 수 있도록 하는 HTTP의 확장 서비스. 웹상의 공동개발을 지원하기 위한 IETF 표준안(RFC 2518)으로써, 원격지 사용자들 간에 인터넷상에서 파일을 공동 편집하고 관리할 수 있도록 함
점검대상 및 판단기준	
대상	■ Windows NT, 2000, 2003, 2008, 2012
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, 2008 WebDAV금지 시 양호)
점검 및 조치 사례	
■ Windows NT, 2000 Step 1) 시작> 실행> SERVICES.MSC> World Wide Web Publishing Service> 속성 Step 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)	

Windows 서버

W-23 (상)	2. 서비스 관리 > 2.17 IIS WebDAV 비활성화

<IIS를 사용하고, WebDAV도 필요한 경우 >

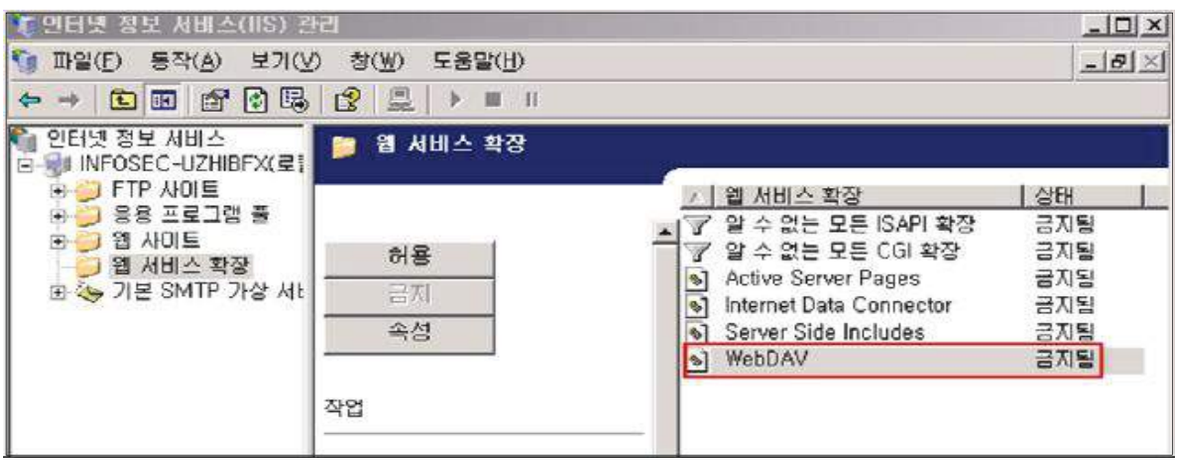
1. Windows NT 인 경우 windows update 실행
2. Windows 2000 서비스팩 버전이 2, 3인 경우 windows update 실행
3. Windows 2000 서비스팩 버전이 4인 경우 - 취약점 없음

※ 시스템 재시작 후 적용됨

■ Windows 2003

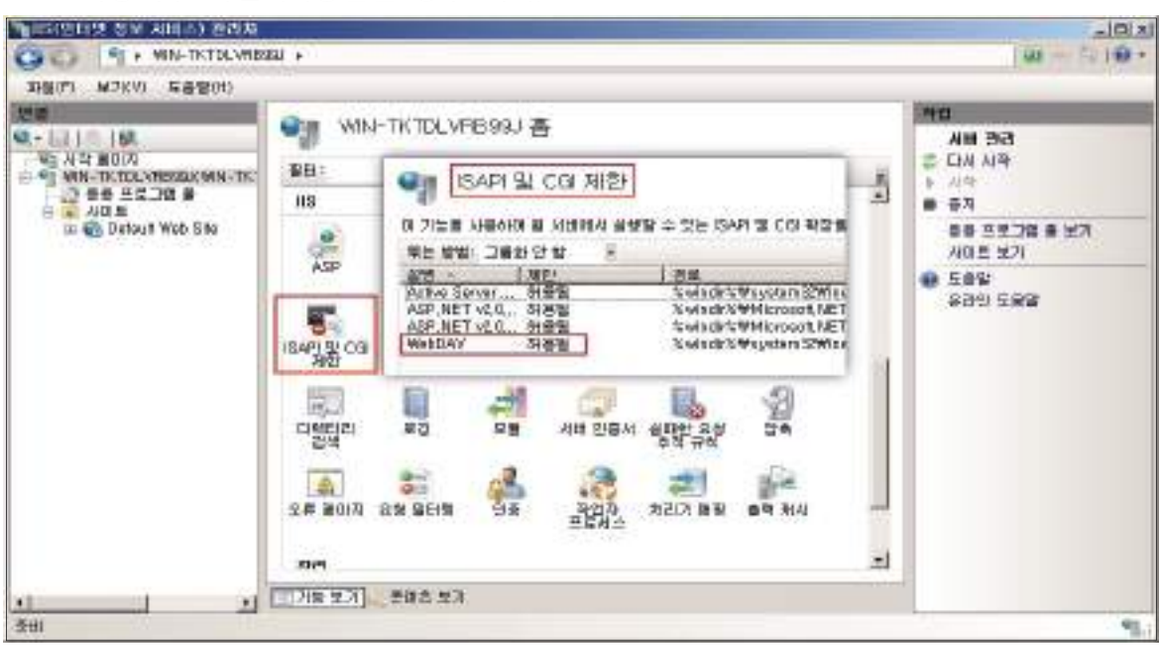
Step 1) 시작> 실행> INETMGR> 웹 사이트> 웹 서비스 확장

Step 2) WebDAV 금지



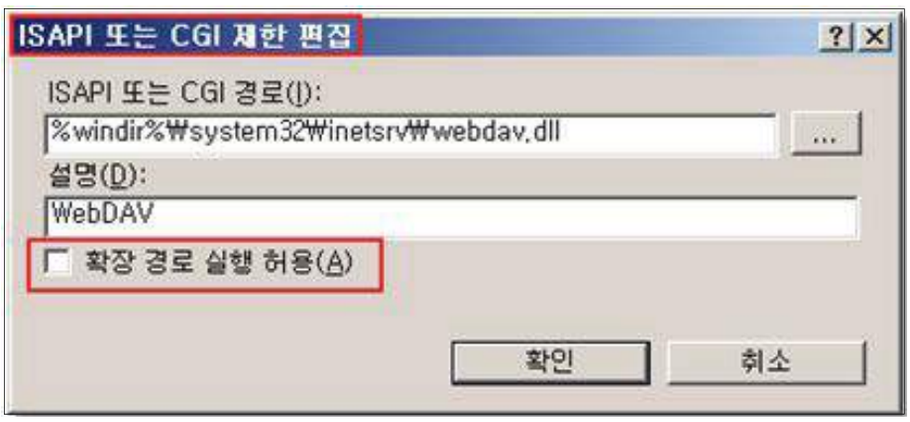
■ Windows 2008, 2012

Step 1) 인터넷 정보 서비스(IIS) 관리자> 서버 선택> IIS> "ISAPI 및 CGI 제한" 선택, WebDAV 사용여부 확인 (허용됨일 경우 취약)



W-23 (상)	2. 서비스 관리 > 2.17 IIS WebDAV 비활성화

Step 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



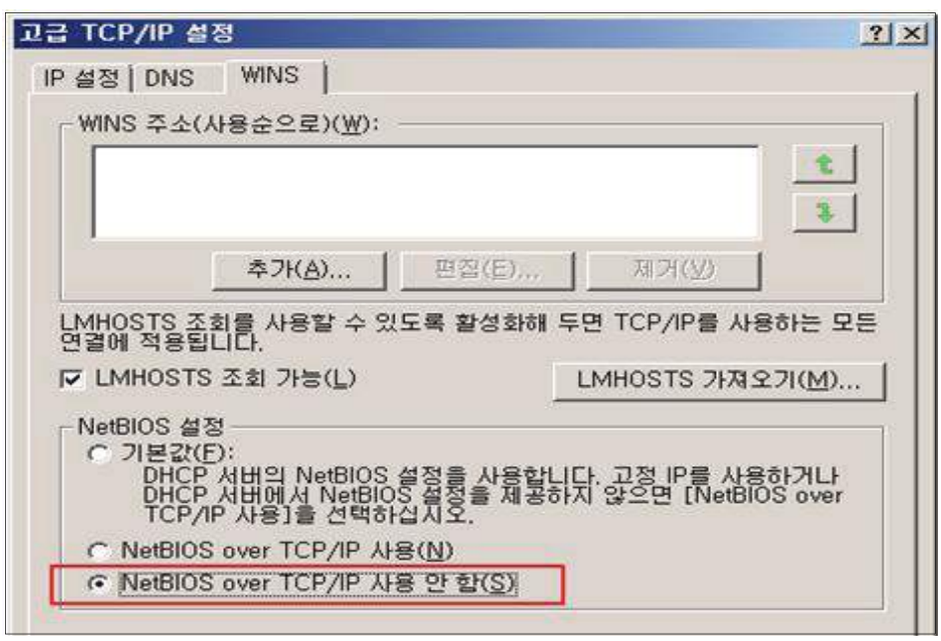
조치 시 영향	일반적인 경우 영향 없음

Windows 서버

W-24 (상)	2. 서비스 관리 > 2.18 NetBIOS 바인딩 서비스 구동 점검
취약점 개요	
점검내용	■ NetBIOS 바인딩 서비스 구동 여부 점검
점검목적	■ NetBIOS와 TCP/IP 바인딩을 제거하여 TCP/IP를 거치게 되는 파일 공유서비스를 제공하지 못하도록 하고, 인터넷에서의 공유자원에 대한 접근 시도를 방지하고자 함
보안위협	■ 인터넷에 직접 연결되어 있는 윈도우 시스템에서 NetBIOS TCP/IP 바인딩이 활성화 되어 있을 경우 공격자가 네트워크 공유자원을 사용할 우려 존재
참고	※ **NetBIOS(Network Basic Input/Output System)**는 별개의 컴퓨터상에 있는 애플리케이션들이 근거리통신망 내에서 서로 통신 할 수 있게 해주는 프로그램. IBM pc를 위한 네트워크 인터페이스 체계로 네임, 세션, 데이터그램의 세가지 서비스를 제공하며 NetBIOS를 통해 파일 공유와 프린터 공유 등을 서비스로 이용
점검대상 및 판단기준	
대상	■ Windows NT, 2000, 2003, 2008, 2012
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
점검 및 조치 사례	

■ **Windows NT, 2000, 2003, 2008, 2012**

Step 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

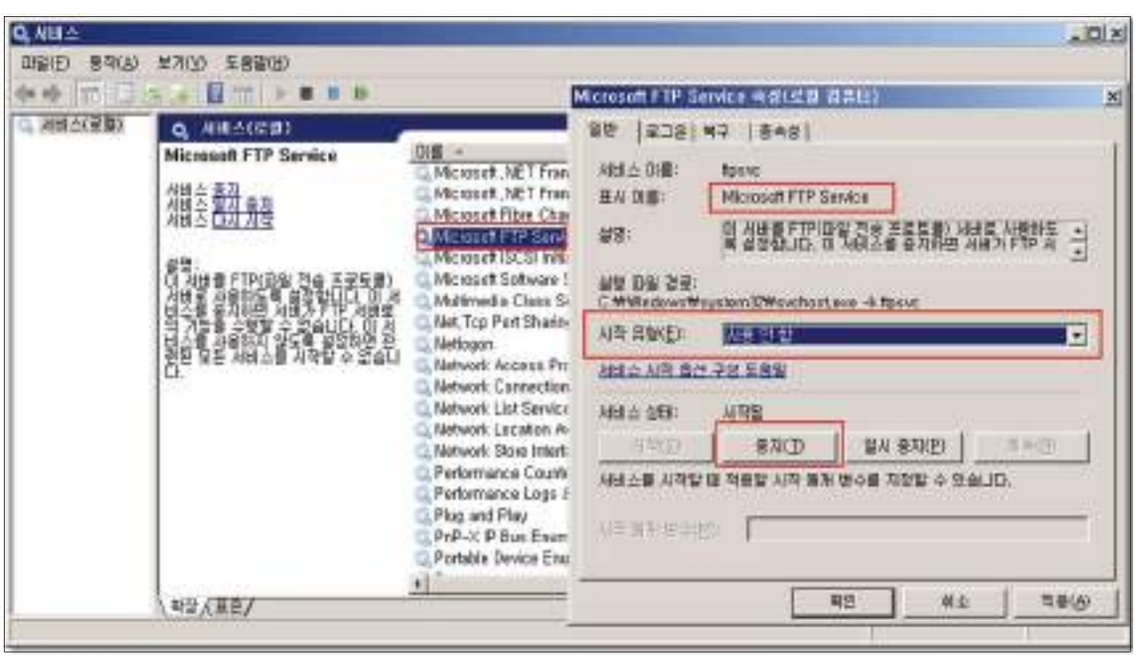


조치 시 영향	TCP/IP을 거치게 되는 파일 공유 서비스가 제공되지 않음 인터넷에서의 공유 자원에 대한 접근시도가 불가능함 (라우터를 거치지 않은 내부 네트워크에서는 가능함)

W-25 (상)	2. 서비스 관리 > 2.19 FTP 서비스 구동 점검
취약점 개요	
점검내용	■ 시스템 내 FTP 서비스 구동 여부 점검
점검목적	■ 인증 정보가 기본적으로 평문전송 되는 취약한 프로토콜인 FTP의 사용을 제한하여 네트워크 보안성을 높이고자 함
보안위협	■ OS에서 제공하는 기본적인 FTP 서비스를 사용할 경우 계정과 패스워드가 암호화 되지 않은 채로 전송 되어 Sniffer에 의한 계정 정보의 노출 위험 존재
참고	※ **Sniffer:** 네트워크 트래픽을 감시하고 분석하는 프로그램
점검대상 및 판단기준	
대상	■ Windows NT, 2000, 2003, 2008, 2012
판단기준	**양호 :** FTP 서비스를 사용하지 않는 경우 또는 secure FTP 서비스를 사용하는 경우
	취약 : FTP 서비스를 사용하는 경우
조치방법	FTP 서비스가 필요하지 않다면 서비스 중지 또는 secure FTP 응용프로그램 사용
점검 및 조치 사례	

■ **Windows NT, 2000, 2003, 2008, 2012**

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



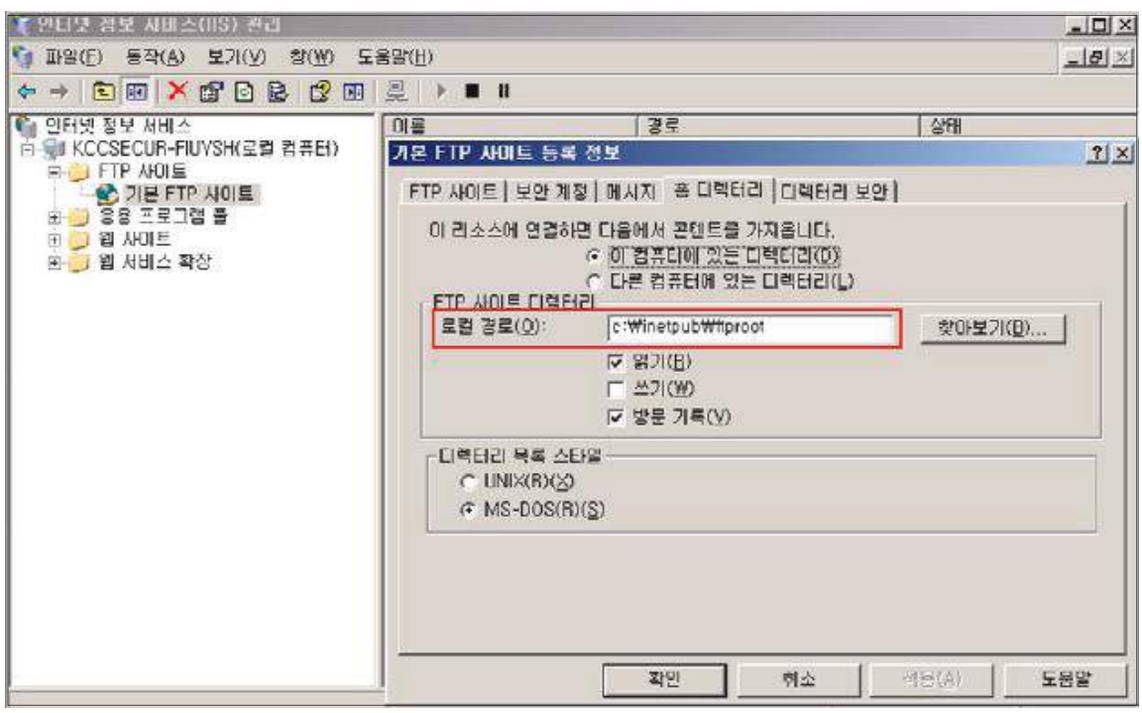
조치 시 영향	일반적인 경우 영향 없음

Windows 서버

W-26 (상)	2. 서비스 관리 > 2.20 FTP 디렉토리 접근권한 설정
취약점 개요	
점검내용	■ FTP 홈디렉토리의 접근 권한 적절성 점검
점검목적	■ FTP 서비스 디렉토리의 접근 권한을 적절하게 설정하여 의도치 않은 정보유출 등의 보안 사고를 방지하고자 함
보안위협	■ FTP 홈디렉토리에 과도한 권한(예. Everyone Full Control)이 부여된 경우 임의의 사용자가 쓰기, 수정이 가능하여 정보유출, 파일 위·변조 등의 위험 존재
참고	※ 기반시설 시스템은 FTP 서비스를 사용하지 않는 것이 원칙이나, 조직 내에서 해당 서비스를 부득이 사용해야 하는 경우 관련 보호 대책을 수립 및 적용하여 활용하여야 함 ※ 관련 점검 항목 : W-27(상), W-28(상)
점검대상 및 판단기준	
대상	■ Windows NT, 2000, 2003, 2008, 2012
판단기준	**양호 :** FTP 홈 디렉토리에 Everyone 권한이 없는 경우
	취약 : FTP 홈 디렉토리에 Everyone 권한이 있는 경우
조치방법	FTP 홈 디렉토리에서 Everyone 권한 삭제, 각 사용자에게 적절한 권한 부여
점검 및 조치 사례	

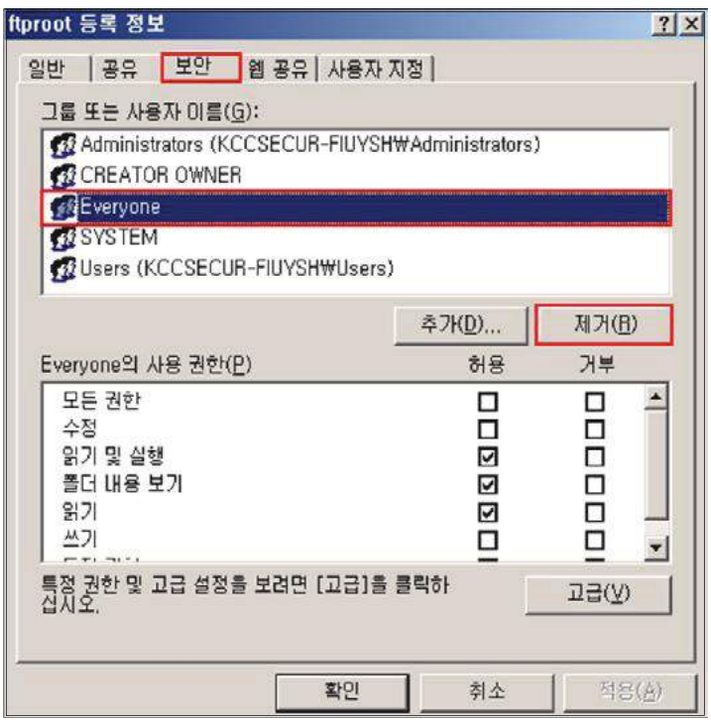
■ **Windows NT(IIS 4.0), 2000(IIS 5.0), 2003(IIS 6.0)**

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



Step 2) 탐색기> 홈 디렉토리> 속성> [보안]탭에서 Everyone 권한 제거

W-26 (상)	2. 서비스 관리 > 2.20 FTP 디렉토리 접근권한 설정



■ Windows 2008(IIS 7.0), 2012(IIS 8.0)

Step 1) 제어판> 관리도구> 인터넷 정보 서비스(IIS) 관리> 해당 웹사이트> 마우스 우클릭> FTP 게시 추가

Step 2) 이후 진행 과정에서 권한 부여 화면의 액세스 허용 대상 선정 시 [지정한 사용자] 만 선택

※ 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)

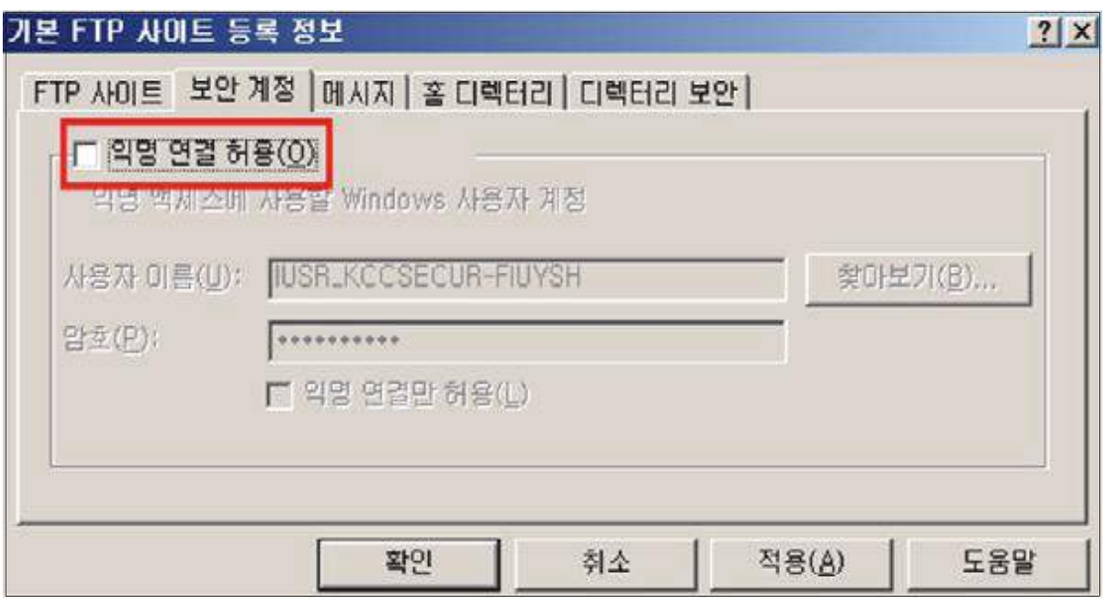
조치 시 영향	일반적인 경우 영향 없음

Windows 서버

W-27 (상)	2. 서비스 관리 > 2.21 Anonymous FTP 금지
취약점 개요	
점검내용	■ FTP 서비스의 Anonymous(익명) 접속 허용 여부 점검
점검목적	■ FTP 익명 접속을 제한하여, 중요 정보의 불법 유출을 차단 하고자 함
보안위협	■ FTP 익명 접속이 허용된 경우 핵심 기밀 자료나 내부 정보의 불법 유출 가능성이 존재함
참고	※ 만약 익명 접속이 허용된 FTP 서버에 익명 사용자에 대해 쓰기 권한이 부여된 경우, 정상적으로 업로드한 파일들의 변조가 가능하므로 공개한 디렉토리 내 중요 데이터가 보관되어 있는지 여부를 추가적으로 확인하여야 함
점검대상 및 판단기준	
대상	■ Windows NT, 2000, 2003, 2008, 2012
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 또는 "익명" 체크 해제
점검 및 조치 사례	

■ **Windows NT(IIS 4.0), 2000(IIS 5.0), 2003(IIS 6.0)**

Step 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)



W-27 (상)	2. 서비스 관리 > 2.21 Anonymous FTP 금지

■ **Windows 2008(IIS 7.0), 2012(IIS 8.0)**

Step 1) 제어판> 관리도구> 인터넷 정보 서비스(IIS) 관리> 해당 웹사이트> 마우스 우클릭> FTP 게시 추가

Step 2) 이후 진행 과정에서 인증 화면의 익명 체크 박스 해제

※ 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)

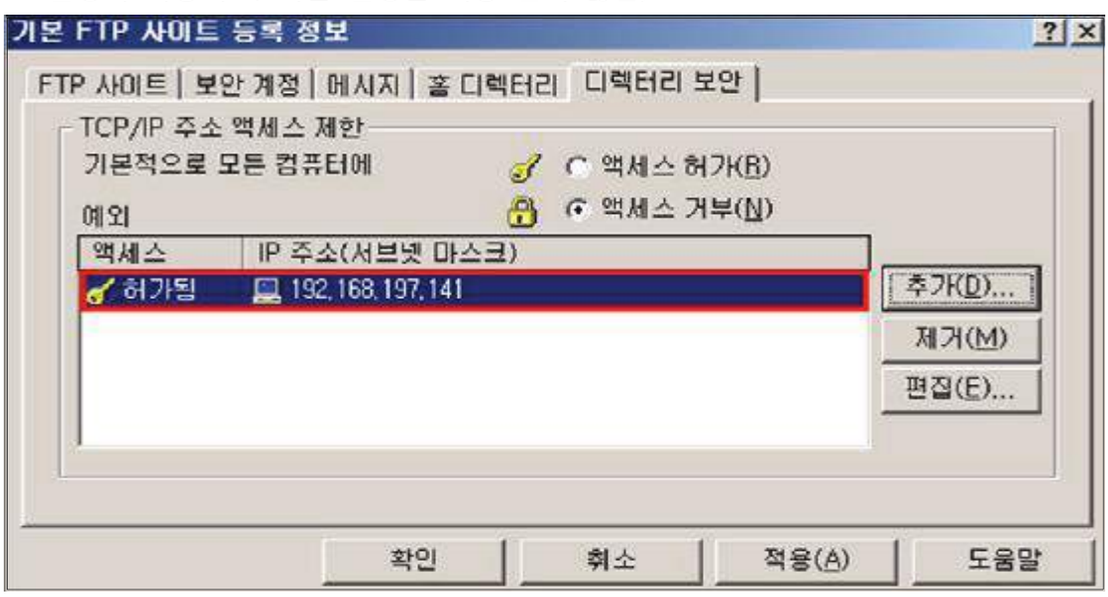
조치 시 영향	애플리케이션에서 익명 연결을 사용할 경우를 제외하고, 일반적으로 영향 없음

Windows 서버

W-28 (상)	2. 서비스 관리 > 2.22 FTP 접근 제어 설정
취약점 개요	
점검내용	■ FTP 접속 가능한 IP 주소 지정 여부 점검
점검목적	■ FTP 접근 시 특정 IP 주소에 대해 콘텐츠 액세스를 허용하여 서비스 보안성을 강화하고자 함
보안위협	■ FTP 프로토콜은 로그온에 지정된 자격 증명이나 데이터 자체가 암호화 되지 않고 모든 자격 증명을 일반 텍스트로 네트워크를 통해 전송되는 특성상 서버 클라이언트간 트래픽 스니핑을 통해 인증정보가 쉽게 노출되므로 접속 허용된 사용자 IP를 지정하여 접속자를 제한할 것을 권고
참고	※ 기반시설 시스템은 FTP 서비스를 사용하지 않는 것이 원칙이나, 조직 내에서 해당 서비스를 부득이 사용해야 하는 경우 관련 보호 대책을 수립 및 적용하여 활용하여야 함 ※ 관련 점검 항목 : W-26(상), W-27(상)
점검대상 및 판단기준	
대상	■ Windows NT, 2000, 2003, 2008, 2012
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
점검 및 조치 사례	

■ **Windows NT(IIS 4.0), 2000(IIS 5.0), 2003(IIS 6.0)**

Step 1) 인터넷 정보 서비스(IIS) 관리> FTP 사이트> 속성> [디렉토리 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)



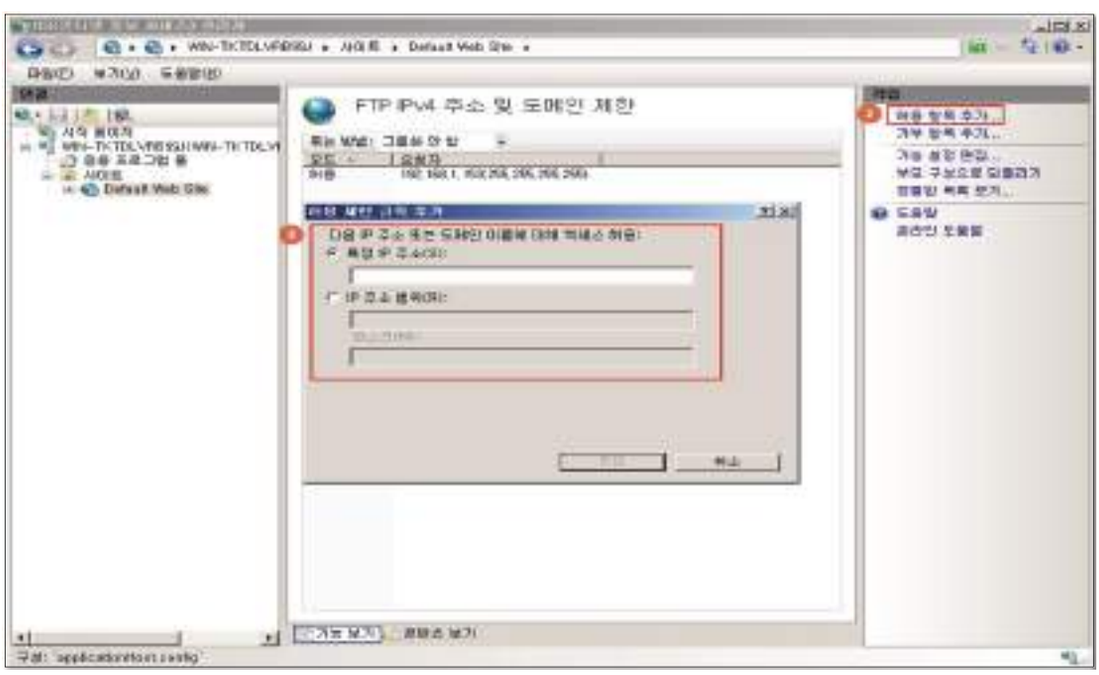
W-28 (상)	2. 서비스 관리 > 2.22 FTP 접근 제어 설정

[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

■ **Windows 2008(IIS 7.0), 2012(IIS 8.0)**

Step 1) 제어판> 관리도구> 인터넷 정보 서비스(IIS) 관리> 해당 웹사이트> FTP IPv4 주소 및 도메인 제한

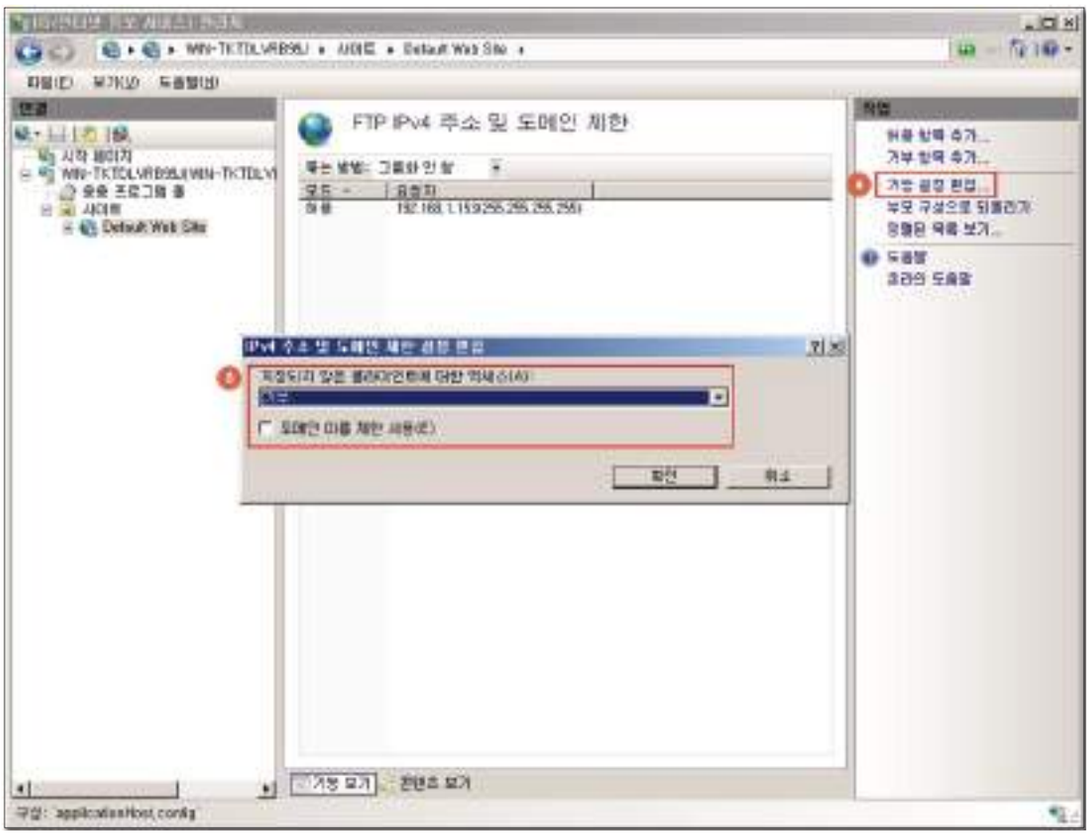
Step 2) [작업]의 허용 항목 추가에서 FTP 접속을 허용할 IP 입력



Windows 서버

W-28 (상)	2. 서비스 관리 > 2.22 FTP 접근 제어 설정

Step 3) [작업] 의 기능 설정 편집에서 지정되지 않은 클라이언트에 대한 액세스를 거부 선택



※ 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)

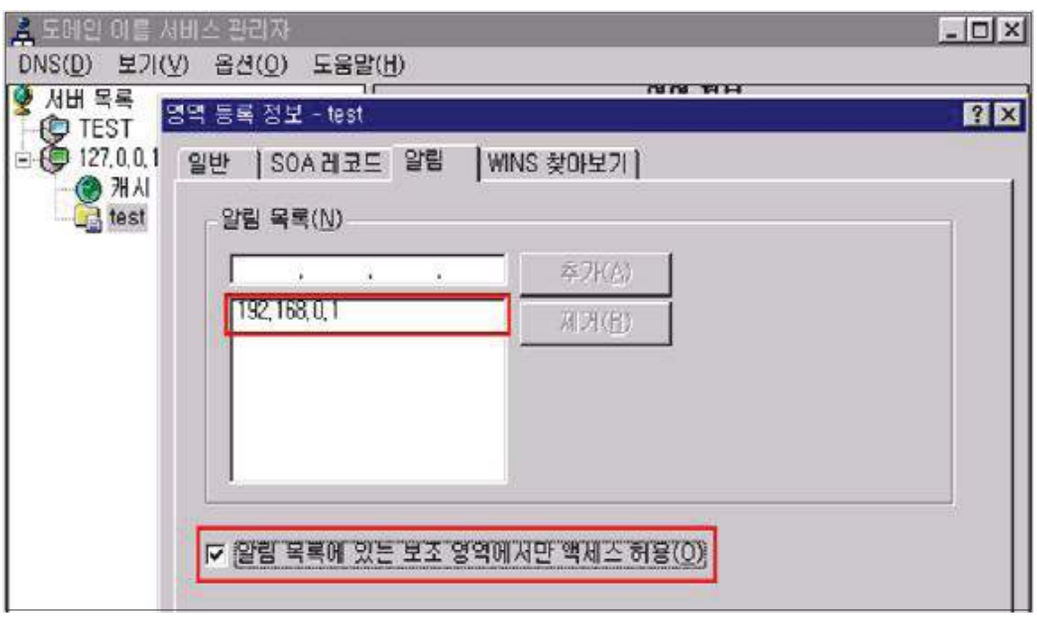
조치 시 영향	일반적인 경우 영향 없음

W-29 (상)	2. 서비스 관리 > 2.23 DNS Zone Transfer 설정
취약점 개요	
점검내용	■ DNS Zone Transfer 차단 설정 여부 점검
점검목적	■ DNS Zone Transfer 차단 설정을 적용하여 도메인 정보의 불법 외부 유출을 막고자 함
보안위협	■ DNS Zone Transfer 차단 설정이 적용되지 않은 경우 DNS 서버에 저장되어 있는 도메인 정보를 승인된 DNS 서버가 아닌 외부로 유출 위험 존재
참고	※ **zone-transfer:** zone(영역) 전송이라고 하며 master와 slave간에 또는 primary와 secondary DNS간에 zone 파일을 동기화하기 위한 용도로 사용되는 기술
점검대상 및 판단기준	
대상	■ Windows NT, 2000, 2003, 2008, 2012
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
점검 및 조치 사례	

■ **Windows NT**

Step 1) 시작> 프로그램> 관리 도구> DNS 관리자> 각 조회 영역> 해당 영역> 등록 정보> 알림

Step 2) "알림 목록에 있는 보조 영역에서만 액세스 허용" 선택 후 서버 IP 추가



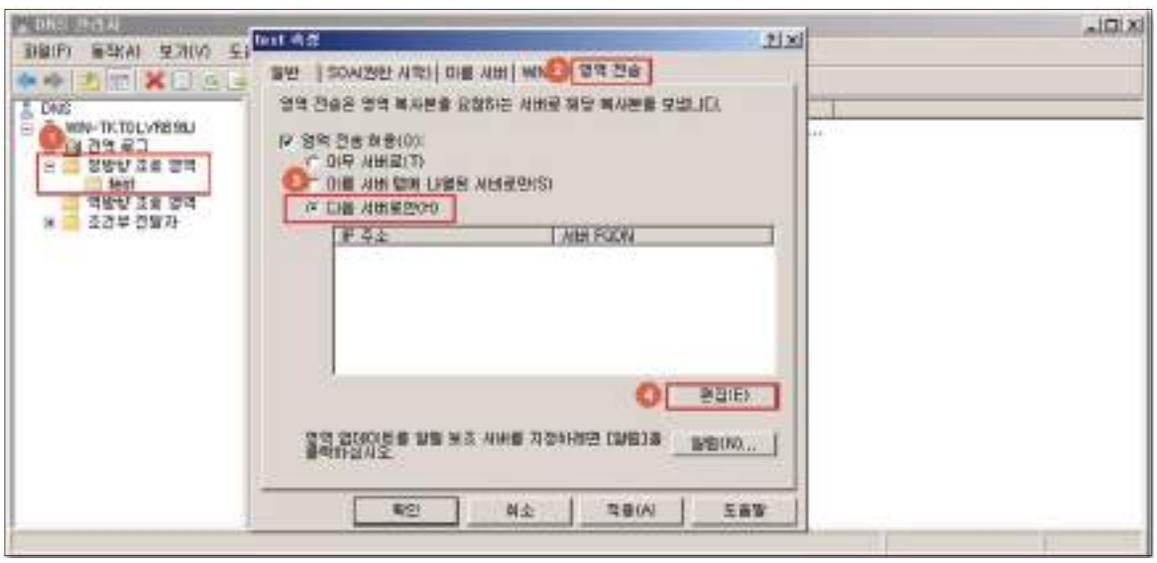
Windows 서버

W-29 (상)	2. 서비스 관리 > 2.23 DNS Zone Transfer 설정

■ **Windows 2000, 2003, 2008, 2012**

Step 1) 시작> 실행> DNSMGMT.MSC> 각 조회 영역> 해당 영역> 속성> 영역 전송

Step 2) "다음 서버로만" 선택 후 전송할 서버 IP 추가



Step 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

W-30 (상)	2. 서비스 관리 > 2.24 RDS(Remote Data Services)제거
취약점 개요	
점검내용	■ RDS(Remonte Data Services) 비활성화 여부 점검
점검목적	■ 취약한 RDS 서비스를 제거하여 불법적인 원격 공격을 차단하기 위함
보안위협	■ 취약한 플랫폼의 RDS가 사용되는 경우 서비스 거부 공격이나 원격에서 관리자 권한으로 임의의 명령을 실행할 수 있는 위험이 존재함
참고	※ MDAC 2.7 미만의 버전에서 웹 서버와 웹 클라이언트는 모두 이 취약점으로 인해 위험해질 수 있으므로 RDS가 불필요할 경우 제거하는 것이 안전함 ※ **RDS(Remote Data Services):** MDAC(Microsoft Data Access Components)의 한 컴포넌트로 클라이언트에 있는 데이터를 다룰 수 있도록 하는 서비스
점검대상 및 판단기준	
대상	■ Windows NT, 2000, 2003, 2008, 2012
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 디렉토리가 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
점검 및 조치 사례	
■ Windows NT, 2000, 2003 < RDS 제거 방법 > Step 1) 웹 사이트로부터 "/msadc" 가상 디렉토리 제거 시작> 실행> INETMGR> 웹 사이트 선택 후 오른쪽 디렉토리에서 msadc 제거 Step 2) 다음의 레지스트리 키/디렉토리 제거 HKEY_LOCAL_MACHINE₩SYSTEM₩CurrentControlSet₩Services₩W3SVC₩Parameters₩ADCLaunch₩RDSServer.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

W-31 (상)	2. 서비스 관리 > 2.25 최신 서비스팩 적용
취약점 개요	
점검내용	■ 최신 서비스팩 적용 여부 점검
점검목적	■ 시스템을 최신 버전으로 유지하여 새로운 위협 및 진행 중인 위협으로부터 중요 정보와 시스템을 보호하기 위함
보안위협	■ 보안 업데이트를 적용하지 않은 경우 시스템 및 응용프로그램의 취약성으로 인해 권한 상승, 원격 코드 실행, 보안 기능 우회 등의 문제를 일으킬 수 있음
참고	※ **서비스팩:** Windows의 안정성을 높이기 위해 응용프로그램, 서비스, 실행 파일 등 여러 수정 파일들을 모아 놓은 업데이트 프로그램
점검대상 및 판단기준	
대상	■ Windows NT, 2000, 2003, 2008, 2012
판단기준	**양호 :** 최신 서비스팩이 설치되어 있으며 적용 절차 및 방법이 수립된 경우
	취약 : 최신 서비스팩이 설치되지 않거나, 적용 절차 및 방법이 수립되지 않은 경우
조치방법	설치에 따른 영향도 확인 후 최신 서비스팩 설치(설치 후 시스템 재시작 필요)
점검 및 조치 사례	

■ **Windows NT, 2000, 2003, 2008, 2012**

Step 1) 시작> 실행> Winver

Step 2) 서비스팩 버전 확인 후 최신 버전이 아닌 경우 아래 사이트에서 최신 서비스팩 다운로드 후 설치 또는 자동업데이트 활용

※ 인터넷 웜(Worm)이 Windows의 취약점을 이용하여 공격하기 때문에 서비스팩 설치 시에는 네트워크와 분리된 상태에서 설치 할 것을 권장

[최신 서비스팩 정보(2015년 12월 기준)]

운영체제 종류	최신 서비스팩	서비스 제공 여부
Windows NT	Service pack 6a	중단
Windows Server 2000	Service pack 4	중단
Windows Server 2003	Service pack 2	중단
Windows Server 2008	2008: Service pack 2 R2: Service pack 1	제공
Windows Server 2012	2012: 없음 R2: 없음	제공

※ Windows Server 2003이하 버전의 경우 현재(2015년 12월 기준) 공식적인 서비스 제공이 중단되어 조직에서 2003 이하 버전의 시스템을 사용하는 것은 적절하지 않음

[보안 패치 사이트(2015년 12월 기준)]

Microsoft Windows Server 제품별 지원

https://technet.microsoft.com/ko-kr/library/bb625087.aspx

조치 시 영향	설치 후 시스템 재시작이 필요하며 설치에 따른 영향 정도를 확인하여야 함

W-32 (상)	3. 패치 관리 > 3.1 최신 HOT FIX 적용
취약점 개요	
점검내용	■ 최신 Hot Fix 적용 여부 점검
점검목적	■ 최신 Hot Fix를 설치하여 시스템 및 응용프로그램의 취약성을 제거하기 위함
보안위협	■ 최신 Hot Fix가 즉시 적용되지 않은 경우 알려진 취약성으로 인한 시스템 공격 가능성 존재
참고	※ Hot Fix보다 취약성을 이용한 공격도구가 먼저 출현할 수 있으므로 Hot Fix는 발표 후 가능한 한 빨리 설치할 것을 권장함 ※ **Hot Fix:** 즉시 교정되어야만 하는 주요한 취약점(주로 보안과 관련된)을 패치하기 위해 배포되는 프로그램. 서비스팩이 발표된 이후 패치가 추가될 필요가 있을 때 별도로 발표됨
점검대상 및 판단기준	
대상	■ Windows NT, 2000, 2003, 2008, 2012
판단기준	**양호 :** 최신 Hotfix가 있는지 주기적으로 모니터링하고 반영하거나, PMS (Patch Management System) Agent가 설치되어 자동패치배포가 적용된 경우
	취약 : 최신 Hotfix가 있는지 주기적으로 모니터 절차가 없거나, 최신 Hotfix를 반영하지 않은 경우, 또한 PMS(Patch Management System) Agent가 설치되어 있지 않거나, 설치되어 있으나 자동패치배포가 적용되지 않은 경우
조치방법	최신 Hotfix 설치
점검 및 조치 사례	
■ **Windows NT, 2000, 2003, 2008, 2012** **< 수동 HOT FIX 적용 >** Step 1) 아래의 패치 리스트를 조회하여, 서버에 필요한 패치를 선별하여 수동으로 설치함 https://technet.microsoft.com/ko-kr/security/ **< 자동 HOT FIX 적용 >** Step 1) Windows 자동 업데이트 기능을 이용한 설치 제어판> windows update **< PMS(Patch Management System) >** Step 1) Agent를 설치하여 자동으로 업데이트 되도록 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

Windows 서버

W-33 (상)	3. 패치 관리 > 3.2 백신 프로그램 업데이트
취약점 개요	
점검내용	■ 사용 백신의 최신 업데이트 여부 점검
점검목적	■ 백신의 최신 업데이트 상태를 유지하기 위함
보안위협	■ 백신이 지속적, 주기적으로 업데이트 되지 않은 경우 계속되는 신종 바이러스의 출현으로 인한 시스템 공격의 우려가 존재
참고	※ 네트워크망이 격리된 기반보호 시설의 경우, 시스템에 설치된 백신의 최신 업데이트 상태 유지를 위해 적절한 업데이트 절차 및 적용 방법 수립이 필요함 ※ 관련 점검 항목 : A-26(상)
점검대상 및 판단기준	
대상	■ Windows NT, 2000, 2003, 2008, 2012
판단기준	**양호 :** 바이러스 백신 프로그램의 최신 엔진 업데이트가 설치되어 있거나, 망 격리 환경의 경우 백신 업데이트를 위한 절차 및 적용 방법이 수립된 경우
	취약 : 바이러스 백신 프로그램의 최신 엔진 업데이트가 설치되어 있지 않거나, 망 격리 환경의 경우 백신 업데이트를 위한 절차 및 적용 방법이 수립되지 않은 경우
조치방법	백신 환경설정 메뉴를 통해 DB 및 엔진의 최신 업데이트를 하도록 설정
점검 및 조치 사례	
■ **Windows NT, 2000, 2003, 2008, 2012** 1. 긴급한 경우 수시로 업데이트 진행 (백신 종류마다 다소 차이는 있으나 매주 업데이트가 진행됨) 2. 정기적인 업데이트를 통해 검색엔진을 최신 버전으로 유지하고, 백신 사에서 발표하는 경보 주시 3. 백신 프로그램의 자동 업데이트 기능을 이용하면 온라인을 통해 변동 사항을 자동으로 업데이트 하여 알 수 있음 ※ 4개 백신 업체 모두 긴급 시 수시 업데이트 및 실시간 업데이트 기능 제공 ※ 기타 기관에서 사용중인 백신의 환경설정에서 업데이트 기능 활성화 여부 확인	
조치 시 영향	일반적인 경우 영향 없음

W-34 (상)	4. 로그 관리 > 4.1 로그의 정기적 검토 및 보고
취약점 개요	
점검내용	■ 로그의 정기적 검토 및 보고 여부 점검
점검목적	■ 정기적인 로그 점검을 통해 안정적인 시스템 상태 유지 및 외부 공격 여부를 파악하기 위함
보안위협	■ 로그의 검토 및 보고 절차가 없는 경우 외부 침입 시도에 대한 식별이 누락될 수 있고, 침입 시도가 의심되는 사례 발견 시 관련 자료를 분석하여 해당 장비에 대한 접근을 차단하는 등의 추가 조치가 어려움
참고	※ 시스템 접속 기록, 계정 관리 로그 등 W-69(중) 점검 항목에서 설정한 보안 로그를 포함하여 응용 프로그램, 시스템 로그 기록에 대하여 주기적인 검토 및 보고가 필요함 ※ 관련 점검 항목 : A-85(하), W-69(중)
점검대상 및 판단기준	
대상	■ Windows NT, 2000, 2003, 2008, 2012
판단기준	**양호 :** 접속기록 등의 보안 로그, 응용 프로그램 및 시스템 로그 기록에 대해 정기적으로 검토, 분석, 리포트 작성 및 보고 등의 조치가 이루어지는 경우
	취약 : 위 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
점검 및 조치 사례	

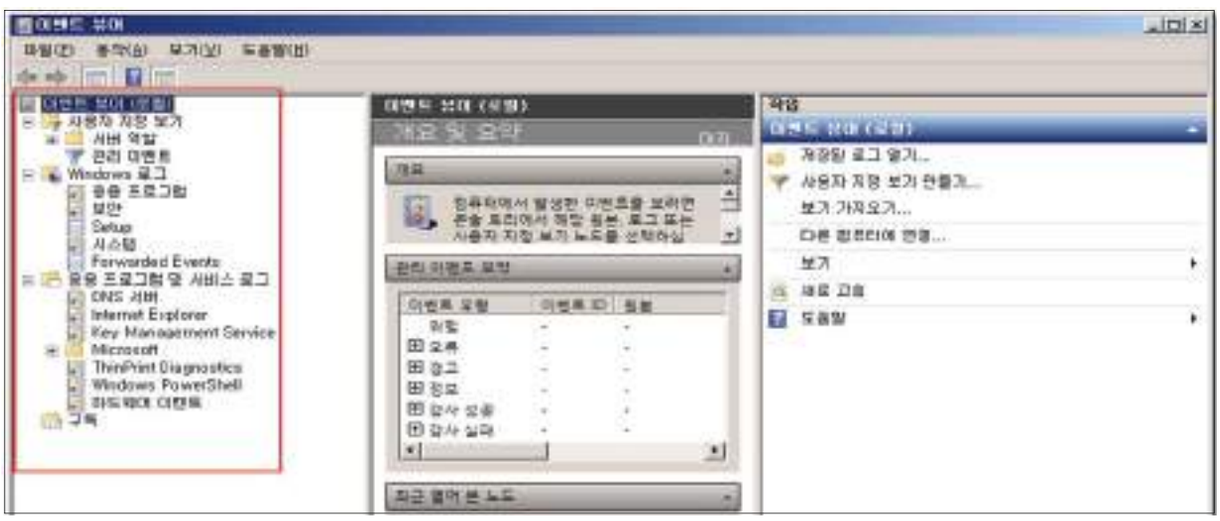
■ Windows NT, 2000, 2003, 2008, 2012

Step 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

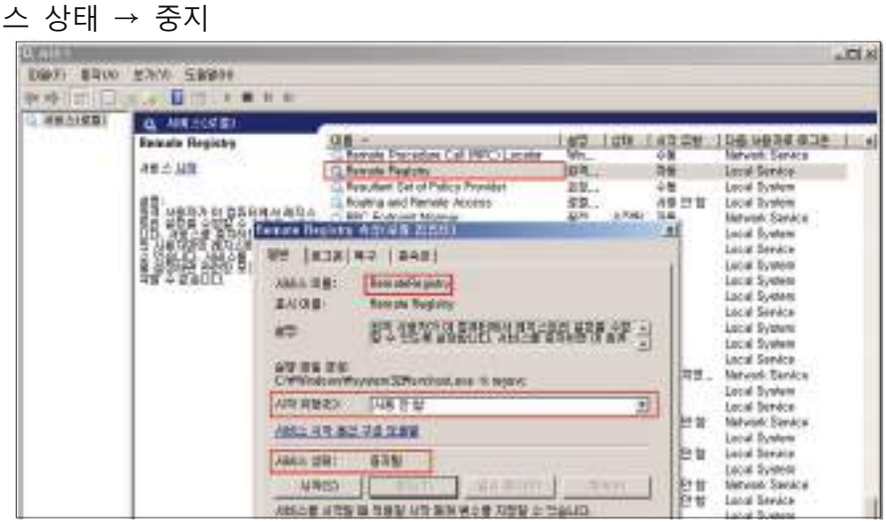
※ OS 구성에 따라 디렉토리 서비스 로그, 파일 복제 서비스 로그, DNS 서버 로그 등 분석



Step 2) 로그 분석 결과에 대한 일일·월간 보고서 작성 및 보고

조치 시 영향	일반적인 경우 영향 없음

Windows 서버

W-35 (상)	4. 로그 관리 > 4.2 원격으로 액세스 할 수 있는 레지스트리 경로
취약점 개요	
점검내용	■ 원격 레지스트리 서비스 사용 여부 점검
점검목적	■ 원격 레지스트리 서비스를 비활성화 하여 레지스트리에 대한 원격 접근을 차단하기 위함
보안위협	■ 원격 레지스트리 서비스는 액세스에 대한 인증이 취약하여 관리자 계정 외 다른 계정들에게도 원격 레지스트리 액세스를 허용할 우려가 있으며, 레지스트리에 대한 권한설정이 잘못되어 있는 경우 원격에서 레지스트리를 통해 임의의 파일을 실행 할 우려가 있음 ■ 레지스트리 서비스의 장애는 전체 시스템에 영향을 줄 수 있어 서비스거부공격(DoS) 공격에 이용될 수 있음
참고	※ **레지스트리:** 윈도우를 실행하는데 필요한 모든 환경설정 데이터를 모아 두는 중앙 저장소 ※ **원격 레지스트리 서비스:** 원격지에 있는 컴퓨터를 한 곳에서 집중관리하기 위한 목적으로 원격 컴퓨터의 레지스트리에 접근할 수 있도록 하는 서비스
점검대상 및 판단기준	
대상	■ Windows NT, 2000, 2003, 2008, 2012
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
점검 및 조치 사례	
■ **Windows NT, 2000, 2003, 2008, 2012** Step 1) 시작> 실행> SERVICES.MSC> Remote Registry> 속성 Step 2) 시작 유형 → 사용 안 함 Step 3) 서비스 상태 → 중지 	
조치 시 영향	Remote Registry Service를 사용하는지 확인 필요 (서비스> Remote Registry Service> 등록 정보> 종속성 참고)

W-36 (상)	5. 보안 관리 > 5.1 백신 프로그램 설치
취약점 개요	
점검내용	■ 시스템 내 백신 프로그램 설치 여부 점검
점검목적	■ 적절한 백신 프로그램을 설치하여 바이러스 감염 여부 진단, 치료 및 파일 보호를 통한 예방 조치를 위함
보안위협	■ 백신 프로그램이 설치되지 않은 경우 웜, 트로이목마 등의 악성 바이러스로 인한 시스템 피해 위험이 있음
참고	※ **웜:** 악의적인 목적을 가지고 자기 자신을 복제해 전파시키며 주로 네트워크 공유 폴더나 메일로 전파됨 ※ **트로이목마:** 고의적으로 악의적 목적이 있는 파일, 주로 다른 악성코드나 위장된 프로그램으로 전파되거나 인터넷을 통해 다운로드 됨 ※ 관련 점검 항목 : A-26(상)
점검대상 및 판단기준	
대상	■ Windows NT, 2000, 2003, 2008, 2012
판단기준	**양호 :** 바이러스 백신 프로그램이 설치되어 있는 경우
	취약 : 바이러스 백신 프로그램이 설치되어 있지 않은 경우
조치방법	담당자를 통해 바이러스 반드시 설치하여야 하도록 함
점검 및 조치 사례	
• 안철수 연구소: http://www.ahnlab.com • 하우리: http://www.hauri.co.kr • 시만텍코리아: http://www.symantec.co.kr • 한국트렌드마이크로: http://www.trendmicro.co.kr • 알약: https://en.estsecurity.com ※ 위 목록에 나열되지 않은 백신에 대해서도 인지도, 효과성 등을 검토하여 설치할 수 있음	
조치 시 영향	일반적인 경우 영향 없음

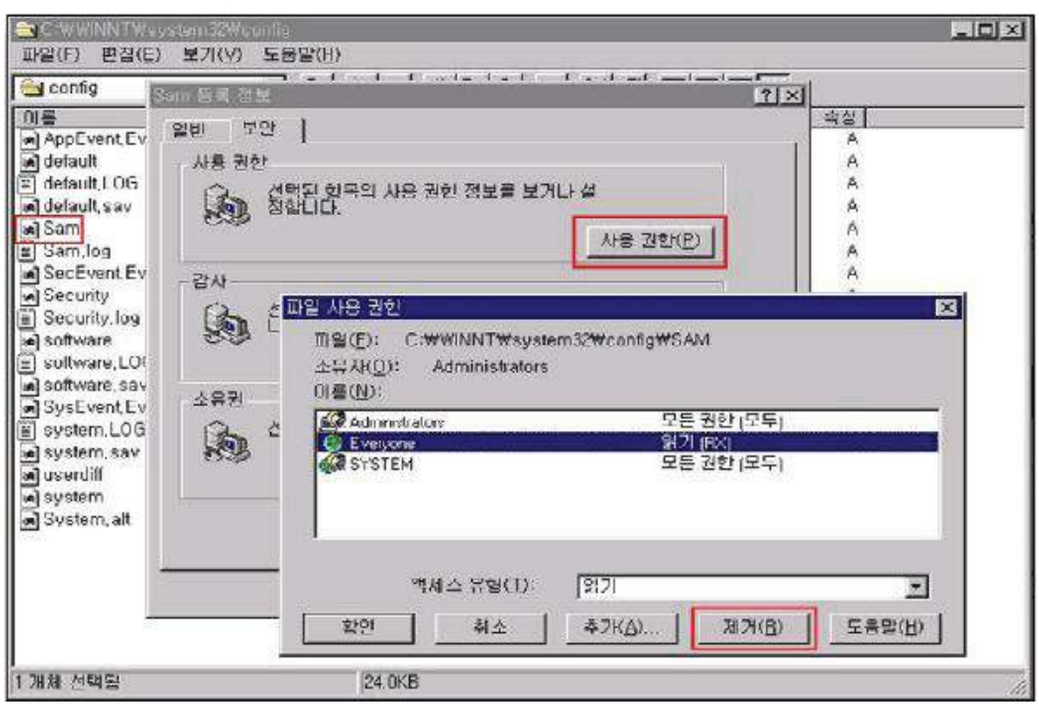
Windows 서버

W-37 (상)	5. 보안 관리 > 5.2 SAM 파일 접근 통제 설정
취약점 개요	
점검내용	■ SAM 파일 접근 통제 설정 여부 점검
점검목적	■ Administrator 및 System 그룹만 SAM 파일에 접근할 수 있도록 제한하여 악의적인 계정 정보 유출을 차단하고자 함
보안위협	■ SAM 파일이 노출될 경우 패스워드 공격 시도로 인해 계정 및 패스워드 데이터베이스 정보가 탈취될 우려 존재
참고	※ **SAM(Security Account Manager):** 사용자와 그룹 계정의 패스워드를 관리하고, LSA(Local Security Authority)를 통한 인증을 제공함
점검대상 및 판단기준	
대상	■ Windows NT, 2000, 2003, 2008, 2012
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
점검 및 조치 사례	

■ **Windows NT**

Step 1) %systemroot%₩system32₩config₩SAM> 속성> 보안

Step 2) Administrator, System 그룹 외 다른 사용자 및 그룹 권한 제거

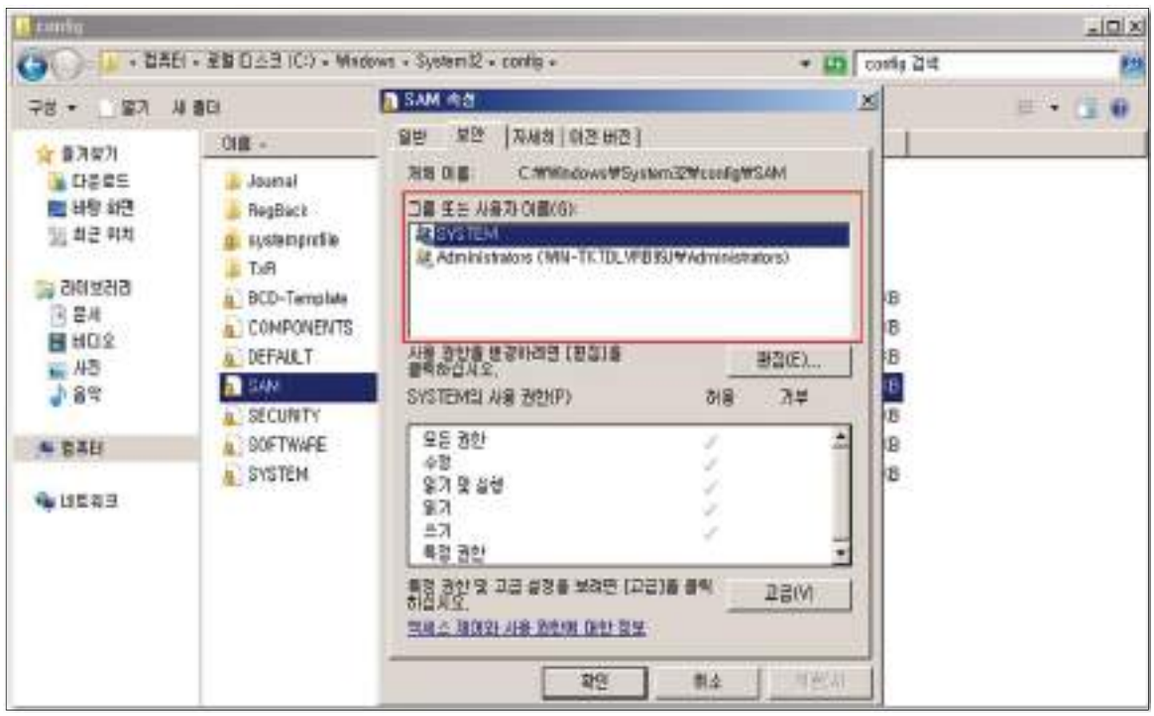


W-37 (상)	5. 보안 관리 > 5.2 SAM 파일 접근 통제 설정

■ **Windows 2000, 2003, 2008, 2012**

Step 1) %systemroot%₩system32₩config₩SAM> 속성> 보안

Step 2) Administrator, System 그룹 외 다른 사용자 및 그룹 권한 제거



조치 시 영향	일반적인 경우 영향 없음

Windows 서버

W-38 (상)	5. 보안 관리 > 5.3 화면보호기 설정
취약점 개요	
점검내용	■ 시스템 화면보호기 설정 여부 점검
점검목적	■ 사용자가 일정 시간 동안 아무런 작업을 수행하지 않을 경우 자동으로 로그오프되거나 워크스테이션이 잠기도록 설정하여, 유휴 시간 내 불법적인 시스템 접근을 차단하기 위함
보안위협	■ 화면보호기 설정을 하지 않은 경우 사용자가 자리를 비운 사이에 임의의 사용자가 해당 시스템에 접근하여 중요 정보를 유출 하거나, 악의적인 행위를 통해 시스템 운영에 악영향을 미칠 수 있음
참고	-
점검대상 및 판단기준	
대상	■ Windows NT, 2000, 2003, 2008, 2012
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
점검 및 조치 사례	

■ **Windows NT, 2000**

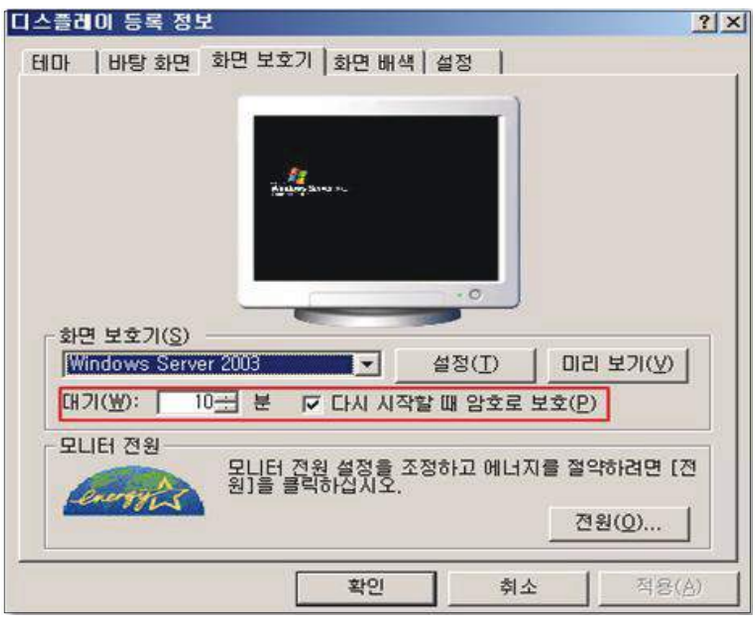
Step 1) 바탕화면> 등록 정보> 화면 보호기> "암호 사용" 체크, 대기 시간 "10분" 설정

W-38 (상)	5. 보안 관리 > 5.3 화면보호기 설정

■ **Windows 2003, 2008, 2012**

< Windows 2003 >

Step 1) 바탕화면> 마우스 우클릭> 속성> 디스플레이 등록 정보> [화면 보호기]> "다시 시작할 때 암호로 보호" 체크 "대기 시간" 10분 설정



< Windows 2008, 2012 >

Step 1) 제어판> 디스플레이> 화면보호기 변경> "다시 시작할 때 로그온 화면 표시" 체크, "대기 시간" 10분 설정

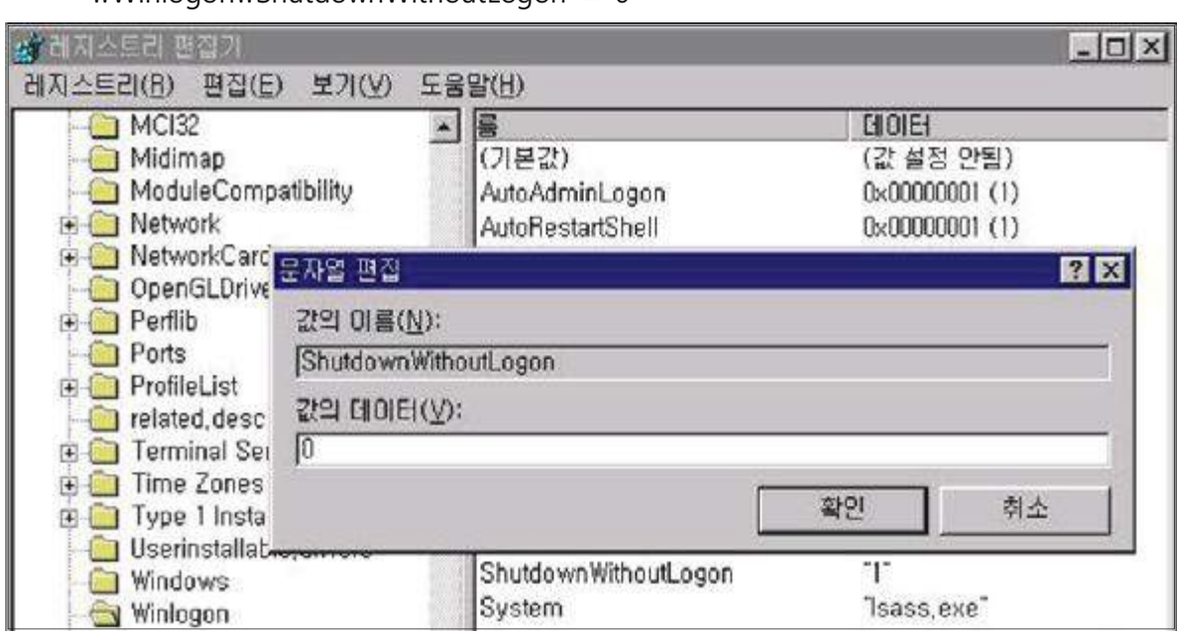
조치 시 영향	일반적인 경우 영향 없음

Windows 서버

W-39 (상)	5. 보안 관리 > 5.4 로그온 하지 않고 시스템 종료 허용 해제
취약점 개요	
점검내용	■ 비로그온 사용자의 시스템 종료 허용 여부 점검
점검목적	■ 시스템 로그온 창의 종료 버튼을 비활성화 시킴으로써 허가되지 않은 사용자를 통한 불법적인 시스템 종료를 방지하고자 함
보안위협	■ 로그온 창에 "시스템 종료" 버튼이 활성화되어 있으면 로그인을 하지 않고도 불법적인 시스템 종료가 가능하여 정상적인 서비스 운영에 영향을 줌
참고	-
점검대상 및 판단기준	
대상	■ Windows NT, 2000, 2003, 2008, 2012
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: 로그온 하지 않고 시스템 종료 허용 → 사용 안 함
점검 및 조치 사례	

■ **Windows NT**

Step 1) HKEY_LOCAL_MACHINE₩SOFTWARE₩Microsoft₩Windows NT₩CurrentVersion ₩Winlogon₩ShutdownWithoutLogon = 0

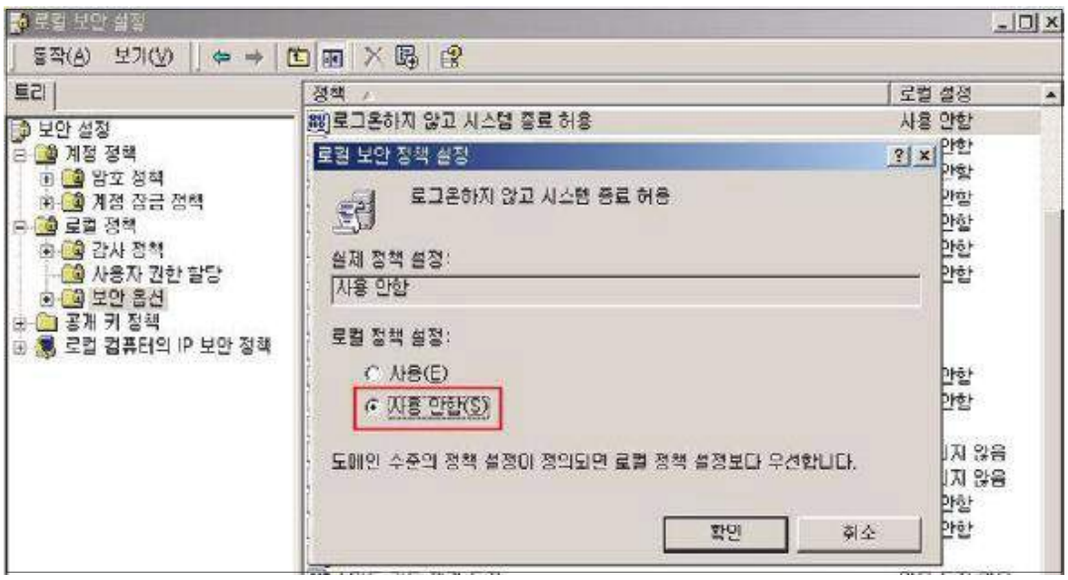


W-39 (상)	5. 보안 관리 > 5.4 로그온 하지 않고 시스템 종료 허용 해제

■ **Windows 2000**

Step 1) 시작> 실행> SECPOL.MSC> 로컬 정책> 보안 옵션

Step 2) "로그온 하지 않고 시스템 종료 허용"을 "사용 안함"으로 설정



■ **Windows 2003, 2008, 2012**

Step 1) 시작> 실행> SECPOL.MSC> 로컬 정책> 보안 옵션

Step 2) "시스템 종료: 로그온 하지 않고 시스템 종료 허용"을 "사용 안 함"으로 설정

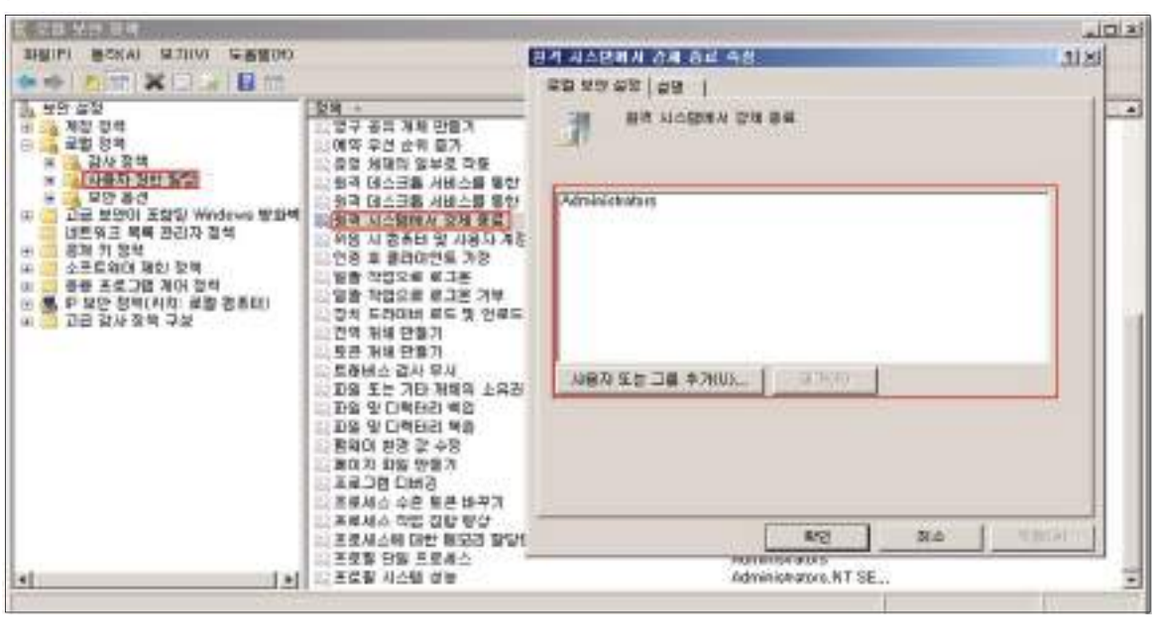
조치 시 영향	일반적인 경우 영향 없음

W-40 (상)	5. 보안 관리 > 5.5 원격 시스템에서 강제로 시스템 종료
취약점 개요	
점검내용	■ 원격 시스템 종료 정책 적절성 점검
점검목적	■ 원격에서 네트워크를 통하여 운영 체제를 종료할 수 있는 사용자나 그룹을 설정하여 특정 사용자만 시스템 종료를 허용하기 위함
보안위협	■ 원격 시스템 강제 종료 설정이 부적절한 경우 서비스 거부 공격 등에 악용될 수 있음
참고	-
점검대상 및 판단기준	
대상	■ Windows NT, 2000, 2003, 2008, 2012
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
점검 및 조치 사례	

■ **Windows NT, 2000, 2003, 2008, 2012**

Step 1) 시작> 실행> SECPOL.MSC> 로컬 정책> 사용자 권한 할당

Step 2) "원격 시스템에서 강제로 시스템 종료" 정책에 Administrators 외 다른 계정 및 그룹 제거



조치 시 영향	일반적인 경우 영향 없음

Windows 서버

W-41 (상)	5. 보안 관리 > 5.6 보안 감사를 로그할 수 없는 경우 즉시 시스템 종료 해제
취약점 개요	
점검내용	■ '보안 감사를 로그할 수 없는 경우 즉시 시스템 종료' 정책 설정 여부 점검
점검목적	■ 해당 정책을 비활성화 함으로써 로그 용량 초과 등의 이유로 이벤트를 기록할 수 없는 경우, 해당 정책으로 인해 시스템이 비정상적으로 종료되는 것을 방지하기 위함
보안위협	■ 해당 정책이 활성화 되어 있는 경우 악의적인 목적으로 시스템 종료를 유발하여 서비스 거부 공격에 악용될 수 있으며, 비정상적인 시스템 종료로 인하여 시스템 및 데이터에 손상을 입힐 수 있음
참고	※ 일반적으로 보안 감사 로그가 꽉 찼을 때 보안 로그에 대한 보존 방법이 [이벤트를 덮어쓰지 않음] 또는 [매일 이벤트 덮어쓰기]인 경우 이벤트가 로그되지 않음. 보안 로그가 꽉 차고 기존 항목을 덮어쓸 수 없을 때 해당 정책을 사용하는 경우 다음과 같은 중지 오류가 나타남 **중지**: C0000244 {감사 실패} 보안 감사를 만들려고 했으나 만들지 못했습니다. 복구하려면 관리자가 로그온하여 로그를 보관한 다음 로그를 지우고 이 옵션을 원하는 대로 다시 설정해야 합니다. 이 보안 설정을 다시 설정할 때까지는 보안 로그가 꽉 차지 않았더라도 Administrators 그룹의 구성원이 아니면 어떤 사용자도 시스템에 로그온할 수 없습니다.
점검대상 및 판단기준	
대상	■ Windows NT, 2000, 2003, 2008, 2012
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	보안 감사를 로그할 수 없는 경우 즉시 시스템 종료 -> 사용 안 함

Windows 서버

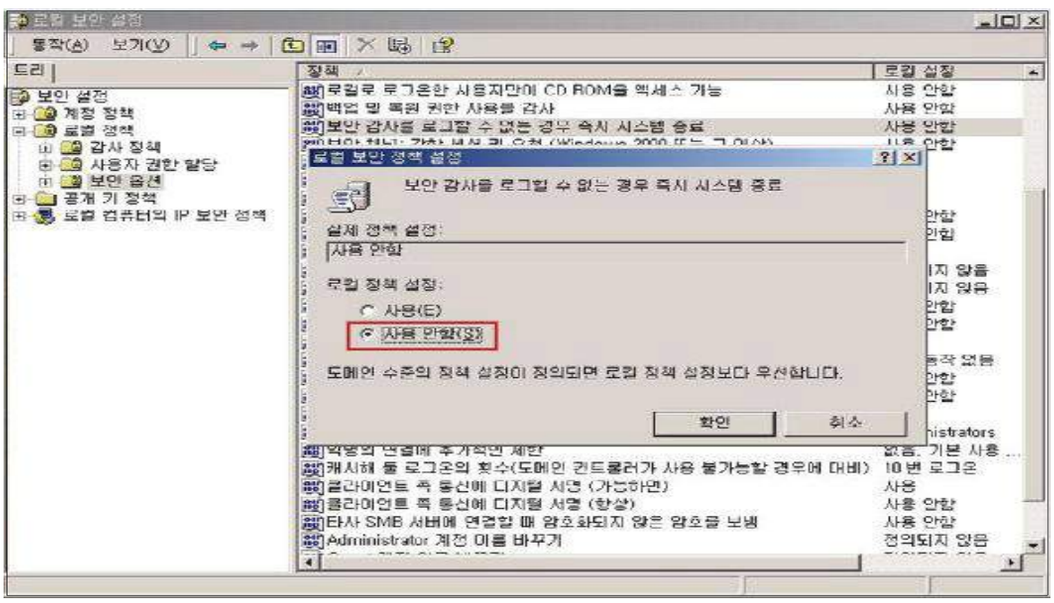
W-41 (상)	5. 보안 관리 > 5.6 보안 감사를 로그할 수 없는 경우 즉시 시스템 종료 해제

점검 및 조치 사례

■ **Windows NT, 2000**

Step 1) 시작> 실행> SECPOL.MSC> 로컬 정책> 보안 옵션

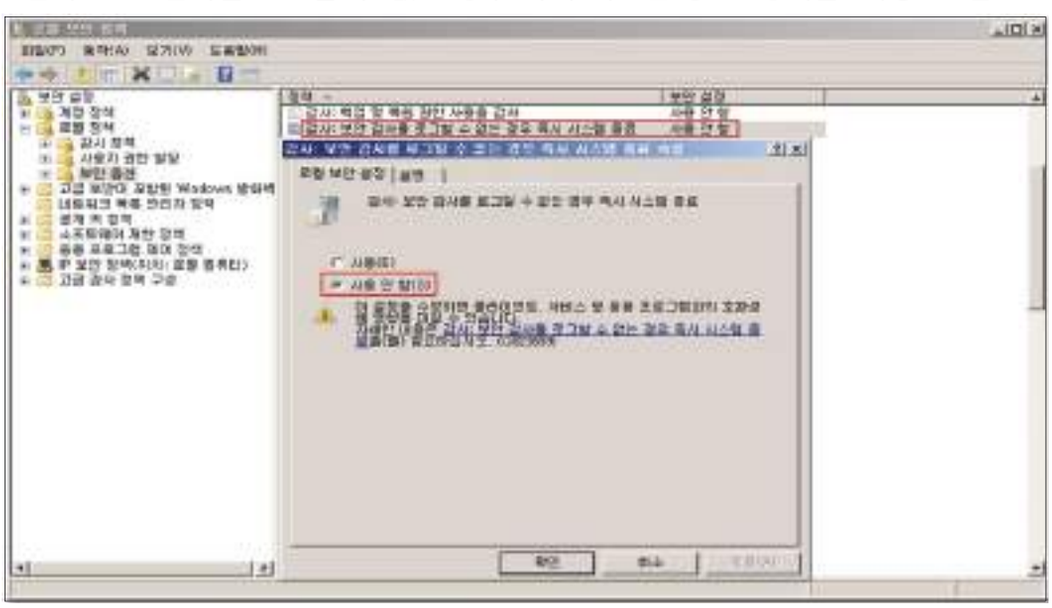
Step 2) "보안 감사를 로그할 수 없는 경우 즉시 시스템 종료" 정책을 "사용 안 함" 으로 설정



■ **Windows 2003, 2008, 2012**

Step 1) 시작> 실행> SECPOL.MSC> 로컬 정책> 보안 옵션

Step 2) "감사: 보안 감사를 로그할 수 없는 경우 즉시 시스템 종료" 정책을 "사용 안 함" 으로 설정



조치 시 영향	일반적인 경우 영향 없음

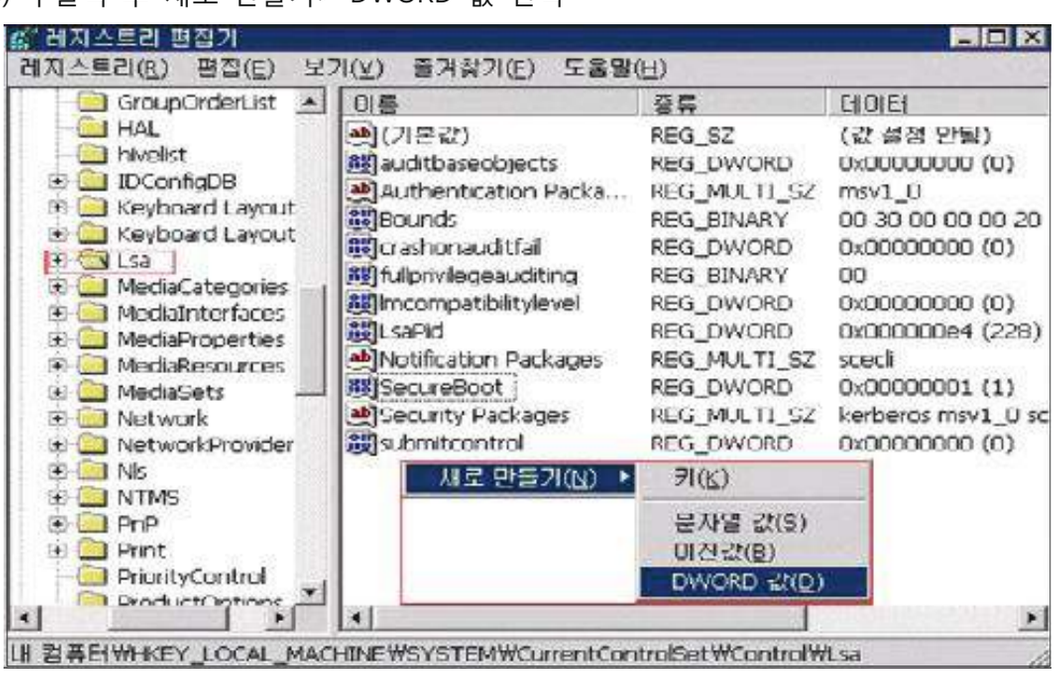
W-42 (상)	5. 보안 관리 > 5.7 SAM 계정과 공유의 익명 열거 허용 안 함
취약점 개요	
점검내용	■ 'SAM 계정과 공유의 익명 열거 허용 안 함' 정책 설정 여부 점검
점검목적	■ 익명 사용자에 의한 악의적인 계정 정보 탈취를 방지하기 위함
보안위협	■ Windows에서는 익명의 사용자가 도메인 계정(사용자, 컴퓨터 및 그룹)과 네트워크 공유 이름의 열거 작업을 수행할 수 있으므로 SAM(보안계정관리자) 계정과 공유의 익명 열거가 허용될 경우 악의적인 사용자가 계정 이름 목록을 확인하고 이 정보를 사용하여 암호를 추측하거나 사회 공학적 공격기법을 수행할 수 있음
참고	※ 방화벽과 라우터에서 135~139(TCP, UDP)포트 차단을 통해 외부로부터의 위협을 차단함 ※ 네트워크 및 전화 접속 연결> 로컬 영역> 등록 정보> 고급> 고급 설정 > Microsoft 네트워크 파일 및 프린트 공유를 해제하여야 함
점검대상 및 판단기준	
대상	■ Windows NT, 2000, 2003, 2008, 2012
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
점검 및 조치 사례	

■ **Windows NT**

Step 1) 시작> 실행> regedit

Step 2) HKLM₩SYSTEM₩CurrentControlSet₩Control₩LSA 레지스트리 검색

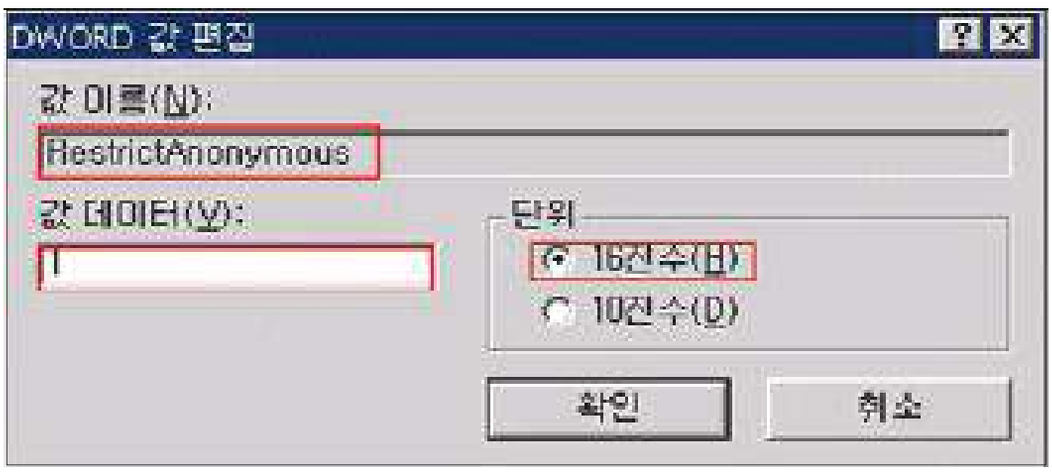
Step 3) 우클릭 후 새로 만들기> DWORD 값 선택



Windows 서버

W-42 (상)	5. 보안 관리 > 5.7 SAM 계정과 공유의 익명 열거 허용 안 함

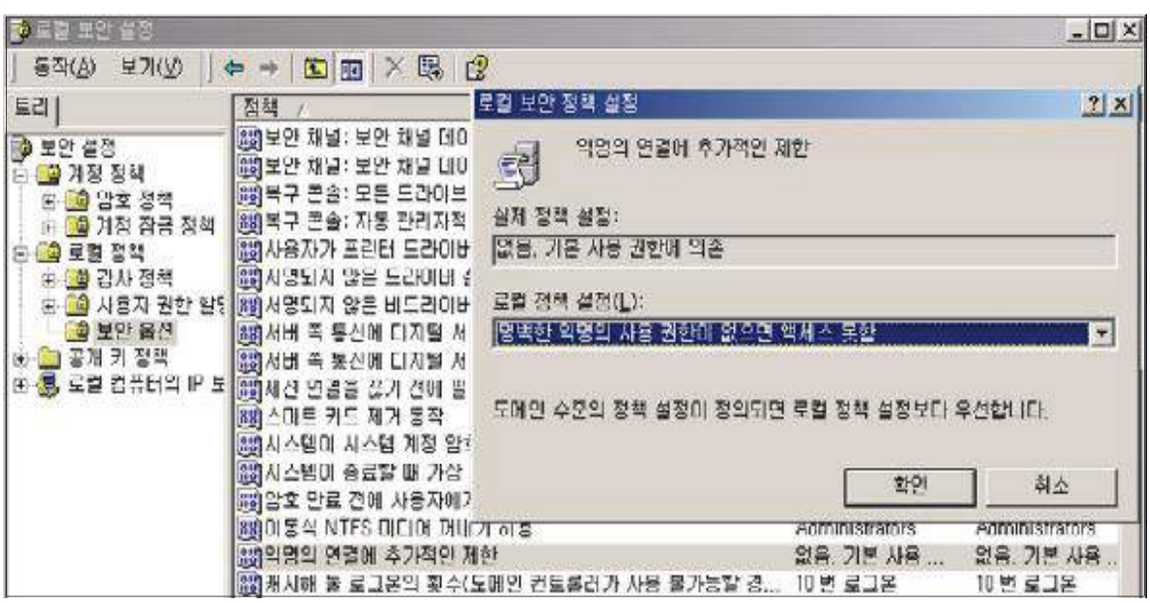
Step 4) RestrictAnonymous를 입력 후 데이터 Default 값인 "0"을 "1"로 변경



■ **Windows 2000**

Step 1) 시작> 실행> SECPOL.MSC> 로컬 정책> 보안 옵션

Step 2) "익명의 연결에 추가적인 제한" 에 "명백한 익명의 사용 권한이 없으면 액세스 제한" 선택

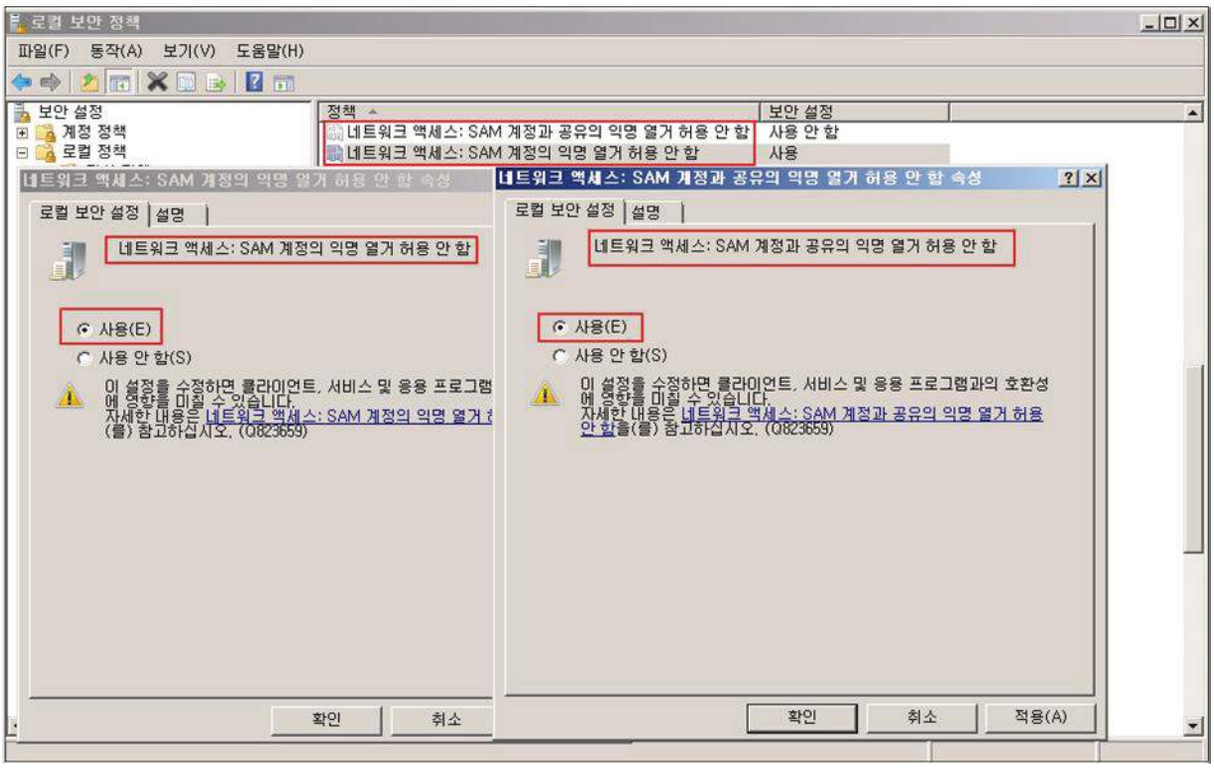


■ **Windows 2003, 2008, 2012**

Step 1) 시작> 실행> SECPOL.MSC> 로컬 정책> 보안 옵션

Step 2) "네트워크 액세스 : SAM 계정과 공유의 익명 열거 허용 안 함"과 "네트워크 액세스 : SAM 계정의 익명 열거 허용 안 함"에 "사용" 선택

W-42 (상)	5. 보안 관리 > 5.7 SAM 계정과 공유의 익명 열거 허용 안 함



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

Windows 서버

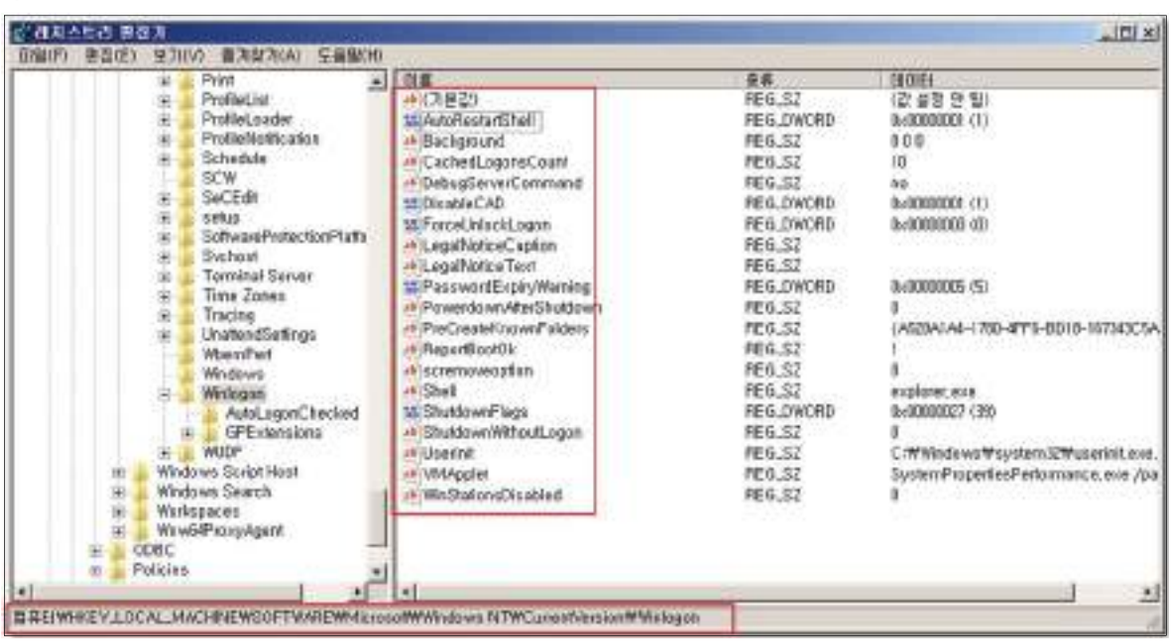
W-43 (상)	5. 보안 관리 > 5.8 Autologin 기능 제어
취약점 개요	
점검내용	■ Autologin 기능 제어 설정 여부 점검
점검목적	■ Autologon 기능을 사용하지 않도록 설정하여 시스템 계정 정보 노출을 차단하기 위함
보안위협	■ Autologon 기능을 사용하면 침입자가 해킹 도구를 이용하여 레지스트리에 저장된 로그인 계정 및 패스워드 정보 유출 가능
참고	※ **Autologon:** 레지스트리에 암호화 되어 저장된 대체 증명을 사용하여 자동으로 로그인하는 기능
점검대상 및 판단기준	
대상	■ Windows NT, 2000, 2003, 2008, 2012
판단기준	**양호 :** AutoAdminLogon 값이 없거나 0으로 설정되어 있는 경우
	취약 : AutoAdminLogon 값이 1로 설정되어 있는 경우
조치방법	해당 레지스트리 값이 존재하는 경우 0으로 설정
점검 및 조치 사례	

■ **Windows NT, 2000, 2003, 2008, 2012**

Step 1) 시작> 실행> REGEDIT>
HKLM₩SOFTWARE₩Microsoft₩WindowsNT₩CurrentVersion₩Winlogon

Step 2) "AutoAdminLogon 값"을 "0"으로 설정

Step 3) DefaultPassword 엔트리가 존재한다면 삭제



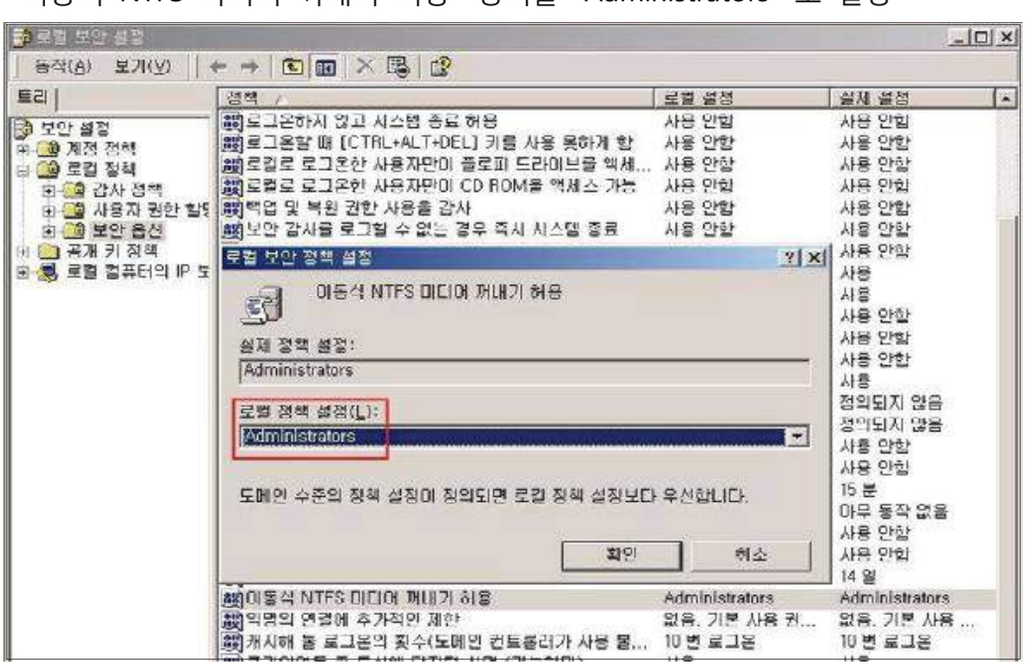
조치 시 영향	반드시 자동 로그인을 사용하여야 할 경우를 제외하고는 일반적으로 영향 없음

W-44 (상)	5. 보안 관리 > 5.9 이동식 미디어 포맷 및 꺼내기 허용
취약점 개요	
점검내용	■ 관리자 이외 NTFS 미디어 포맷 및 꺼내기 허용 여부 점검
점검목적	■ 이동식 미디어의 NTFS 포맷 및 꺼내기가 허용되는 사용자를 관리 권한자로 제한함으로써 관리 권한이 없는 사용자 및 비인가자에 의한 불법적인 이동식 미디어의 포맷 및 이동을 차단하기 위함
보안위협	■ 관리자 이외 사용자에게 해당 정책이 설정된 경우 비인가자에 의한 불법적인 매체 처리를 허용할 수 있음
참고	※ 해당 보안 설정은 이동식 NTFS 미디어를 포맷하거나 꺼낼 수 있는 사용자를 결정하는 옵션으로 Administrators, Administrators 및 Power Users, Administrators 및 Interactive Users 그룹에 이 기능을 허용할 수 있음
점검대상 및 판단기준	
대상	■ Windows NT, 2000, 2003, 2008, 2012
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
점검 및 조치 사례	

■ **Windows NT, 2000**

Step 1) 시작> 실행> SECPOL.MSC> 로컬 정책> 보안 옵션

Step 2) "이동식 NTFS 미디어 꺼내기 허용" 정책을 "Administrators" 로 설정



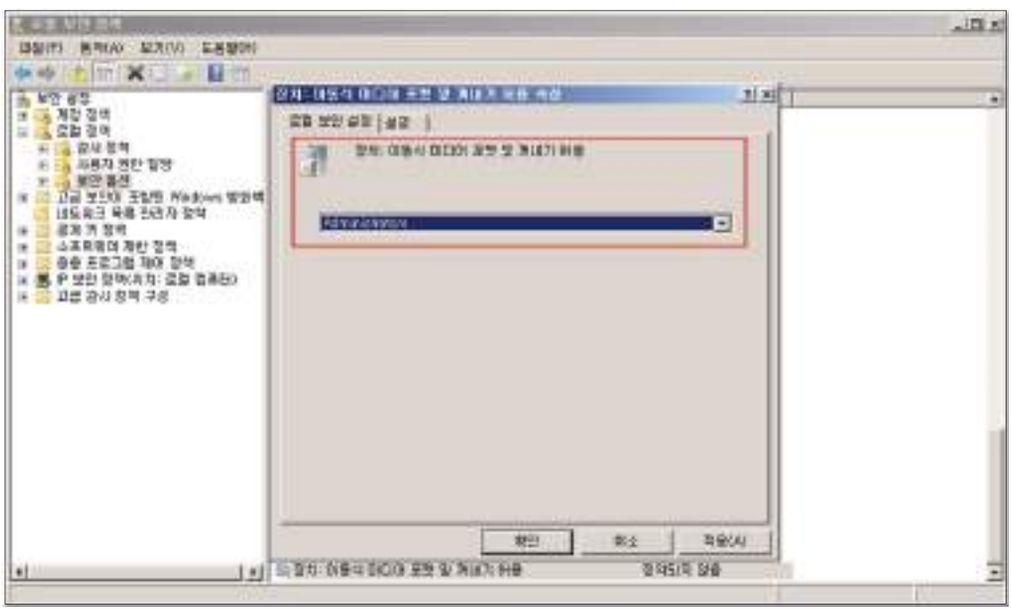
Windows 서버

W-44 (상)	5. 보안 관리 > 5.9 이동식 미디어 포맷 및 꺼내기 허용

■ **Windows 2003, 2008, 2012**

Step 1) 시작> 실행> SECPOL.MSC> 로컬 정책> 보안 옵션

Step 2) "장치 : 이동식 미디어 포맷 및 꺼내기 허용" 정책을 "Administrators" 로 설정

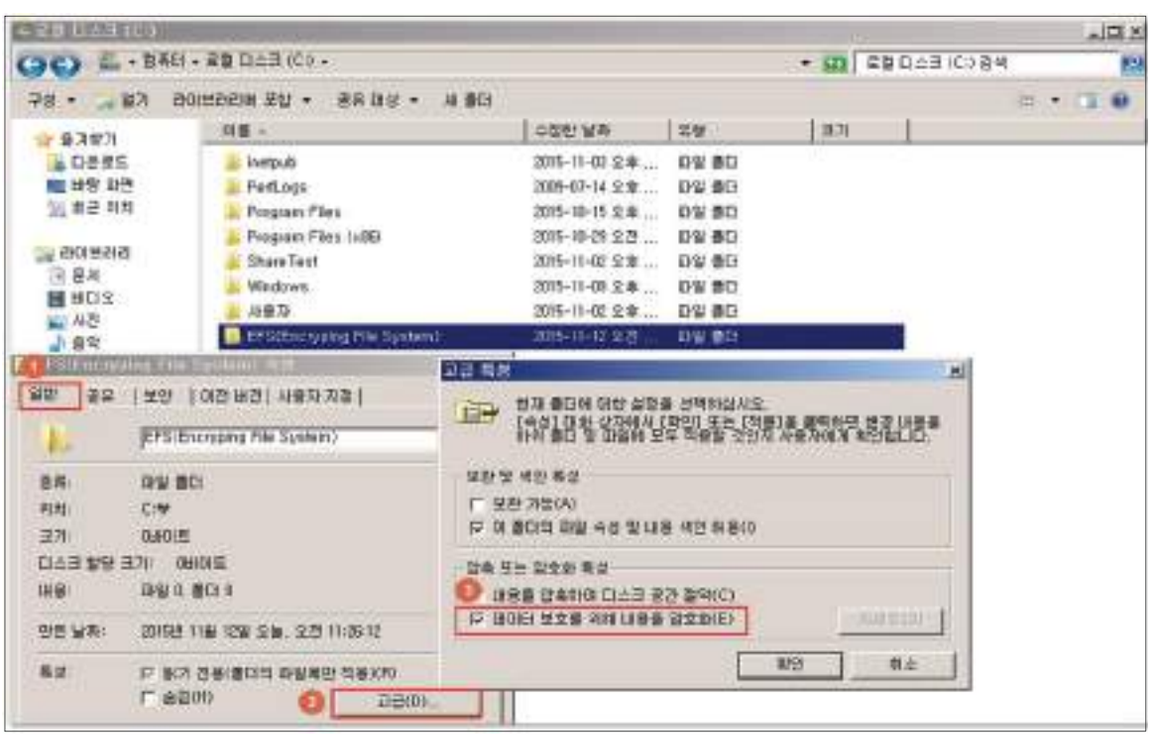


조치 시 영향	일반적으로 영향 없음

W-45 (상)	5. 보안 관리 > 5.10 디스크볼륨 암호화 설정
취약점 개요	
점검내용	■ 디스크볼륨 암호화 설정 여부 점검
점검목적	■ 디스크볼륨 암호화 설정을 적용하여 비인가 액세스로부터 중요 데이터를 보호하기 위함
보안위협	■ 디스크 볼륨이 암호화 되어 있지 않은 경우 비인가자가 데이터를 열람할 수 있음
참고	-
점검대상 및 판단기준	
대상	■ Windows NT, 2000, 2003, 2008, 2012
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
점검 및 조치 사례	

■ **Windows 2000, 2003, 2008, 2012**

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



※ 폴더 속성> [보안] 탭에서 허가된 사용자 외에는 폴더 내 파일 접근 불가함

조치 시 영향	복호키 분실 시 데이터복구 어려움

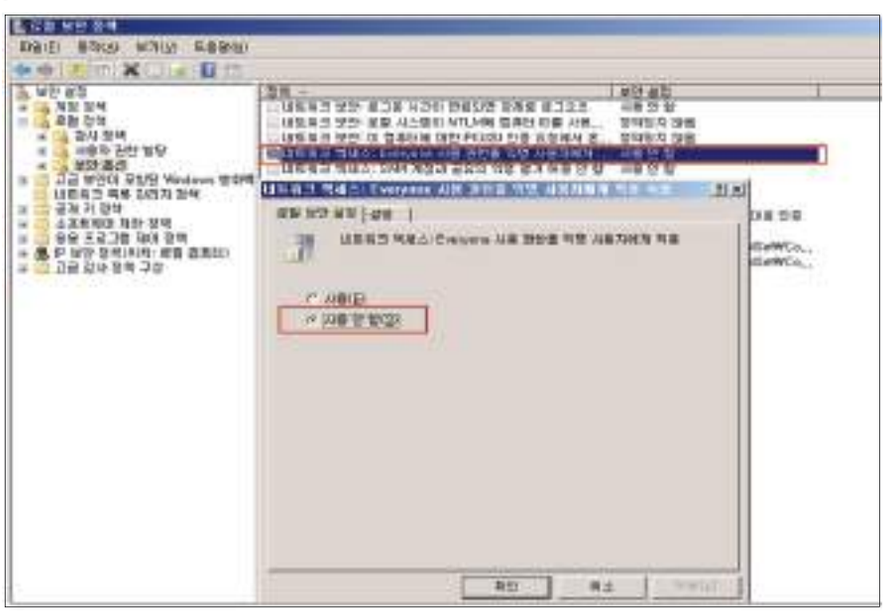
Windows 서버

W-46 (중)	1. 계정관리 > 1.7 Everyone 사용 권한을 익명 사용자에 적용 해제
취약점 개요	
점검내용	■ 'Everyone 사용 권한을 익명 사용자에 적용' 정책의 설정 여부 점검
점검목적	■ 익명 사용자가 Everyone 그룹으로 사용 권한을 준 모든 리소스에 접근하는 것을 차단하여 비인가자에 의한 접근 가능성을 제한하기 위함
보안위협	■ 해당 정책이 "사용"으로 설정될 경우 권한이 없는 사용자가 익명으로 계정 이름 및 공유 리소스를 나열하고 이 정보를 사용하여 암호를 추측하거나 DoS(Denial of Service) 공격을 실행할 수 있음
참고	※ **DoS(Denial of Service):** 관리자 권한 없이도 특정서버에 처리할 수 없을 정도로 대량의 접속신호를 한꺼번에 보내 해당 서버가 마비되도록 하는 해킹 기법
점검대상 및 판단기준	
대상	■ Windows NT, 2000, 2003, 2008, 2012
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
점검 및 조치 사례	

■ **Window 2003, 2008, 2012**

Step 1) 시작> 실행> SELPOL.MSC> 로컬 정책> 보안 옵션

Step 2) "Everyone 사용 권한을 익명 사용자에게 적용" 정책이 "사용 안 함"으로 설정

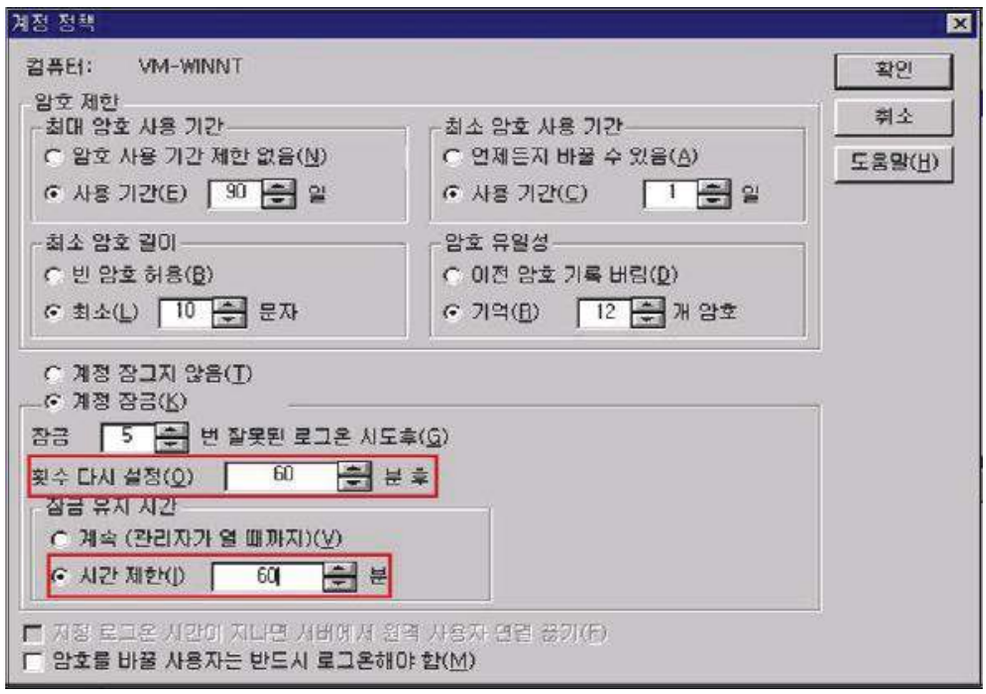


조치 시 영향	애플리케이션이나 Backup 용도로 Everyone 공유를 사용하지 않는지 확인 필요

W-47 (중)	1. 계정관리 > 1.8 계정 잠금 기간 설정
취약점 개요	
점검내용	■ 사용자 계정 잠금 기간 정책 설정 여부 점검
점검목적	■ 로그인 실패 임계값 초과 시 일정 시간 동안 계정 잠금을 실시하여 공격자의 자유로운 암호 유추 공격을 차단하기 위함
보안위협	■ 로그인 실패 시 일정 시간 동안 계정 잠금을 하지 않은 경우, 공격자의 자동화된 암호 추측 공격이 가능하여, 사용자 계정의 패스워드 정보가 유출될 수 있음
참고	※ 계정 잠금 기간 설정은 계정 잠금 임계값을 초과한 사용자 계정이 잠기는 시간을 결정함. 잠긴 계정은 관리자가 재설정하거나 해당 계정의 잠금 유지 시간이 만료되어야 사용할 수 있음 ※ 계정 잠금 기간 설정을 사용하면 지정한 기간 동안 잠긴 계정은 사용할 수 없으며, 계정 잠금이 해제될 때까지 접근할 수 없음 ※ **계정 잠금 정책:** 해당 계정이 시스템으로부터 잠기는 환경과 시간을 결정하는 정책으로 '계정 잠금 기간', '계정 잠금 임계값', '다음 시간 후 계정 잠금 수를 원래대로 설정'의 세가지 하위 정책을 가짐 ※ 관련 점검 항목 : W-4(상)
점검대상 및 판단기준	
대상	■ Windows NT, 2000, 2003, 2008, 2012
판단기준	**양호 :** "계정 잠금 기간" 및 "계정 잠금 기간 원래대로 설정 기간"이 설정되어 있는 경(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
점검 및 조치 사례	
■ **Window NT** Step 1) 시작> 프로그램> 관리도구> 도메인 사용자 관리자> 정책> 계정 정책 Step 2) "횟수 다시 설정"을 "60분 후"로 설정, "잠금 유지 기간"의 "시간 제한"을 "60분" 으로 설정	

Windows 서버

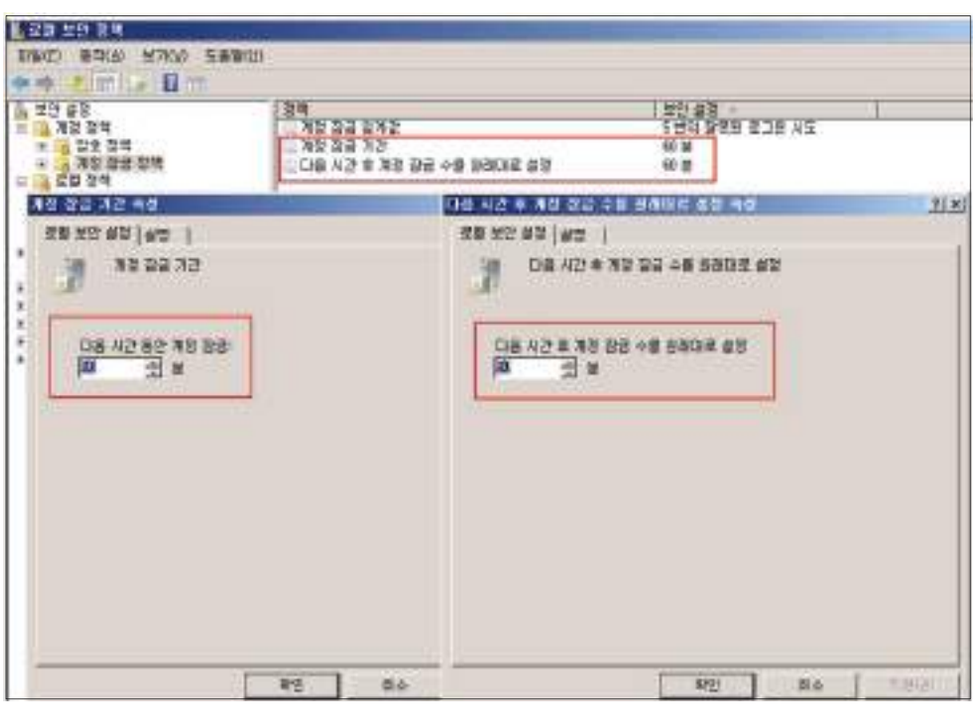
W-47 (중)	1. 계정관리 > 1.8 계정 잠금 기간 설정



■ **Windows 2000, 2003, 2008, 2012**

Step 1) 시작> 실행> SECPOL.MSC> 계정 정책> 계정 잠금 정책

Step 2) "계정 잠금 기간", "다음 시간 후 계정 잠금 수를 원래대로 설정"에 대해 각각 "60분" 설정



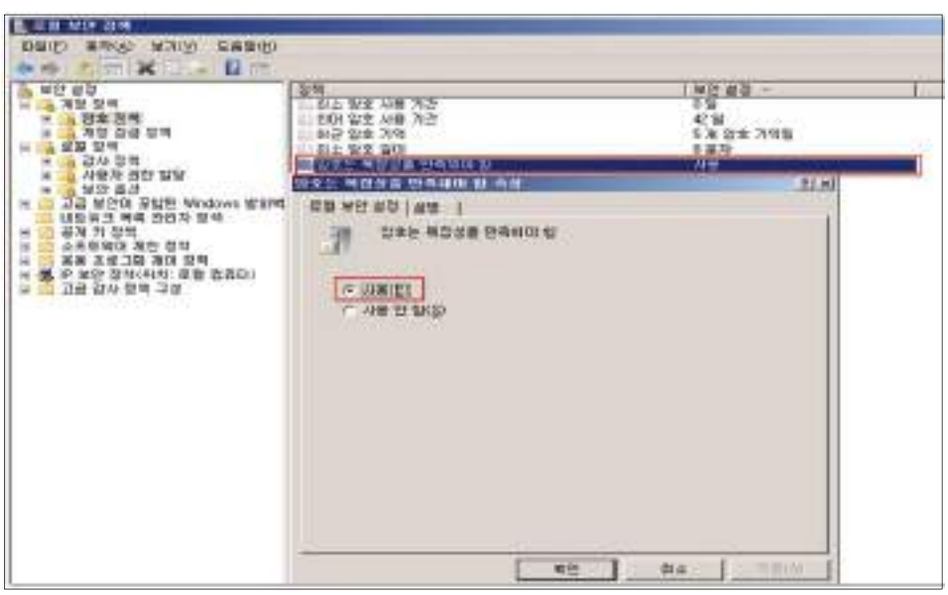
조치 시 영향	일반적으로 영향 없음

W-48 (중)	1. 계정관리 > 1.9 패스워드 복잡성 설정
취약점 개요	
점검내용	■ 계정 패스워드 복잡성 정책 설정 여부 점검
점검목적	■ 패스워드 설정 시 문자/숫자/특수문자를 모두 포함한 강화된 패스워드를 사용하여 패스워드 복잡성을 만족하도록 함
보안위협	■ 사용자 암호가 패스워드 복잡성을 만족하지 못하는 반복되는 문자, 연속되는 숫자, 계정이름이 포함된 패스워드 등을 사용할 경우 무작위 대입 공격(Brute Force Attack)이나 패스워드 추측 공격(Password Guessing Attack)에 쉽게 크랙될 수 있음
참고	※ 패스워드 설정 시 영문/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 ※ 관련 점검 항목 : W-49(중), W-50(중), W-51(중)
점검대상 및 판단기준	
대상	■ Windows NT, 2000, 2003, 2008, 2012
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
점검 및 조치 사례	

■ Windows NT, 2000, 2003, 2008, 2012

Step 1) 시작> 실행> SECPOL.MSC> 계정 정책> 암호 정책

Step 2) "암호는 복잡성을 만족해야 함"을 "사용"으로 설정



Windows 서버

W-48 (중)	1. 계정관리 > 1.9 패스워드 복잡성 설정
※ 이 정책 설정은 암호를 변경하거나 새로운 암호 생성 시 아래와 같은 일련의 규정을 만족하는지 결정함. 영문, 숫자, 특수문자 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

W-49 (중)	1. 계정관리 > 1.10 패스워드 최소 암호 길이
취약점 개요	
점검내용	■ 패스워드 최소 암호 길이 정책 설정 여부 점검
점검목적	■ 암호에 필요한 최소 문자 수를 지정하여 강화된 패스워드를 사용하기 위함
보안위협	■ 짧은 패스워드 및 일반적인 단어와 일반적인 어구를 이용해 암호를 설정한 경우 사전 공격이나 가능한 모든 문자의 조합을 시도하는 무작위 공격을 통해 쉽게 패스워드가 도용될 수 있음
참고	※ **암호정책:** 사용자에게 암호를 정기적으로 변경하게 하고, 암호의 최소 길이를 지정하며, 암호가 특정 복잡성을 만족시키도록 하는 등 암호 설정을 사용자 강제하여 컴퓨터를 보호하는 정책 ※ 관련 점검 항목 : W-48(중), W-50(중), W-51(중)
점검대상 및 판단기준	
대상	■ Windows NT, 2000, 2003, 2008, 2012
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
점검 및 조치 사례	

■ **Windows NT**

Step 1) 시작> 프로그램> 관리도구> 도메인 사용자 관리자> 정책> 계정 정책

Step 2) "최소 암호 길이"에 "최소"를 "8문자"로 설정

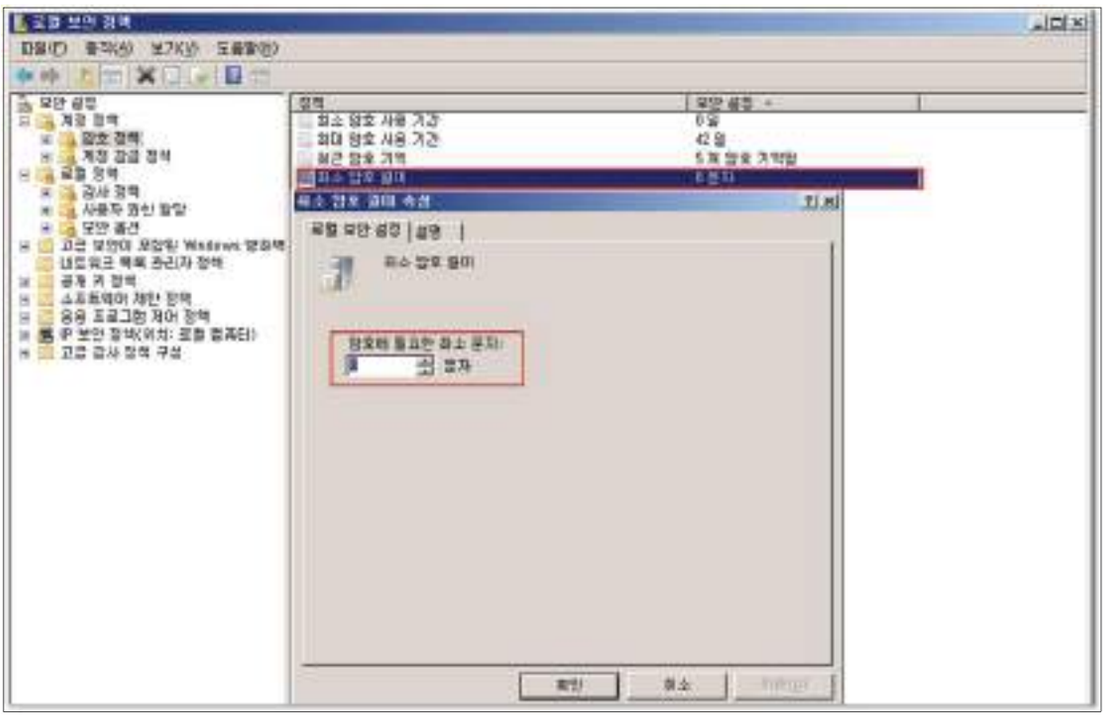
Windows 서버

W-49 (중)	1. 계정관리 > 1.10 패스워드 최소 암호 길이

■ **Windows 2000, 2003, 2008, 2012**

Step 1) 시작> 실행> SECPOL.MSC> 계정정책> 암호 정책

Step 2) "최소 암호 길이"를 "8문자"로 설정



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

W-50 (중)	1. 계정관리 > 1.11 패스워드 최대 사용 기간
취약점 개요	
점검내용	■ 패스워드 최대 사용 기간 정책의 설정 여부 점검
점검목적	■ 암호가 유효한 최대 날짜를 설정하여 이 날짜가 경과된 사용자는 암호를 변경하도록 하여 암호 크래킹의 가능성을 낮추고, 불법으로 획득한 암호의 무단 사용을 방지하고자 함
보안위협	■ 오랫동안 변경하지 않은 패스워드를 지속적으로 사용하는 경우 암호 추측 공격에 의해 유출될 수 있으므로 사용자가 암호를 자주 바꾸도록 하면 유효한 암호가 공격당하는 위험을 줄일 수 있음
참고	※ **암호정책:** 사용자에게 암호를 정기적으로 변경하게 하고, 암호의 최소 길이를 지정하며, 암호가 특정 복잡성을 만족시키도록 하는 등 암호 설정을 강제하여 컴퓨터를 보호하는 정책 ※ 관련 점검 항목 : W-48(중), W-49(중), W-51(중)
점검대상 및 판단기준	
대상	■ Windows NT, 2000, 2003, 2008, 2012
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
점검 및 조치 사례	

■ **Windows NT**

Step 1) 시작> 프로그램> 관리도구> 도메인 사용자 관리자> 정책> 계정

Step 2) "최대 암호 사용 기간"의 "사용 기간"을 "90일"로 설정

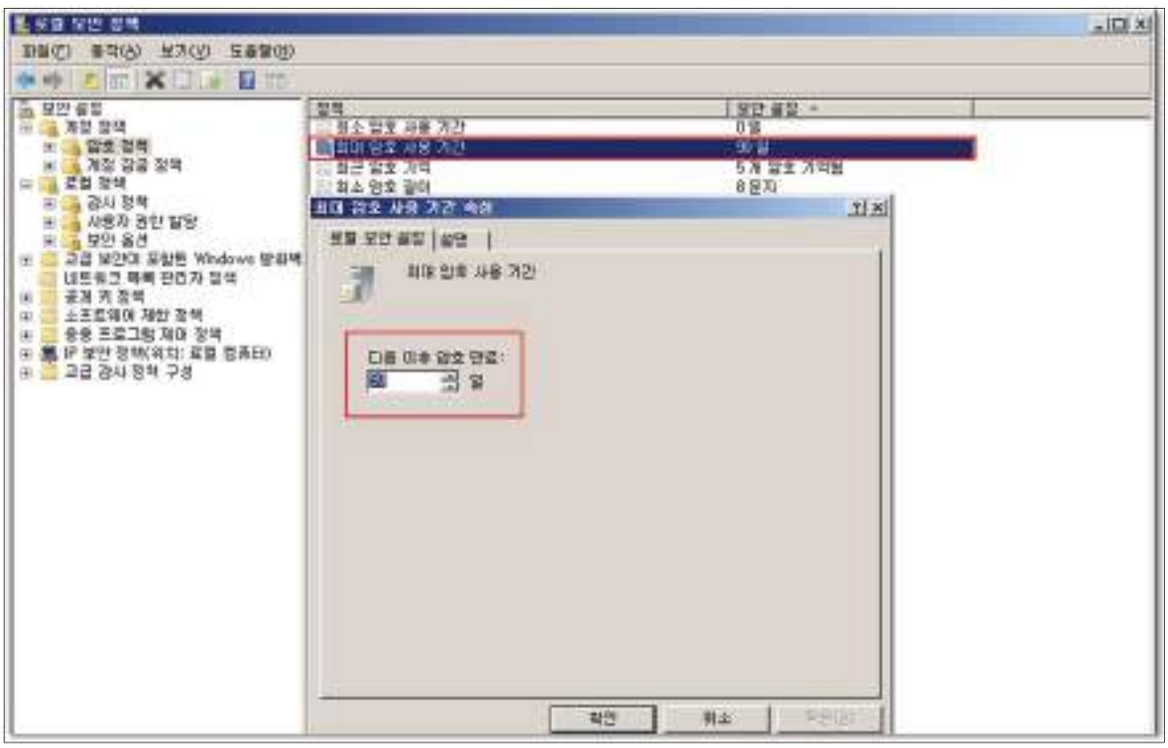
Windows 서버

W-50 (중)	1. 계정관리 > 1.11 패스워드 최대 사용 기간

■ **Windows 2000, 2003, 2008, 2012**

Step 1) 시작> 실행> SECPOL.MSC> 계정정책> 암호 정책

Step 2) "최대 암호 사용 기간"의 다음 이후 암호 만료 기간을 "90일"로 설정



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

W-51 (중)	1. 계정관리 > 1.12 패스워드 최소 사용 기간
취약점 개요	
점검내용	■ 패스워드 최소 사용 기간 정책 설정 여부 점검
점검목적	■ 암호를 변경할 수 있기 전까지 경과해야 하는 최소 날짜를 설정하여 원래 패스워드로 즉시 변경할 수 없도록 함
보안위협	■ 패스워드 변경 후 최소 사용 기간이 설정되지 않은 경우 사용자에게 익숙한 패스워드로 즉시 변동이 가능하여, 이를 재사용함으로써 원래 암호를 같은 날 다시 사용할 수 있음 ■ 패스워드 변경 정책에 따른 주기적인 패스워드 변경이 무의미해 질 수 있으며, 이로 인해 조직의 계정 보안성을 낮출 수 있음
참고	※ **암호정책:** 사용자에게 암호를 정기적으로 변경하게 하고, 암호의 최소 길이를 지정하며, 암호가 특정 복잡성을 만족시키도록 하는 등 암호 설정을 강제하여 컴퓨터를 보호하는 정책 ※ 이 정책은 이전 암호를 그대로 재사용 하는 것을 방지하기 위해 W-55(중) '최근 암호 기억' 정책과 같이 적용될 경우 보안성이 훨씬 강화됨 ※ 관련 점검 항목 : W-48(중), W-49(중), W-50(중), W-55(중)
점검대상 및 판단기준	
대상	■ Windows NT, 2000, 2003, 2008, 2012
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
점검 및 조치 사례	
■ **Windows NT** Step 1) 시작> 프로그램> 관리도구> 도메인 사용자 관리자> 정책> 계정 Step 2) "최소 암호 사용 기간"에서 "사용 기간"을 "1일"로 설정	

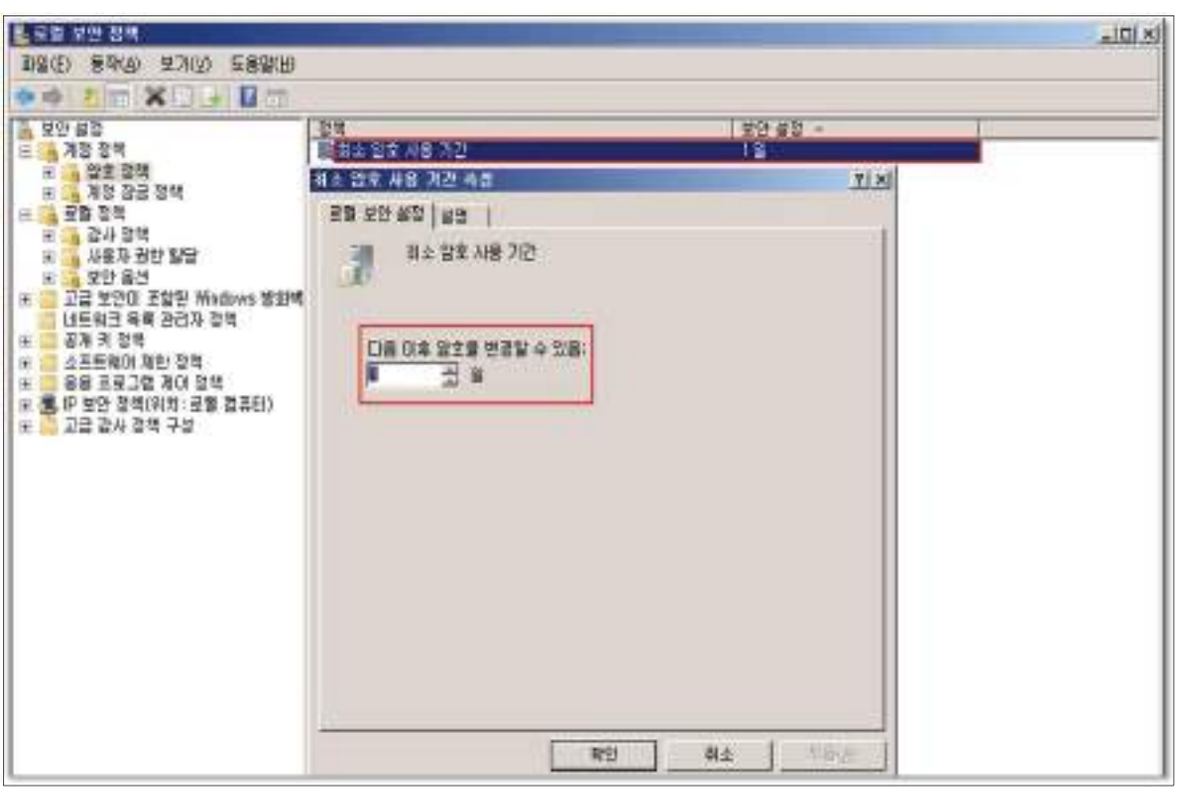
Windows 서버

W-51 (중)	1. 계정관리 > 1.12 패스워드 최소 사용 기간

■ **Windows 2000, 2003, 2008, 2012**

Step 1) 시작> 실행> SECPOL.MSC> 계정정책> 암호 정책

Step 2) "최소 암호 사용 기간"을 "1일"로 설정

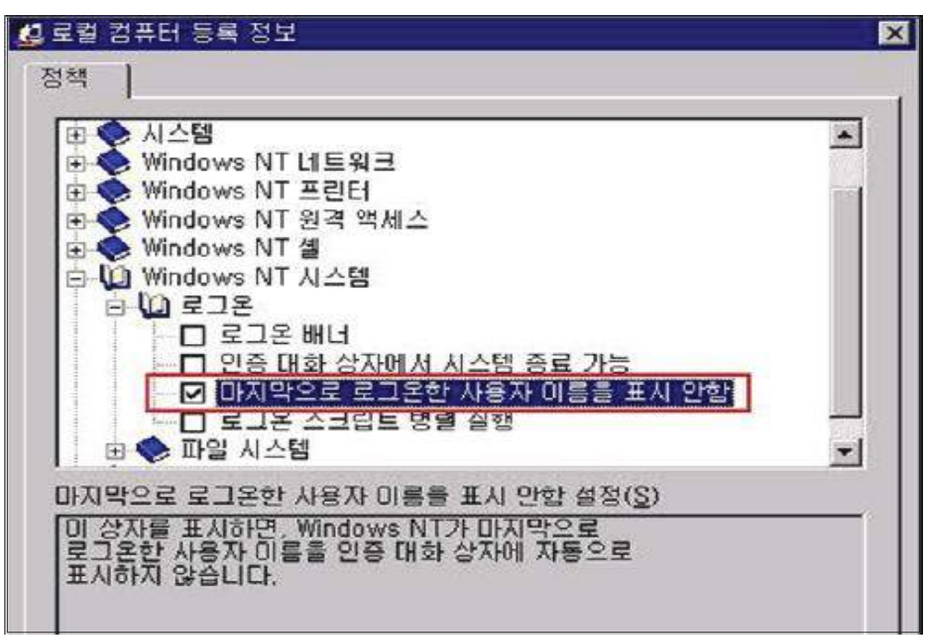


조치 시 영향	패스워드를 변경 후 다시 변경하기 위해서는 1일이 지나야 하며, 일반적으로 영향 없음

W-52 (중)	1. 계정관리 > 1.13 마지막 사용자 이름 표시 안 함
취약점 개요	
점검내용	■ 로그인 화면에 마지막 로그온 사용자 이름을 표시하지 않도록 설정되었는지 여부를 점검
점검목적	■ Windows 로그인 화면에 마지막 로그온 한 사용자 이름이 표시되지 않도록 하여 악의적인 사용자에게 계정 정보가 노출되는 것을 차단하고자 함
보안위협	■ 마지막으로 로그온한 사용자의 이름이 로그온 대화 상자에 표시될 경우 공격자는 이를 획득하여 암호를 추측하거나 무작위 공격을 시도할 수 있음
참고	※ Windows 로그인 화면에 마지막 로그온 한 사용자 이름이 표시될 경우 주로 콘솔 사용자 및 터미널 서비스 이용자에게 시스템에 존재하는 사용자 계정 정보를 노출함
점검대상 및 판단기준	
대상	■ Windows NT, 2000, 2003, 2008, 2012
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 로그온한 사용자 이름 표시 안 함 → 설정 후 저장 • Windows 2000 : 로그온 스크린에 마지막 사용자 이름 표시 안 함 → 사용 • Windows 2003, 2008, 2012 : 대화형 로그온: 마지막 사용자 이름 표시 안 함 → 사용
점검 및 조치 사례	

■ **Windows NT**

Step 1) 시작> 프로그램> 관리도구> 시스템 정책 편집기> 파일> 레지스트리 열기> 로컬 컴퓨터> 편집> 등록 정보> Windows NT 시스템> 로그온> "마지막으로 로그온한 사용자 이름 표시 안함"을 설정한 후 저장



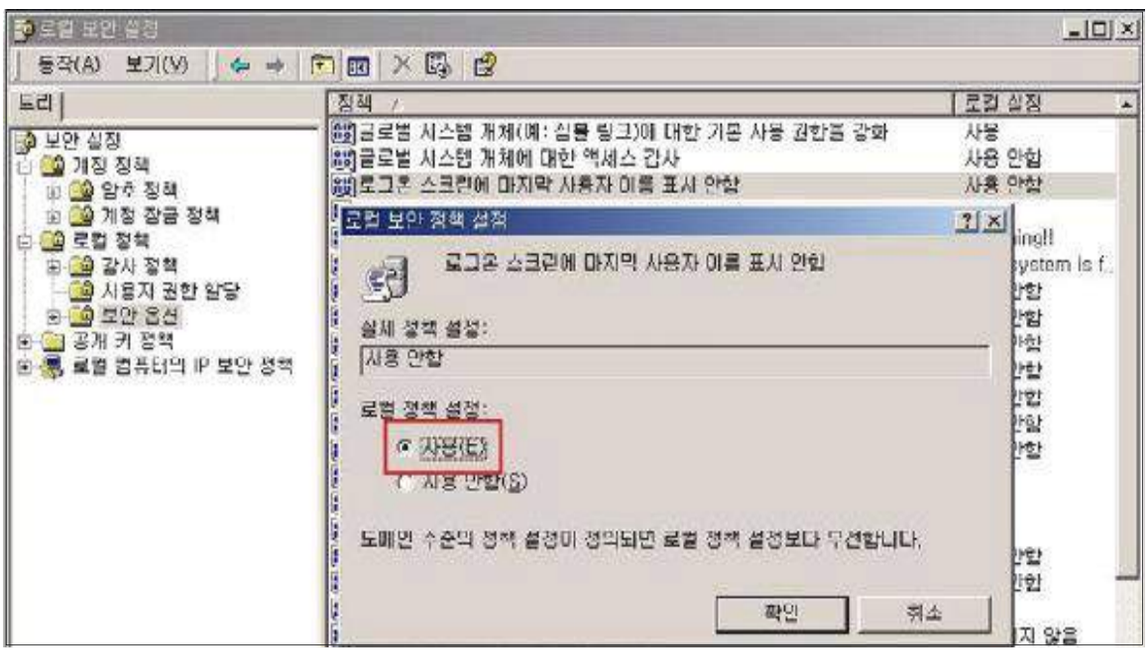
Windows 서버

W-52 (중)	1. 계정관리 > 1.13 마지막 사용자 이름 표시 안 함

■ **Windows 2000**

Step 1) 시작> 실행> SECPOL.MSC> 로컬 정책> 보안 옵션

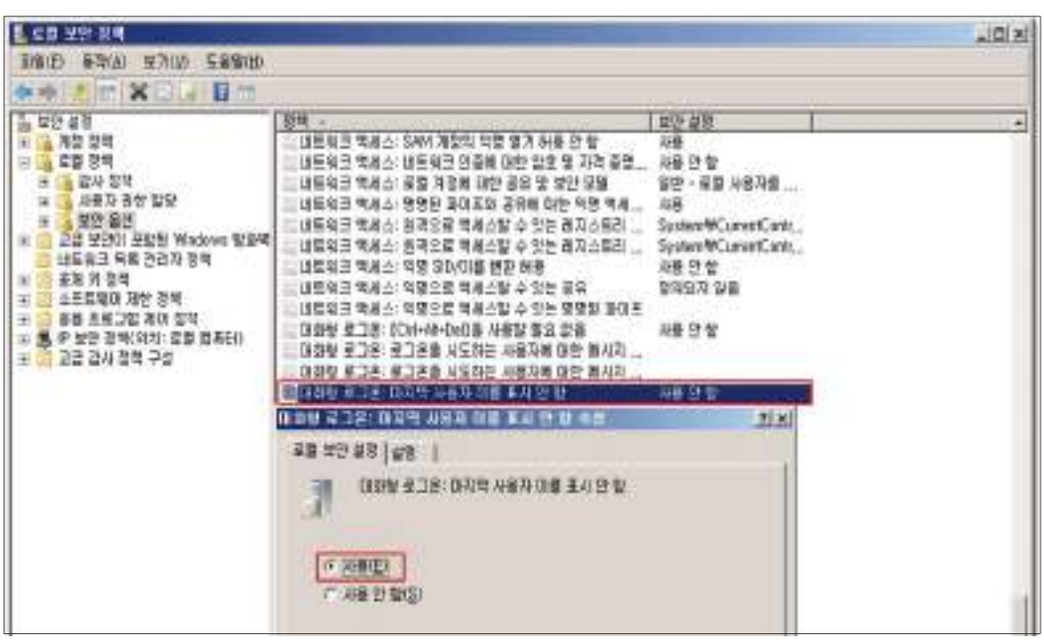
Step 2) "로그온 스크린에 마지막 사용자 이름 표시 안함"을 "사용"으로 설정



■ **Windows 2003, 2008, 2012**

Step 1) 시작> 실행> SECPOL.MSC> 로컬 정책> 보안 옵션

Step 2) "대화형 로그온: 마지막 사용자 이름 표시 안 함"을 "사용"으로 설정



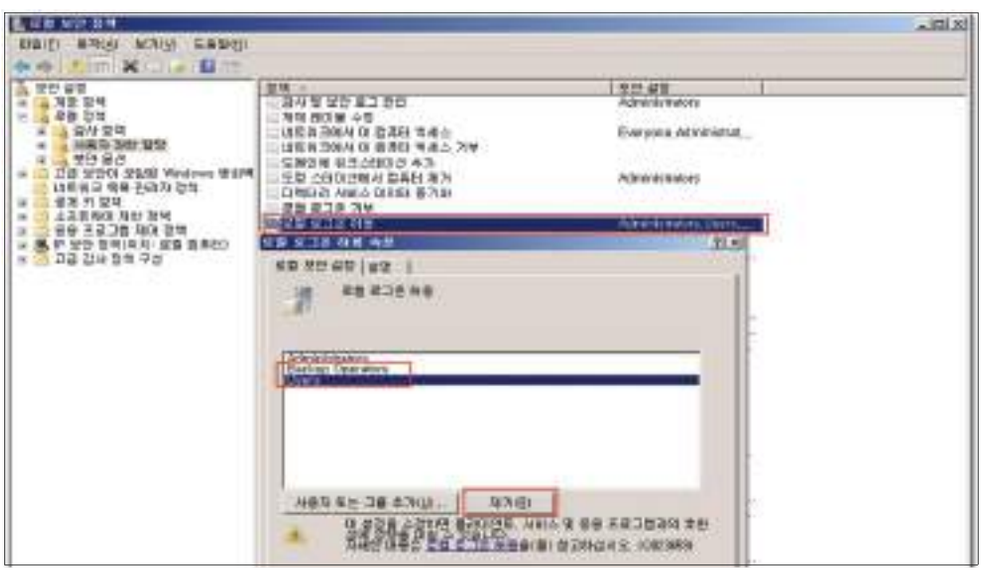
조치 시 영향	일반적인 경우 영향 없음

W-53 (중)	1. 계정관리 > 1.14 로컬 로그온 허용
취약점 개요	
점검내용	■ 불필요한 계정의 로컬 로그온을 허용 여부 점검
점검목적	■ 불필요한 계정에 로컬 로그온이 허용된 경우를 찾아 비인가자의 불법적인 시스템 로컬 접근을 차단하고자 함
보안위협	■ 불필요한 사용자에게 로컬 로그온이 허용된 경우 비인가자를 통한 권한 상승을 위한 악성 코드의 실행 우려가 있음
참고	※ "로컬로 로그온 허용" 권한은 시스템 콘솔에 로그인을 허용하는 권한으로 반드시 콘솔 접근이 필요한 사용자 계정에만 해당 권한을 부여하여야 함 ※ IIS 서비스를 사용할 경우 이 권한에 IUSR_<ComputerName> 계정을 할당함
점검대상 및 판단기준	
대상	■ Windows NT, 2000, 2003, 2008, 2012
판단기준	**양호 :** 로컬 로그온 허용 정책에 Administrators, IUSR_ 만 존재하는 경우
	취약 : 로컬 로그온 허용 정책에 Administrators, IUSR_ 외 다른 계정 및 그룹이 존재하는 경우
조치방법	Administrators, IUSR_ 외 다른 계정 및 그룹의 로컬 로그온 제한
점검 및 조치 사례	

■ **Windows NT, 2000, 2003, 2008, 2012**

Step 1) 시작> 실행> SECPOL.MSC> 로컬 정책> 사용자 권한 할당

Step 2) "로컬 로그온 허용(또는, 로컬 로그온)" 정책에 "Adminstrators", "IUSR_" 외 다른 계정 및 그룹 제거



조치 시 영향	Administrators, IUSR_ 계정 외 로컬에서 접속이 필요한 계정 삭제 시 사용중인 서비스에 장애를 줄 수 있음

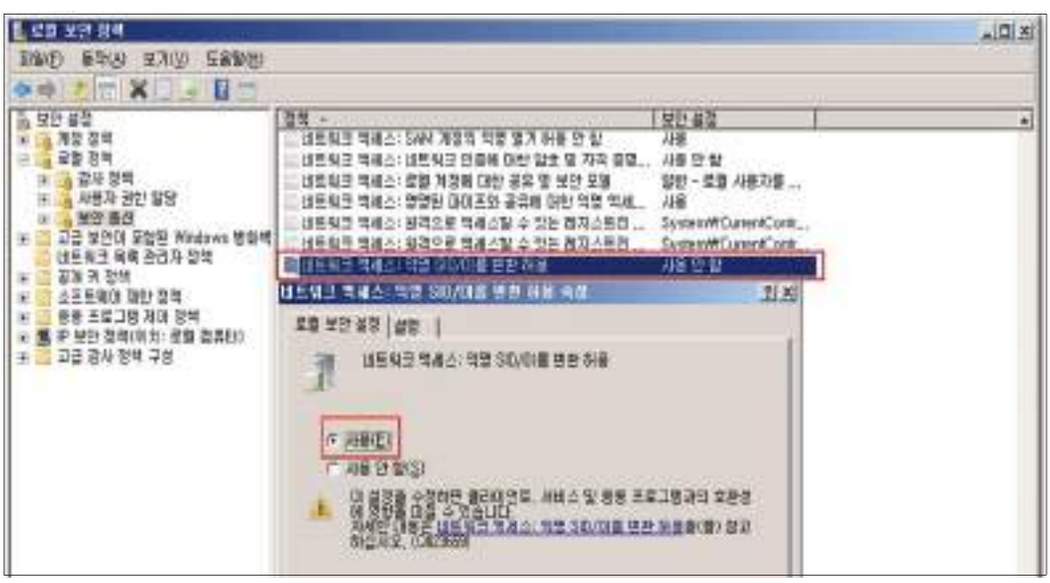
Windows 서버

W-54 (중)	1. 계정관리 > 1.15 익명 SID/이름 변환 허용 해제
취약점 개요	
점검내용	■ 익명 SID/이름 변환 정책 적용 여부 점검
점검목적	■ 익명 SID/이름 변환 정책을 "사용 안 함"으로 설정하여, SID(보안식별자)를 사용하여 관리자 이름을 찾을 수 없도록 하기 위함
보안위협	■ 이 정책이 "사용함"으로 설정된 경우 로컬 접근 권한이 있는 사용자가 잘 알려진 Administrator SID를 사용하여 Administrator 계정의 실제 이름을 알아낼 수 있으며 암호 추측 공격을 실행할 수 있음
참고	※ 이 정책이 설정된 경우 익명 사용자가 다른 사용자의 SID(보안식별자) 특성을 요청할 수 있음 ※ "사용 안 함"으로 정책을 설정할 경우 Windows NT 도메인 환경에서 통신이 불가능하게 될 수 있음
점검대상 및 판단기준	
대상	■ Windows 2003, 2008, 2012
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
점검 및 조치 사례	

■ **Windows 2003, 2008, 2012**

Step 1) 시작> 실행> SECPOL.MSC> 로컬 정책> 보안 옵션

Step 2) "네트워크 액세스: 익명 SID/이름 변환 허용" 정책이 "사용 안 함"으로 설정



※ Windows Server 2000 이하 버전 해당 사항 없음

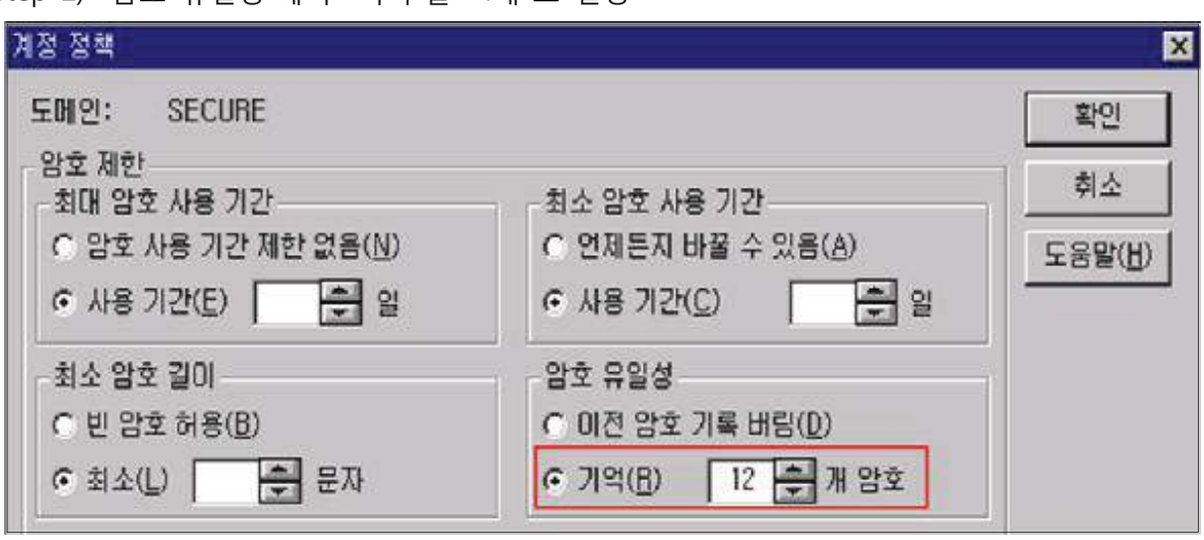
조치 시 영향	일반적인 경우 영향 없음

W-55 (중)	1. 계정관리 > 1.16 최근 암호 기억
취약점 개요	
점검내용	■ 최근 암호 기억 정책 설정 여부 점검
점검목적	■ 사용자가 현재 암호 또는 최근에 사용했던 암호와 동일한 새 암호를 만드는 것을 방지하기 위함
보안위협	■ 최근 암호 기억 정책이 설정되지 않은 경우 특정 계정에 동일한 암호를 오랫동안 사용하는 것이 가능하여 공격자가 무작위 공격을 통해 패스워드 정보 노출 가능성이 커짐
참고	※ 사용자가 현재 암호 또는, 최근에 사용했던 암호와 똑같은 새 암호로 설정할 수 없도록 하여야 함 ※ 이 정책은 암호정책 중 하나로 W-51(중) '패스워드 최소 사용 기간' 정책과 같이 적용될 경우 보안성이 훨씬 강화됨 ※ 관련 점검 항목 : W-48(중), W-49(중), W-50(중), W-51(중)
점검대상 및 판단기준	
대상	■ Windows NT, 2000, 2003, 2008, 2012
판단기준	**양호 :** 최근 암호 기억이 4개 이상으로 설정되어 있는 경우
	취약 : 최근 암호 기억이 4개 미만으로 설정되어 있는 경우
조치방법	최근 암호 기억이 4개 이상으로 설정되어 있는 경우
점검 및 조치 사례	

■ **Windows NT**

Step 1) 시작> 프로그램> 관리도구> 도메인 사용자 관리자> 정책> 계정

Step 2) "암호 유일성"에서 "기억"을 "4개"로 설정



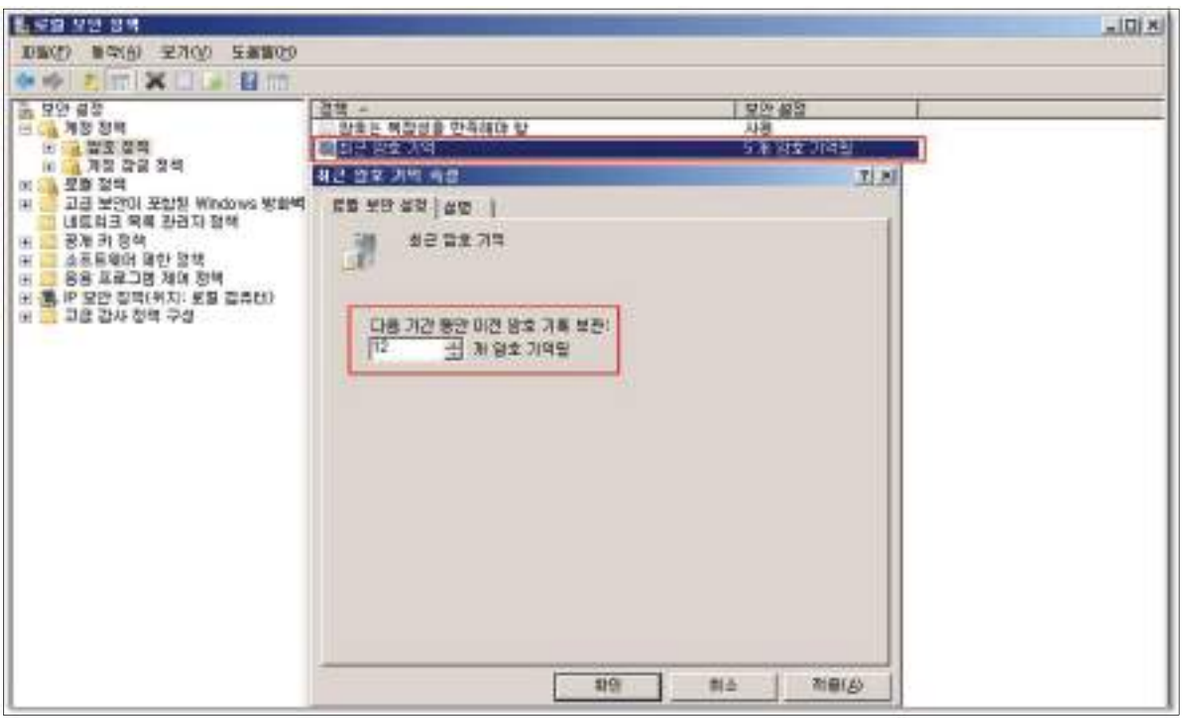
Windows 서버

W-55 (중)	1. 계정관리 > 1.16 최근 암호 기억

■ **Windows 2000, 2003, 2008, 2012**

Step 1) 시작> 실행> SECPOL.MSC> 계정정책> 암호 정책

Step 2) "최근 암호 기억"을 "4개 암호 기억됨"으로 설정



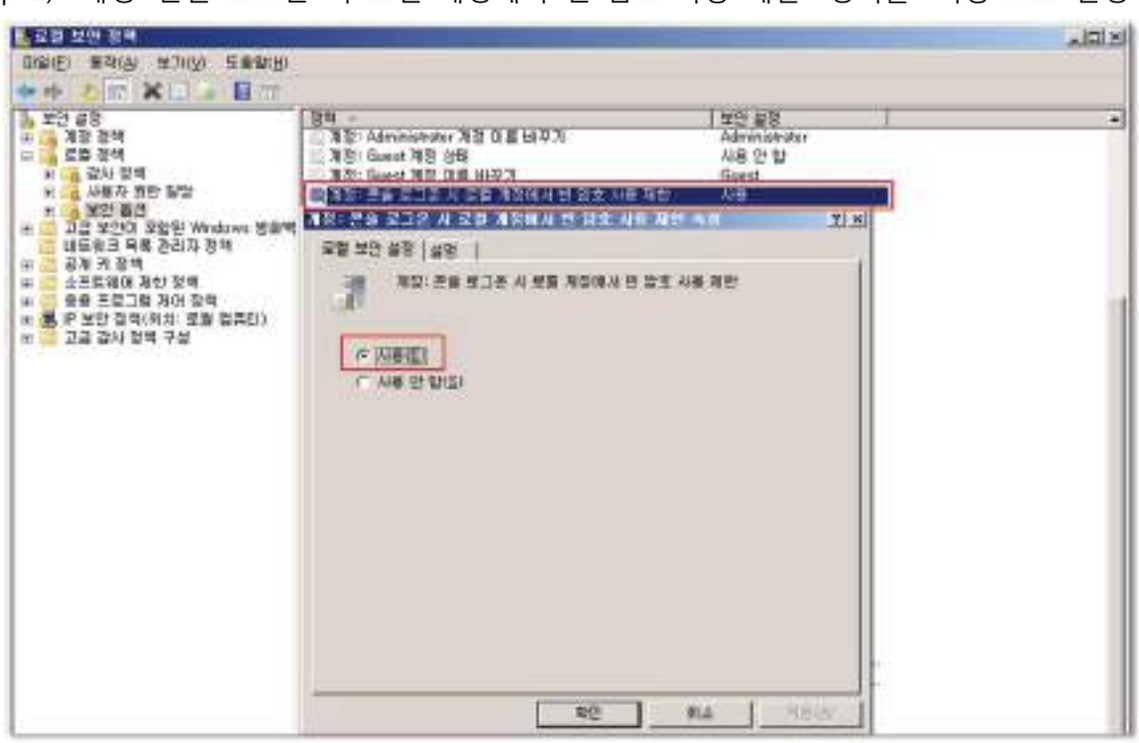
조치 시 영향	일반적인 경우 영향 없음

W-56 (중)	1. 계정관리 > 1.17 콘솔 로그온 시 로컬 계정에서 빈 암호 사용 제한
취약점 개요	
점검내용	■ 콘솔 로그인 시 빈 암호 사용 가능 여부 점검
점검목적	■ 빈 암호를 가진 계정의 콘솔 및 네트워크 서비스 접근을 차단하기 위함
보안위협	■ 이 정책이 "사용 안 함"으로 설정된 경우 빈 암호를 가진 로컬 계정에 대하여 터미널 서비스(원격 데스크톱 서비스), Telnet 및 FTP와 같은 네트워크 서비스의 원격 대화형 로그온이 가능하여, 시스템 보안에 심각한 위험을 줄 수 있음
참고	※ 윈도우 원격 제어(mstsc)는 보안상 계정에 암호가 걸린 계정만 접속하도록 하고 있으나 이 정책을 활성화하면 계정에 암호가 걸려 있지 않아도 원격 제어가 가능함
점검대상 및 판단기준	
대상	■ Windows 2003, 2008, 2012
판단기준	**양호 :** "콘솔 로그온 시 로컬 계정에서 빈 암호 사용 제한" 정책이 "사용"인 경우
	취약 : "콘솔 로그온 시 로컬 계정에서 빈 암호 사용 제한" 정책이 "사용 안 함"인 경우
조치방법	계정: 콘솔 로그온 시 로컬 계정에서 빈 암호 사용 제한 → 사용
점검 및 조치 사례	

■ **Windows 2003, 2008, 2012**

Step 1) 시작> 실행> SECPOL.MSC> 로컬 정책> 보안 옵션

Step 2) "계정: 콘솔 로그온 시 로컬 계정에서 빈 암호 사용 제한" 정책을 "사용"으로 설정



조치 시 영향	일반적인 경우 영향 없음

Windows 서버

W-57 (중)	1. 계정관리 > 1.18 원격터미널 접속 가능한 사용자 그룹 제한
취약점 개요	
점검내용	■ 원격터미널 사용자 그룹 내 비인가자 포함 여부 점검
점검목적	■ 비인가자의 원격터미널 접속을 제한하기 위함
보안위협	■ 원격터미널의 그룹이나 계정을 제한하지 않으면 임의의 사용자가 원격으로 접속하여 해당 서버에 정보를 변경하거나 정보가 유출될 가능성이 있으므로 사용자 그룹과 계정을 설정하여 접속을 제한하여야 함
참고	※ 컴퓨터 관리 > 로컬 사용자 및 그룹 > Remote Desktop Users 그룹에서 추가 가능
점검대상 및 판단기준	
대상	■ Windows 2003, 2008, 2012
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
점검 및 조치 사례	

■ **Windows 2003**

Step 1) 제어판> 사용자 계정> 관리자 계정 이외의 계정 생성한 후

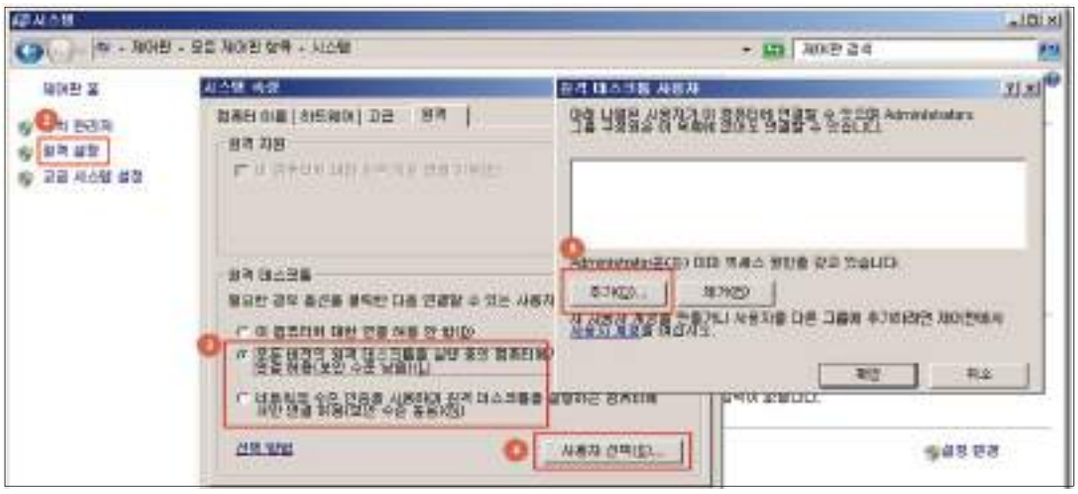
Step 2) 제어판> 시스템> [원격] 탭> [원격] 탭 메뉴에서 "사용자가 이 컴퓨터에 원격으로 연결할 수 있음"에 체크> "원격 사용자 선택"에서 원격 사용자 지정 후 확인

■ **Windows 2008**

Step 1) 제어판> 사용자 계정> 관리자 계정 이외의 계정 생성한 후

Step 2) 제어판> 시스템> 원격 설정> [원격] 탭> [원격 데스크톱] 메뉴> "모든 버전의 원격 데스크톱을 실행 중인 컴퓨터에서 연결 허용(보안 수준 낮음)" 또는 "네트워크 수준 인증을 사용하여 원격 데스크톱을 실행하는 컴퓨터에서만 연결 허용(보안 수준 높음)" 중 하나에 체크> "사용자 선택" 에서 원격 사용자 지정 후 확인

W-57 (중)	1. 계정관리 > 1.18 원격터미널 접속 가능한 사용자 그룹 제한



■ **Windows 2012**

Step 1) 제어판> 사용자 계정> 관리자 계정 이외의 계정 생성한 후

Step 2) 제어판> 시스템> 원격 설정> [원격] 탭> [원격 데스크톱] 메뉴> "이 컴퓨터에 대한 원격 연결 허용" 에 체크> "사용자 선택" 에서 원격 사용자 지정 후 확인

조치 시 영향	일반적인 경우 영향 없음

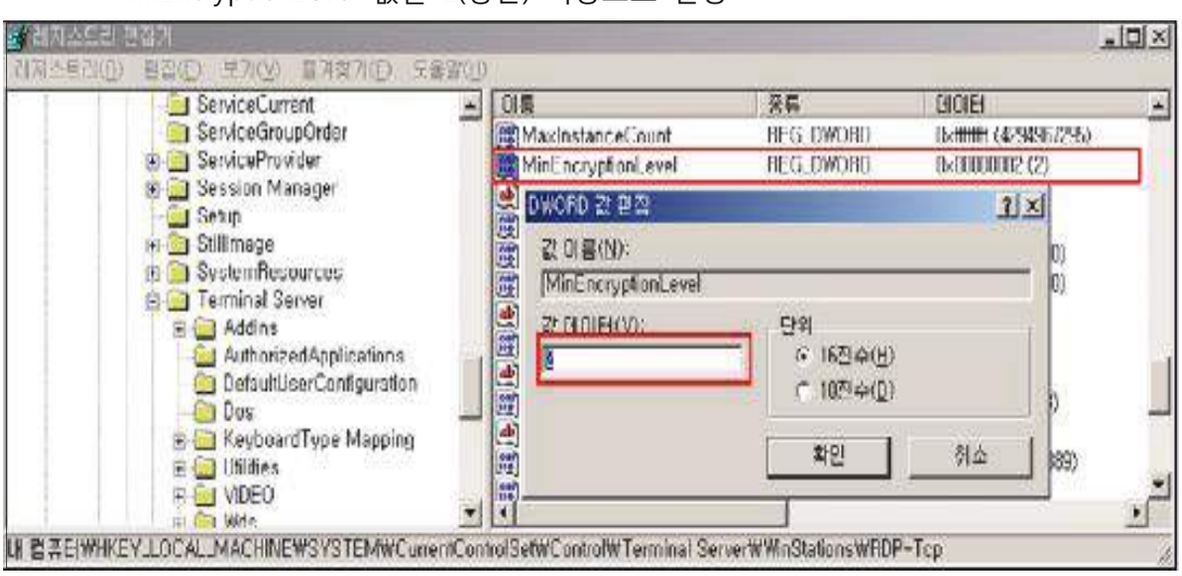
Windows 서버

W-58 (중)	2. 서비스 관리 > 2.26 터미널 서비스 암호화 수준 설정
취약점 개요	
점검내용	■ 터미널 서비스 암호화 수준 적절성 점검
점검목적	■ 터미널 서비스 암호화 설정으로 데이터를 암호화하여 클라이언트와 서버간의 통신에서 전송되는 데이터를 보호하기 위함
보안위협	■ 서버 접속 시에 낮은 암호화 수준을 적용할 경우 악의적인 사용자에 의해 서버와 클라이언트간 주고받는 정보가 노출될 우려가 있음
참고	※ 기반시설 시스템은 터미널 서비스의 사용을 원칙적으로 금지하나, 부득이 해당 서비스를 사용해야 하는 경우 클라이언트 서버간의 데이터 전송 시 암호화하여 보호해야 함
점검대상 및 판단기준	
대상	■ Windows NT, 2000, 2003, 2008, 2012
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	터미널 서비스의 가동을 '중지' 및 '사용 안 함' 설정을 하거나, 부득이 사용할 경우 암호화 수준 설정 적용
점검 및 조치 사례	

■ **Windows NT**

Step 1) 시작> 실행> regedit

Step 2) HKLM₩SYSTEM₩CurrentControlSet₩Control₩Terminal Server₩WinStations₩RDP-Tcp ₩MinEncryptionLevel 값을 2(중간) 이상으로 설정



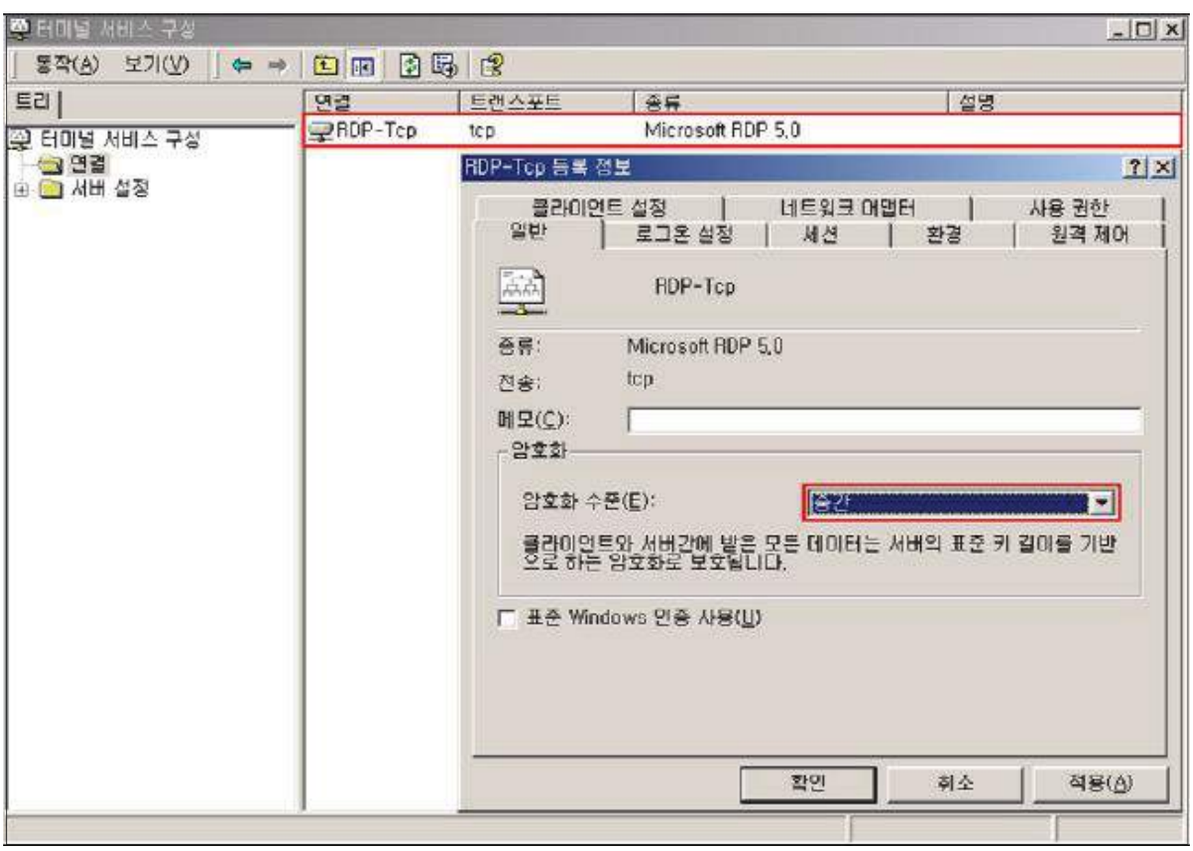
W-58 (중)	2. 서비스 관리 > 2.26 터미널 서비스 암호화 수준 설정

■ **Windows 2000**

Step 1) 시작> 실행> TSCC.MSC> "해당 서비스" 선택> 속성

Step 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



■ **Windows 2003, 2008, 2012**

Step 1) Windows 2003: 시작> 실행> TSCC.MSC> "해당 서비스" 선택> 속성

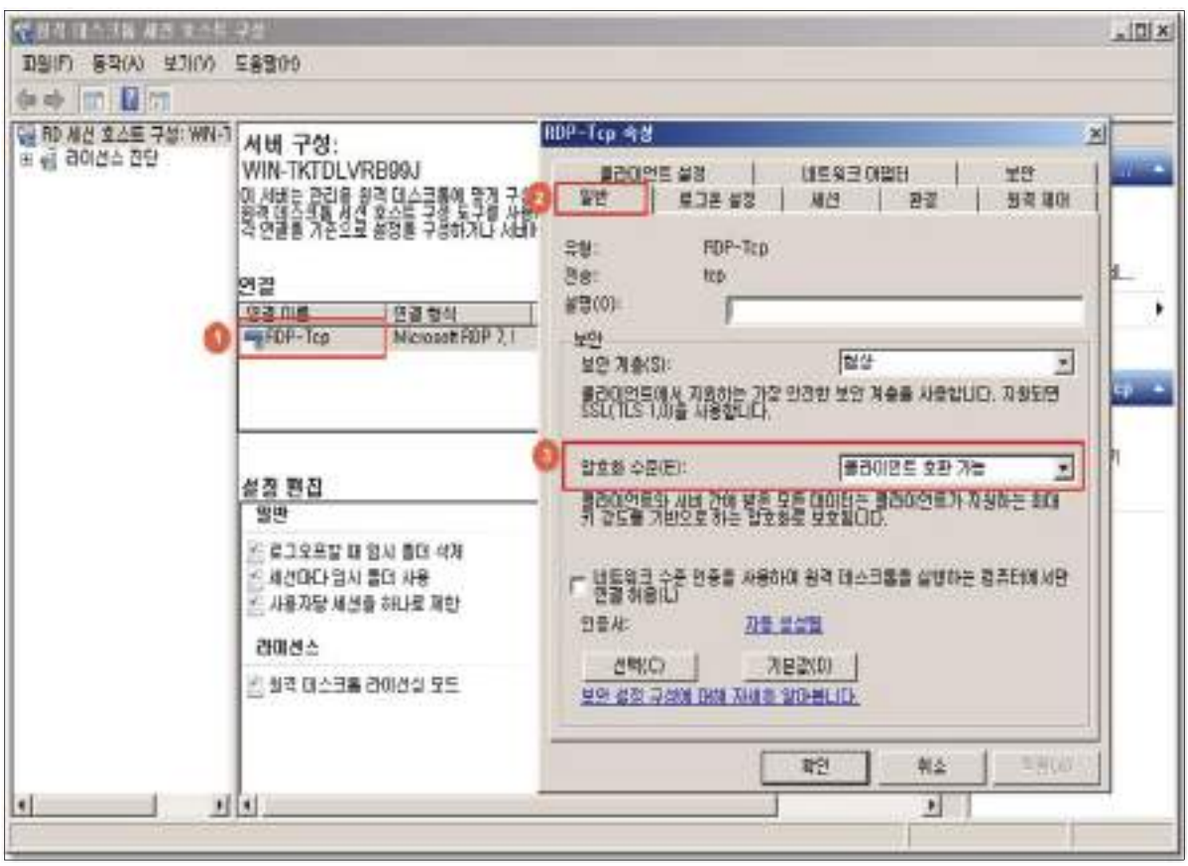
Windows 2008, 2012: 시작> 관리 도구> 원격 데스크톱 서비스> 원격 데스크톱 세션 호스트 구성> RDP-Tcp 속성

Step 2) [일반] 탭에서 암호화 수준 설정 → 클라이언트 호환 가능(Windows 2003, 2008, 2012)

Windows 서버

W-58 (중)	2. 서비스 관리 > 2.26 터미널 서비스 암호화 수준 설정

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 보호하며 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



※ 터미널 서비스가 필요한 경우 추가 보완 대책

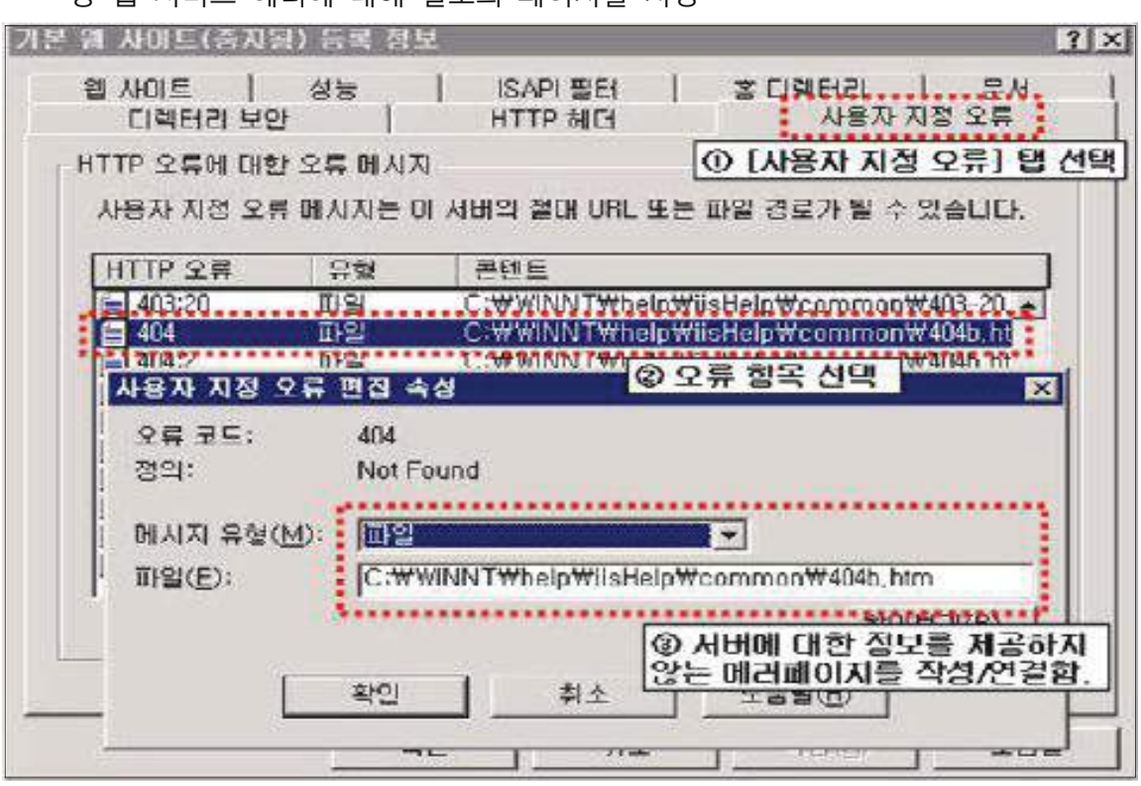
1. 관리자 이외의 일반 사용자의 터미널 서비스 접속을 허용하지 않음
2. 방화벽에서 터미널 서비스 포트(3389)의 사용을 관리자 컴퓨터의 IP로 제한

조치 시 영향	암호화 수준 변경 시 일반적으로 영향 없음

W-59 (중)	2. 서비스 관리 > 2.27 IIS 웹서비스 정보 숨김
취약점 개요	
점검내용	■ IIS 웹서비스 정보 숨김 설정 여부 점검
점검목적	■ IIS 웹서비스 운용 시 에러 페이지, 웹 서버 종류, 사용 OS, 사용자 계정이름 등 웹 서버와 관련된 불필요한 정보가 노출되지 않도록 하기 위함
보안위협	■ IIS 웹서비스 정보 숨김 설정이 적용되지 않은 경우 악의적인 사용자에게 불필요한 정보가 노출되어 외부 공격을 위한 기초 자료로 이용될 수 있음
참고	-
점검대상 및 판단기준	
대상	■ Windows NT, 2000, 2003, 2008, 2012
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
점검 및 조치 사례	

■ **Windows NT, 2000, 2003**

Step 1) 인터넷 정보 서비스(IIS) 관리> 속성> [사용자 지정 오류] 탭에서 400, 401, 403, 404, 500 등 웹 서비스 에러에 대해 별도의 페이지를 지정



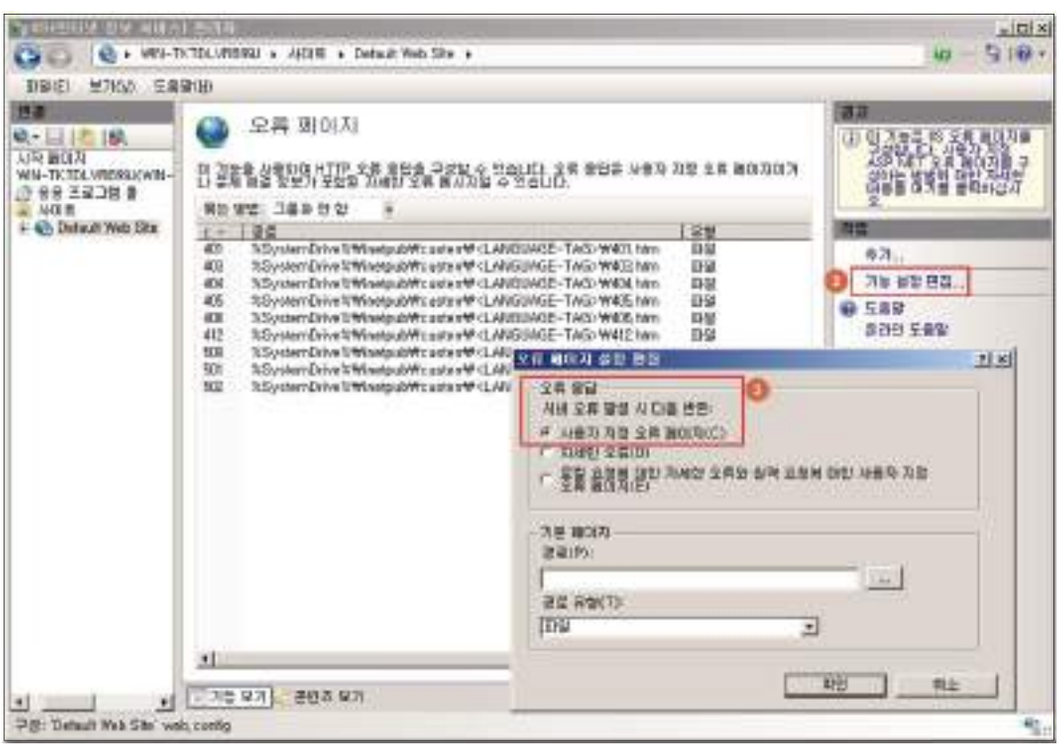
Windows 서버

W-59 (중)	2. 서비스 관리 > 2.27 IIS 웹서비스 정보 숨김

■ **Windows 2008, 2012**

Step 1) 오류 페이지 설정 편집

제어판> 관리도구> 인터넷 정보 서비스(IIS) 관리자> 해당 웹 사이트> [오류 페이지] > [작업] 탭에서 [기능 설정 편집]> "서버오류 발생 시 다음 반환" 항목을 "사용자 지정 오류 페이지"로 설정



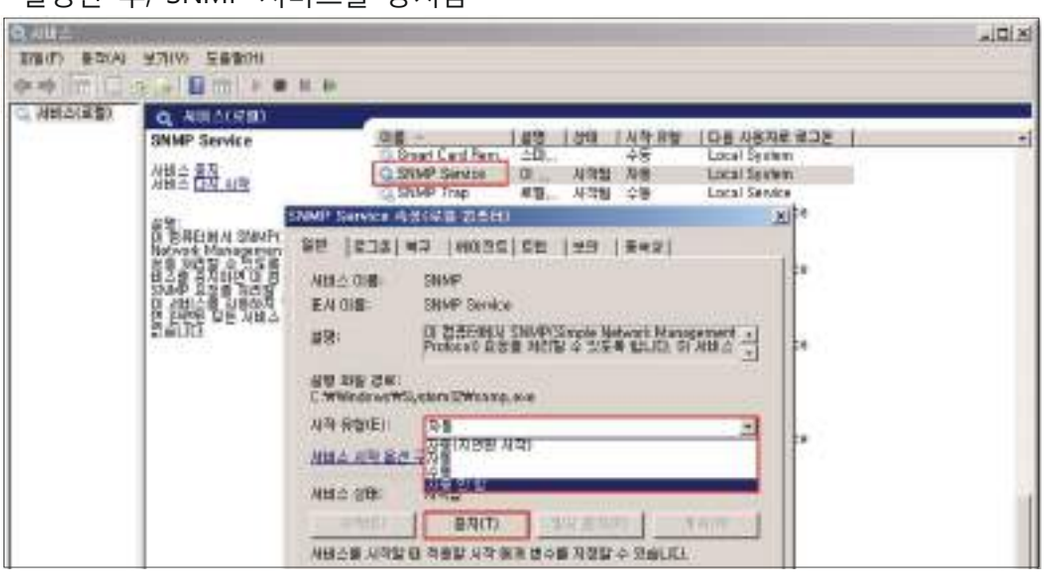
조치 시 영향	일반적인 경우 영향 없음

W-60 (중)	2. 서비스 관리 > 2.28 SNMP 서비스 구동 점검
취약점 개요	
점검내용	■ SNMP 서비스 구동 여부 점검
점검목적	■ 취약한 SNMP 서비스를 비활성화 하여 시스템의 주요정보 유출 및 불법수정을 방지하기 위함
보안위협	■ 취약한 SNMP 서비스를 사용하는 경우 서비스거부공격(DoS, DDoS), 버퍼 오버플로우, 비인가 접속 등의 공격의 위험이 있음
참고	※ **SNMP:** SNMP(Simple Network Management Protocol)는 MIB(Management Information Base)에 기반한 네트워크 망을 관리하기 위한 목적으로 만들어진 프로토콜로, 간단한 명령으로 원격 시스템의 CPU정보에서부터, 인터페이스 트래픽량 등 여러 가지 정보를 확인 가능
점검대상 및 판단기준	
대상	■ Windows 2000, 2003, 2008, 2012
판단기준	**양호 :** SNMP 서비스를 사용하지 않는 경우
	취약 : SNMP 서비스를 사용하는 경우
조치방법	불필요 시 서비스 중지/사용 안 함
점검 및 조치 사례	

■ **Windows 2000, 2003, 2008, 2012**

Step 1) 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 String을 사용하여야 함(서비스> SNMP> 등록 정보> 종속성 참고) ※ NMS(Network Management System): 네트워크 관리 시스템

Windows 서버

W-61 (중)	2. 서비스 관리 > 2.29 SNMP 서비스 커뮤니티스트링의 복잡성 설정
취약점 개요	
점검내용	■ SNMP 서비스 커뮤니티 스트링(Community String) 적절성 점검
점검목적	■ SNMP에서 일종의 패스워드로 사용하는 Community String을 유추할 수 없는 복잡한 값으로 변경하여 불필요한 시스템 정보 노출을 차단하기 위함
보안위협	■ Community String 설정을 변경하지 않고 public, private 등 Default 설정 값으로 사용하는 경우, 기본 String 값을 통한 시스템의 주요 정보 및 설정 상태의 비인가자 노출 위험이 존재
참고	-
점검대상 및 판단기준	
대상	■ Windows NT, 2000, 2003, 2008, 2012
판단기준	**양호 :** SNMP 서비스를 사용하지 않거나 Community String이 public, private이 아닌 경우
	취약 : SNMP 서비스를 사용하며, Community String이 public, private인 경우
조치방법	불필요 시 서비스 중지/사용 안 함, 사용 시 Default Community String 변경
점검 및 조치 사례	

■ **Windows NT**

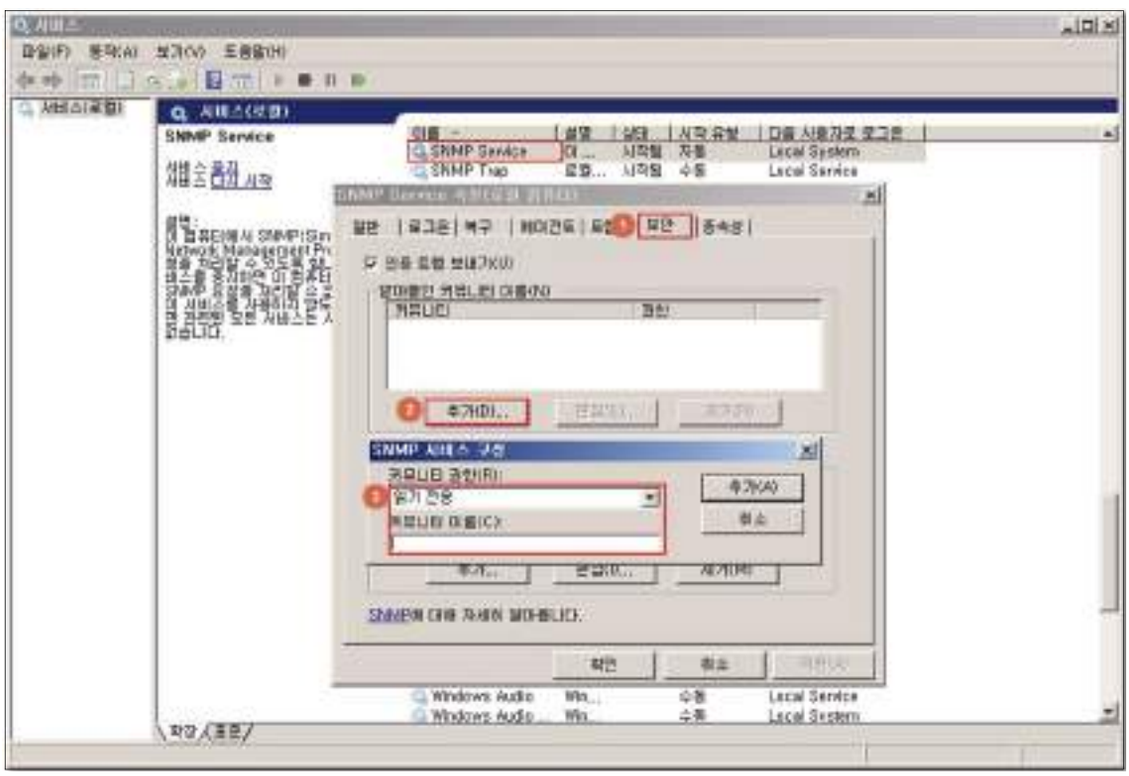
Step 1) 바탕화면> 네트워크 환경> 등록 정보> 서비스/SNMP Service> 등록 정보> 보안

W-61 (중)	2. 서비스 관리 > 2.29 SNMP 서비스 커뮤니티스트링의 복잡성 설정

■ **Windows 2000, 2003, 2008, 2012**

Step 1) 시작> 실행> SERVICES.MSC> SNMP Service> 속성> 보안> [인증 트랩 보내기] 아래 [추가] 버튼>

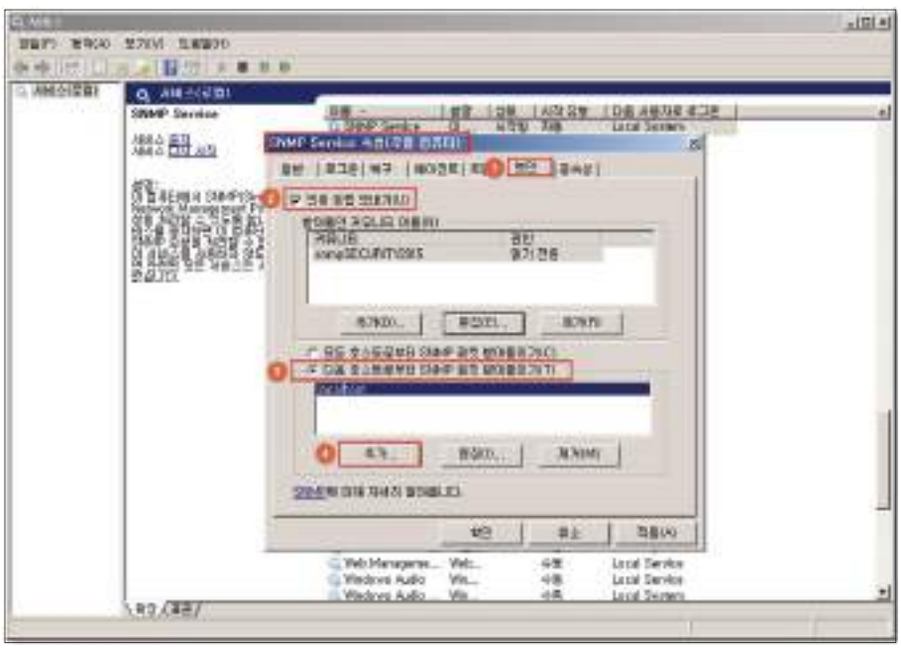
Step 2) [SNMP 서비스 구성]> 쓰기 권한이 필요하지 않다면 커뮤니티 이름을 읽기 전용 으로 Public/Private이 아닌 이름을 추가(NT의 경우 시작> 제어판> 서비스에서 설정)



Step 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 String을 사용하여야 함.(서비스> SNMP> 등록 정보> 종속성 참고)

Windows 서버

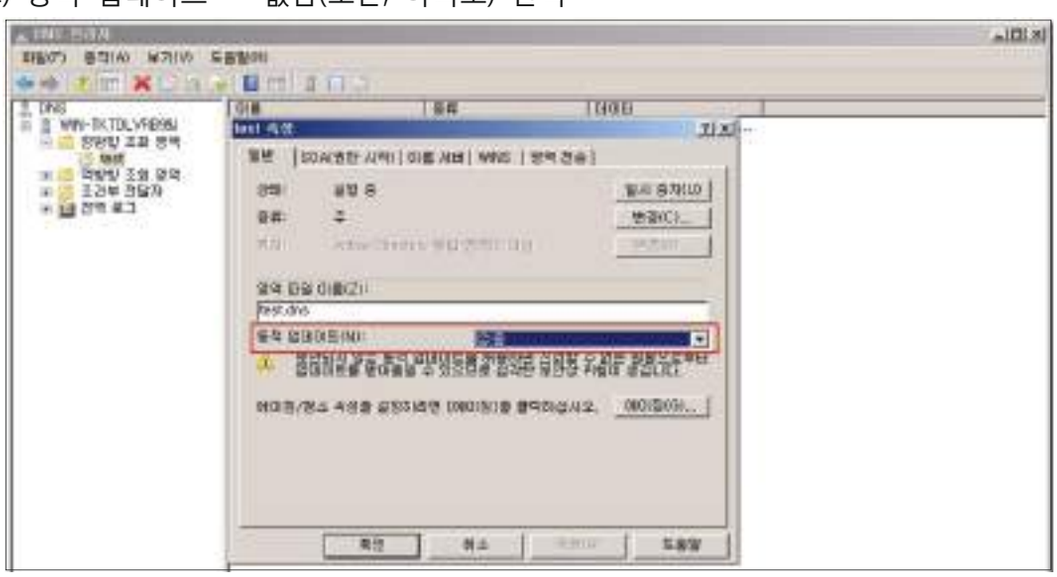
W-62 (중)	2. 서비스 관리 > 2.30 SNMP Access control 설정
취약점 개요	
점검내용	■ SNMP 패킷 접근 제어 설정 여부 점검
점검목적	■ SNMP 트래픽에 대한 접근 제어 설정을 하여 내부 네트워크로부터의 악의적인 공격을 차단하기 위함
보안위협	■ SNMP Access control 설정을 적용하지 않아 인증되지 않은 내부 서버로부터의 SNMP 트래픽을 차단하지 않을 경우, 장치 구성 변경, 라우팅 테이블 조작, 악의적인 TFTP 서버 구동 등의 SNMP 공격에 노출될 수 있음
참고	※ SNMP(v1, v2c)에서 클라이언트와 데몬간의 get_request(요청)와 get_response(응답) 과정은 암호화가 아닌 평문으로 전송되므로 스니핑(sniffing)이 가능함 ※ SNMP v3의 경우 인증을 위해 암호화가 제공
점검대상 및 판단기준	
대상	■ Windows 2000, 2003, 2008, 2012
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 SNMP 패킷 수령 호스트 지정
점검 및 조치 사례	
■ **Windows 2000, 2003, 2008, 2012** Step 1) 시작> 실행> SERVICES.MSC> SNMP Service> 속성> 보안 Step 2) "인증 트랩 보내기" 및 "다음 호스트로부터 SNMP 패킷 받아들이기" 선택 Step 3) SNMP 호스트 등록 	
조치 시 영향	일반적인 경우 영향 없음

W-63 (중)	2. 서비스 관리 > 2.31 DNS 서비스 구동 점검
취약점 개요	
점검내용	■ DNS 서비스의 동적 업데이트 설정 여부 점검
점검목적	■ DNS 동적 업데이트를 비활성화 함으로 신뢰할 수 없는 원본으로부터 업데이트를 받아들이는 위험을 차단하기 위함
보안위협	■ DNS 서버에서 동적 업데이트를 사용할 경우 악의적인 사용자에 의해 신뢰할 수 없는 데이터가 받아들여질 위험이 존재함
참고	※ **동적 업데이트:** 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
점검대상 및 판단기준	
대상	■ Windows 2000, 2003, 2008, 2012
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
점검 및 조치 사례	

■ **Windows 2000, 2003, 2008, 2012**

Step 1) 시작> 실행> DNSMGMT.MSC> 각 조회 영역> 해당 영역> 속성> 일반

Step 2) 동적 업데이트 → 없음(또는, 아니오) 선택



Step 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	일반적인 경우 영향 없음

Windows 서버

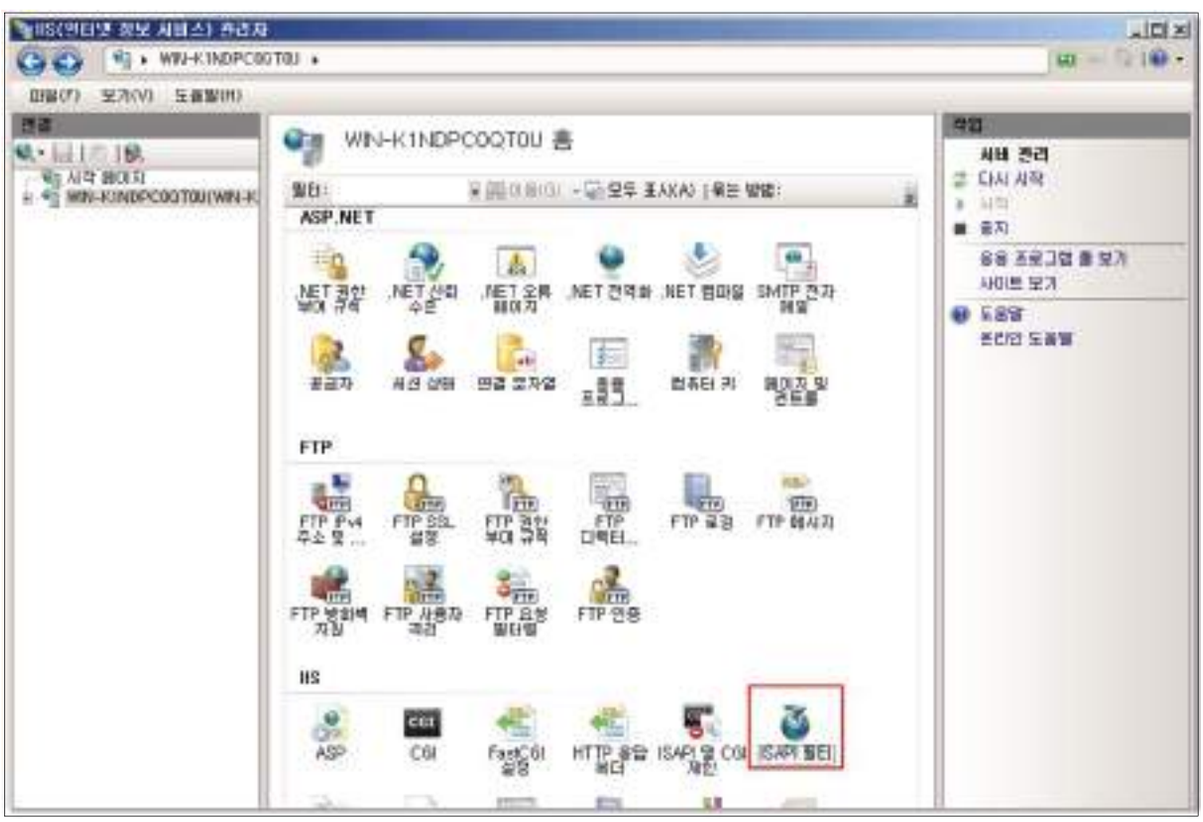
W-64 (하)	2. 서비스 관리 > 2.32 HTTP/FTP/SNMP 배너 차단
취약점 개요	
점검내용	■ HTTP/FTP/SNMP 서비스 배너 차단 적용 여부 점검
점검목적	■ HTTP/FTP/SNMP 서비스 접속 배너를 통한 불필요한 정보 노출을 방지하기 위함
보안위협	■ 서비스 접속 배너가 차단되지 않은 경우 임의의 사용자가 HTTP, FTP, SMTP 접속 시도 시 노출되는 접속 배너 정보를 수집하여 악의적인 공격에 이용할 수 있음
참고	-
점검대상 및 판단기준	
대상	■ Windows NT, 2000, 2003, 2008, 2012
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
점검 및 조치 사례	

■ **HTTP**

Step 1) Microsoft 다운로드 센터에서 UrlScan을 설치

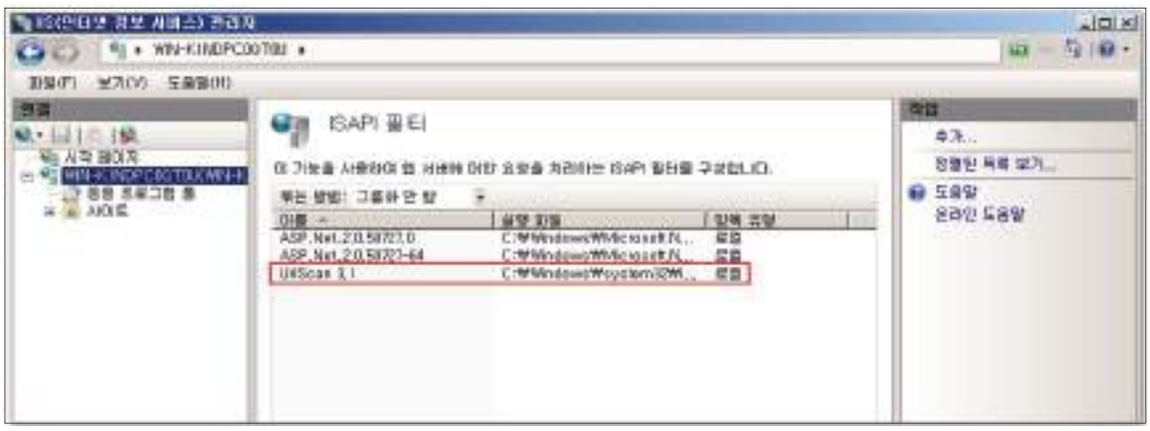
http://www.iis.net/learn/extensions/working-with-urlscan/urlscan-setup

Step 2) IIS관리자> IIS> ISAPI 필터



W-64 (하)	2. 서비스 관리 > 2.32 HTTP/FTP/SNMP 배너 차단

Step 3) 필터 추가 - UrlScan 3.1 - "C₩Windows₩System32₩inetsrv₩urlscan₩urlscan.dll"



Step 4) UrlScal.ini 파일 내 해당 값 변경 "C₩Windows₩System32₩inetsrv₩urlscan₩urlscan.ini"

- RemoteserverHeader=1
- AllowDotInPath=1

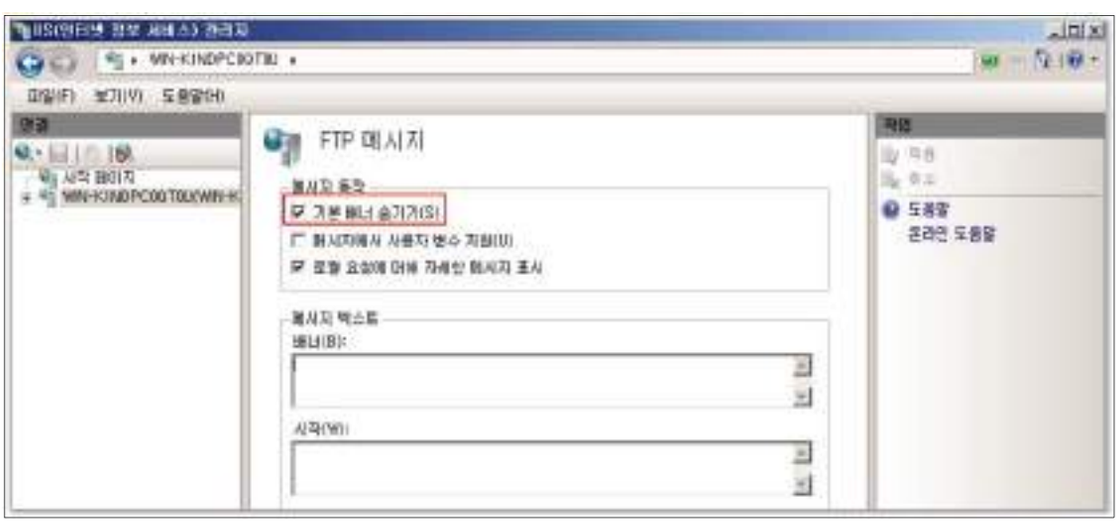
```
AllowHighBitCharacters=0        ; If 1, allow high bit (ie. UTF8 or MBCS)
                                ; characters in URL.  The default is 0.

AllowDotInPath=1                ; If 1, allow dots that are not file
                                ; extensions. The default is 0. Note that
                                ; setting this property to 1 will make checks
                                ; based on extensions unreliable and is
                                ; therefore not recommended other than for
                                ; testing.

RemoveServerHeader=1            ; If 1, remove the 'Server' header from
                                ; response.  The default is 0.
```

■ **FTP**

Step 1) IIS 관리자 > FTP 메시지> 기본 배너 숨기기 설정



Windows 서버

W-64 (하)	2. 서비스 관리 > 2.32 HTTP/FTP/SNMP 배너 차단

■ **SMTP**

Step 1) IIS 관리자 > 서버 개체 우클릭 > 메타베이스 직접 편집 허용 설정

※ 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"
```

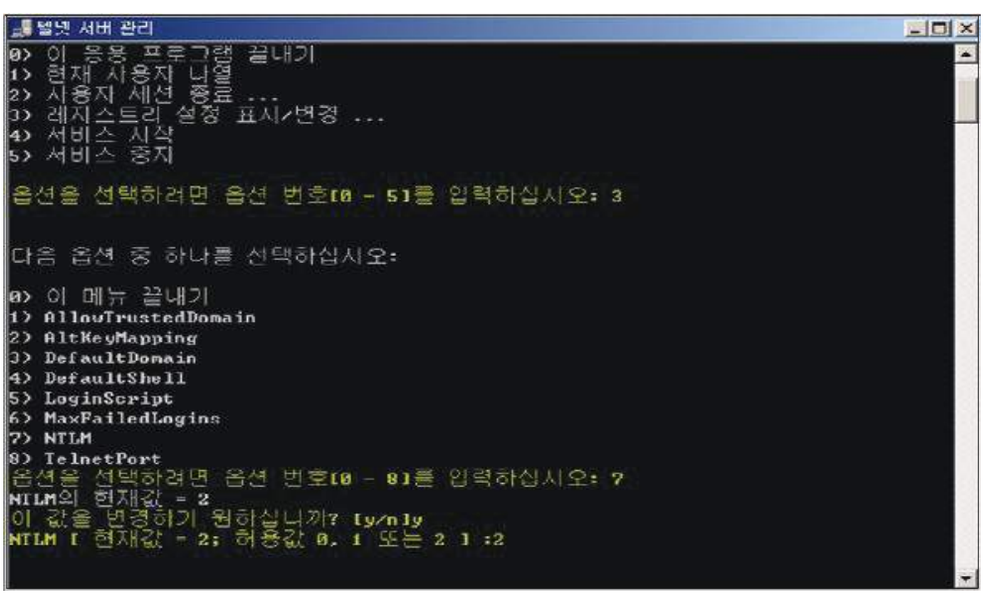
조치 시 영향	일반적인 경우 영향 없음

W-65 (중)	2. 서비스 관리 > 2.33 Telnet 보안 설정
취약점 개요	
점검내용	■ Telnet 서비스 구동 비활성화 및 취약한 인증 사용 여부 점검
점검목적	■ 취약 프로토콜인 Telnet 서비스의 사용을 원칙적으로 금지하고, 부득이 이용할 경우 네트워크상으로 패스워드를 전송하지 않는 NTLM 인증을 사용하도록 하여 인증 정보의 노출을 차단하기 위함
보안위협	■ Telnet 서비스는 평문으로 데이터를 송수신하기 때문에 Password 방식으로 인증을 수행할 경우 ID 및 Password가 외부로 노출될 위험성이 있음
참고	※ Windows 서버의 Telnet 서비스의 두 가지 인증 방법 • **NTLM 인증:** 암호를 전송하지 않고 negotiate/challenge/response 절차로 인증 수행 • **Password 인증:** 관리자 및 Telnet Clients 그룹에 포함된 ID/PW로 인증 수행 ※ 기반시설 시스템에서 Telnet 서비스의 이용은 원칙적으로 금지하나, 조직에서 부득이 유사 기능을 활용해야 하는 경우 SSH를 사용하는 것을 권고함
점검대상 및 판단기준	
대상	■ Windows NT, 2000, 2003, 2008, 2012
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
점검 및 조치 사례	

■ **Windows NT, 2000**

Step 1) 시작> 설정> 제어판> 관리 도구> 텔넷 서버 설정

Step 2) NTLM 인증 방식만 사용



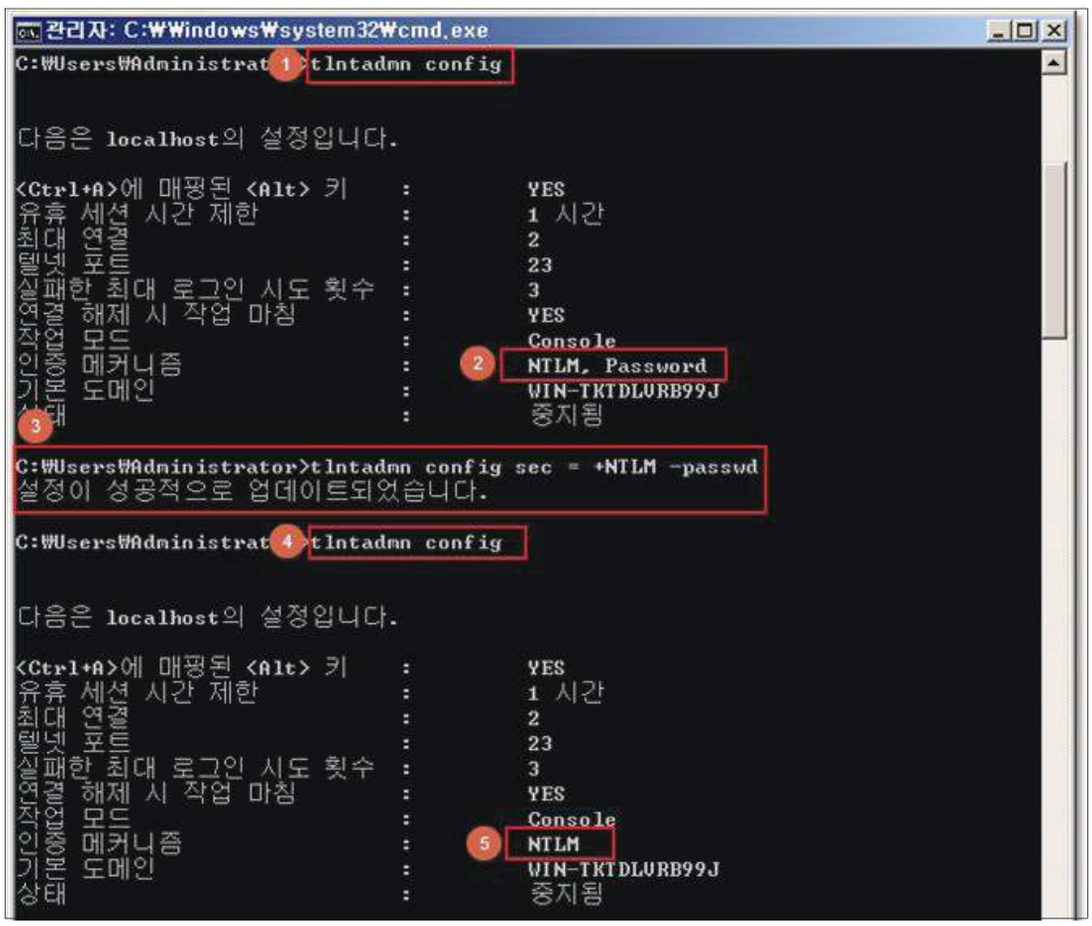
Windows 서버

W-65 (중)	2. 서비스 관리 > 2.33 Telnet 보안 설정

■ **Windows 2003, 2008, 2012**

Step 1) 시작> 실행> cmd> `tlntadmn config`

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



Step 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

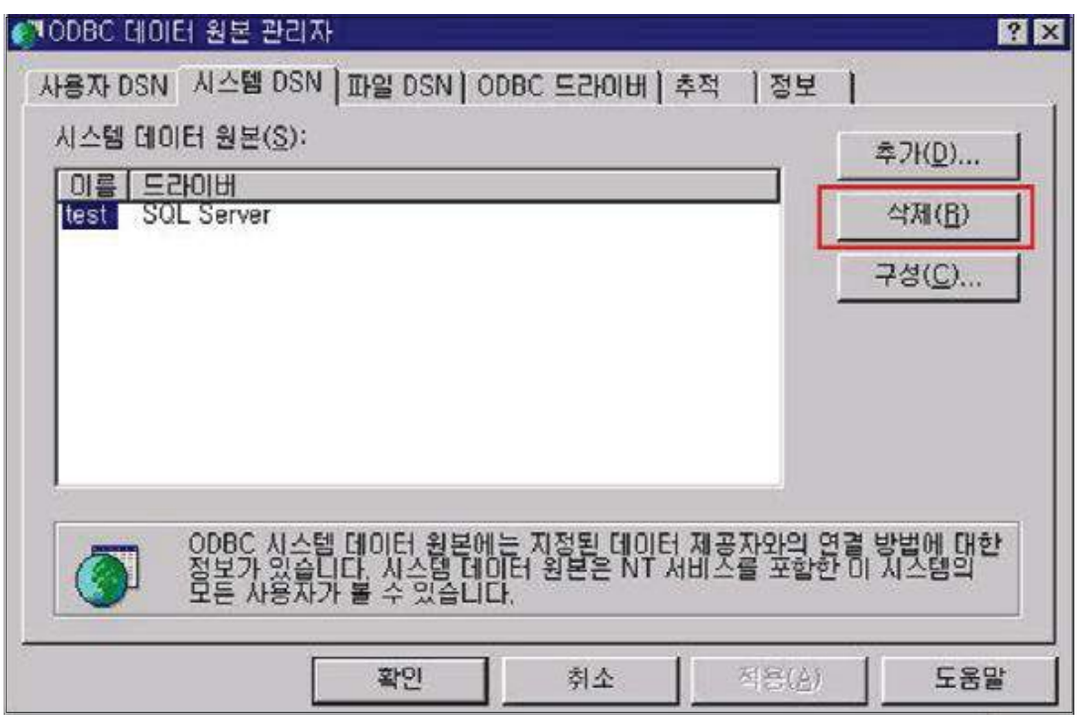
조치 시 영향	일반적인 경우 영향 없음

W-66 (중)	2. 서비스 관리 > 2.34 불필요한 ODBC/OLE-DB 데이터 소스와 드라이브 제거
취약점 개요	
점검내용	■ 불필요한 ODBC/OLE-DB 데이터 소스와 드라이브 제거 여부 점검
점검목적	■ 불필요한 데이터 소스 및 드라이버를 ODBC 데이터 소스 관리자 도구를 이용해 제거하여 비인가자에 의한 데이터베이스 접속 및 자료 유출을 차단하기 위함
보안위협	■ 불필요한 ODBC/OLE-DB 데이터 소스를 통한 비인가자에 의한 데이터베이스 접속 및 자료 유출 위험 존재
참고	※ 특정 샘플 애플리케이션은 샘플 데이터베이스를 위해 ODBC 데이터 소스를 설치하거나 불필요한 ODBC/OLE-DB 데이터베이스 드라이버를 설치하므로 불필요한 데이터 소스나 드라이버는 ODBC 데이터 소스 관리자 도구를 이용해서 제거하는 것이 바람직함
점검대상 및 판단기준	
대상	■ Windows NT, 2000, 2003, 2008, 2012
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
점검 및 조치 사례	

■ **Windows NT**

Step 1) 시작> 설정> 제어판> 데이터 원본(ODBC)> 시스템 DSN> 해당 드라이브 클릭

Step 2) 사용하지 않은 데이터 소스 제거



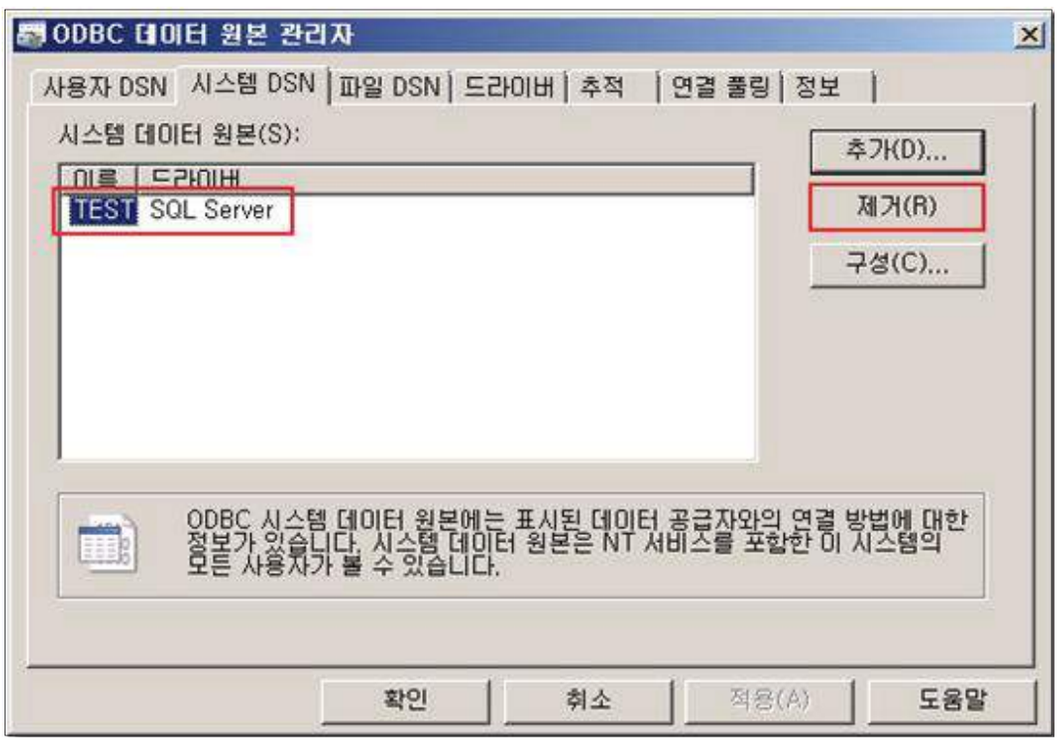
Windows 서버

W-66 (중)	2. 서비스 관리 > 2.34 불필요한 ODBC/OLE-DB 데이터 소스와 드라이브 제거

■ **Windows 2000, 2003, 2008, 2012**

Step 1) 시작> 설정> 제어판> 관리 도구> 데이터 원본(ODBC)> 시스템 DSN> 해당 드라이브 클릭

Step 2) 사용하지 않는 데이터 소스 제거



조치 시 영향	애플리케이션에서 사용할 경우 양호

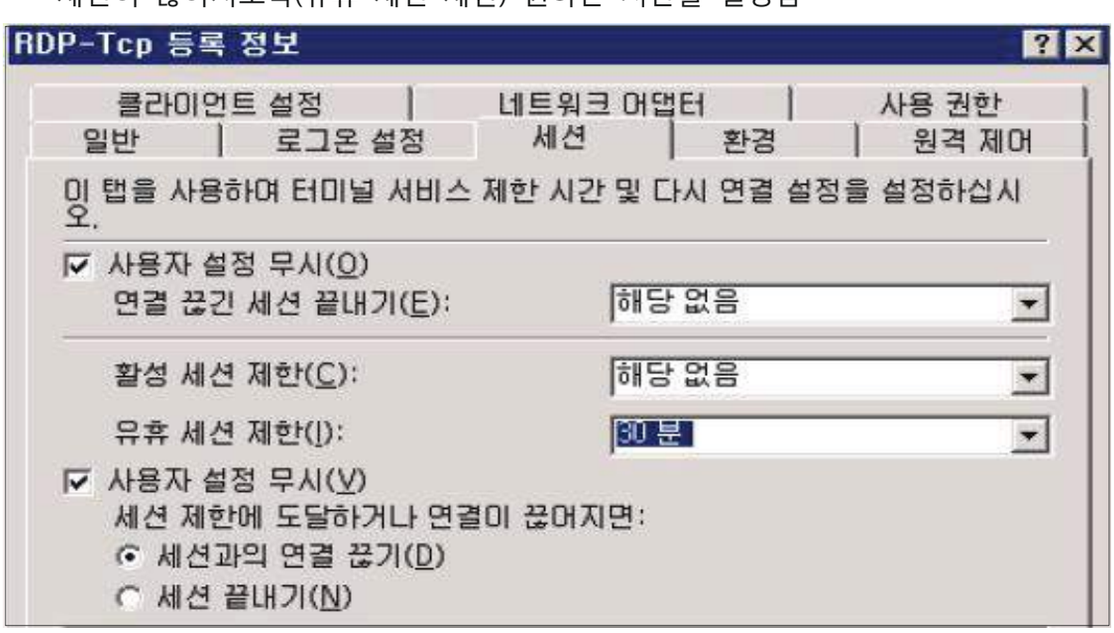
W-67 (중)	2. 서비스 관리 > 2.35 원격터미널 접속 타임아웃 설정
취약점 개요	
점검내용	■ 원격터미널 접속 타임아웃 설정 여부 점검
점검목적	■ 조직에서 부득이 원격터미널 접속을 허용해야 할 경우, 원격터미널 접속 후 일정 시간 동안 이벤트가 발생하지 않은 호스트의 접속을 차단하여 비인가자의 불필요한 접근을 차단하고 정보의 노출을 방지하기 위함
보안위협	■ 접속 타임아웃 값이 설정되지 않은 경우 유휴 시간 내 비인가자의 시스템 접근으로 인해 불필요한 내부 정보의 노출 위험이 존재함
참고	※ 기반시설 시스템에서 원격 터미널 서비스의 이용은 원칙적으로 금지하나, 부득이 해당 기능을 활용해야 하는 경우 접속 타임아웃 설정 등의 보안 조치를 반드시 적용하여야 함
점검대상 및 판단기준	
대상	■ Windows 2000, 2003, 2008, 2012
판단기준	**양호 :** 원격제어 시 Timeout 제어 설정을 적용한 경우
	취약 : 원격제어 시 Timeout 제어 설정을 적용하지 않은 경우
조치방법	Timeout 제어 설정 적용
점검 및 조치 사례	

■ **Windows 2000, 2003, 2008**

Step 1) 시작> 실행> 열기> TSCC.MSC 실행(Windows 2008은 TSCONFIG.MC)

Step 2) RDP-Tcp connection에서 우클릭> 속성 실행

Step 3) [세션] 탭에서 아래 Override user settings(사용자 설정 무시)을 체크하고 Idle session time 세션이 끊어지도록(유휴 세션 제한) 원하는 시간을 설정함



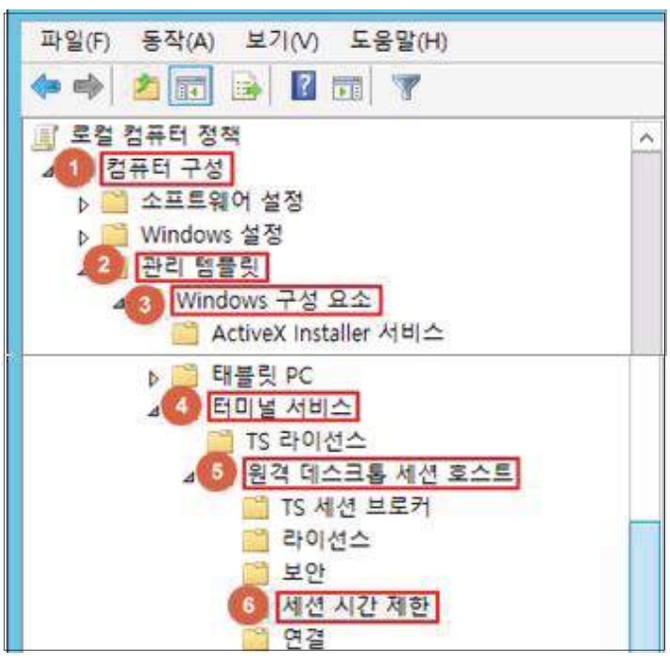
Windows 서버

W-67 (중)	2. 서비스 관리 > 2.35 원격터미널 접속 타임아웃 설정

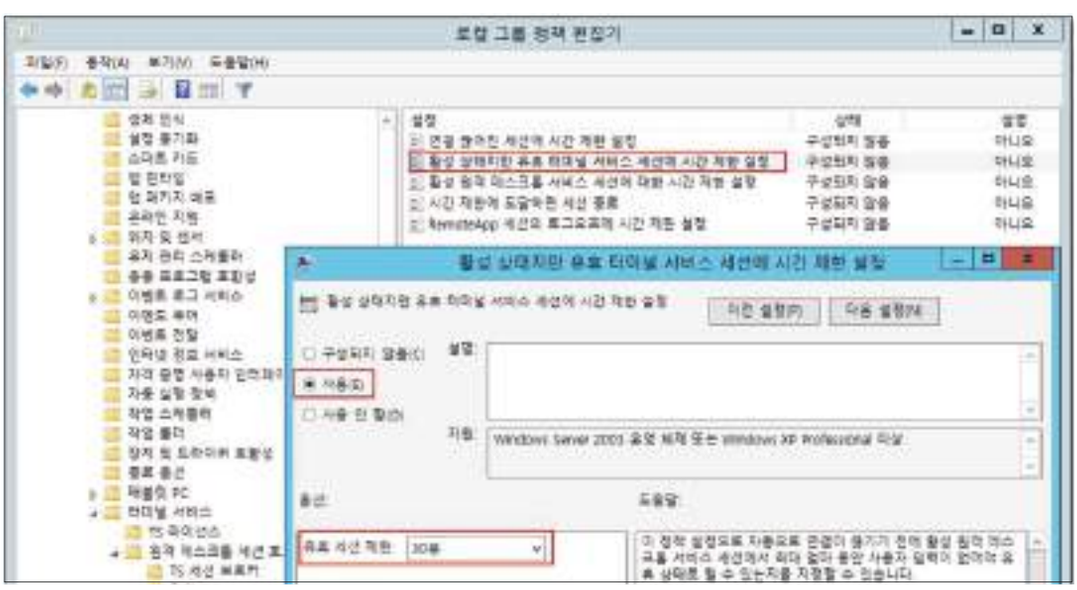
■ **Windows 2012**

Step 1) 시작> 실행> GPEDIT.MSC(로컬 그룹 정책 편집기)

Step 2) 컴퓨터 구성> 관리 템플릿> Windows 구성 요소> 터미널 서비스> 원격 데스크톱 세션 호스트> 세션 시간 제한>



Step 3) [활성 상태지만 유휴 터미널 서비스 세션에 시간 제한 설정]> [유휴 세션 제한]을 30분으로 설정



조치 시 영향	일반적인 경우 영향 없음

W-68 (중)	2. 서비스 관리 > 2.36 예약된 작업에 의심스러운 명령이 등록되어 있는지 점검
취약점 개요	
점검내용	■ 예약된 작업에 의심스러운 명령의 등록 여부 점검
점검목적	■ 외부 무단 침입 시 설정될 수 있는 불필요한 예약 작업의 등록 여부를 확인하기 위함
보안위협	■ 일정 시간마다 미리 설정해둔 프로그램을 실행할 수 있는 예약된 작업은 시작프로그램과 더불어서 해킹과 트로이 목마, 백도어를 설치하여 공격하기 좋은 루트로 사용될 수 있음
참고	-
점검대상 및 판단기준	
대상	■ Windows 2000, 2003, 2008, 2012
판단기준	**양호 :** 불필요한 명령어나 파일 등 주기적인 예약 작업의 존재 여부를 주기적으로 점검하고 제거한 경우
	취약 : 불필요한 명령어나 파일 등 주기적인 예약 작업의 존재 여부를 주기적으로 점검하지 않거나, 해당 작업을 제거하지 않은 경우
조치방법	예약 작업에 대한 주기적인 확인
점검 및 조치 사례	

■ Windows 2000, 2003, 2008, 2012

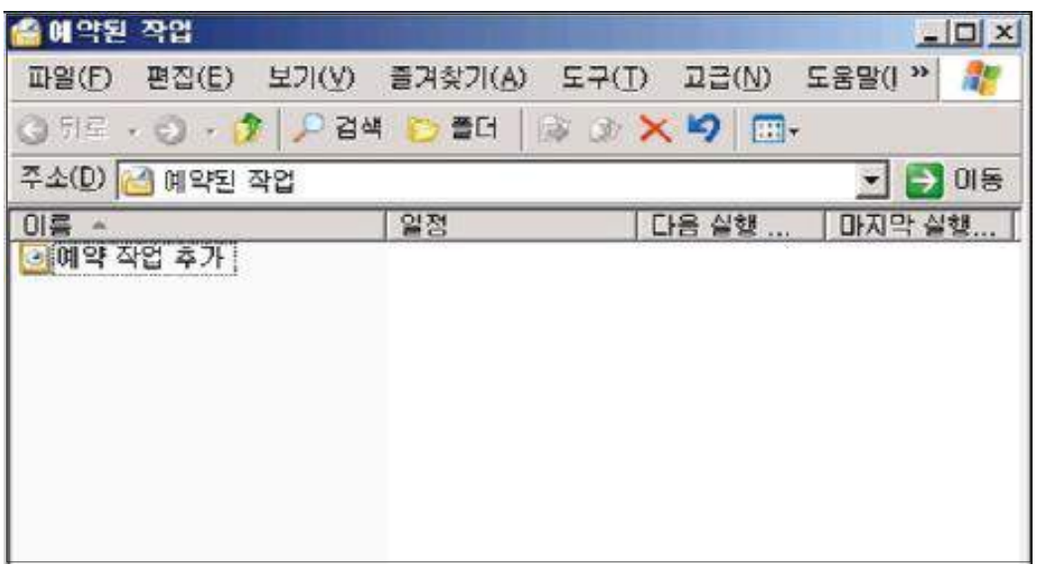
< GUI 확인 방법 >

Step 1) 시작> 설정> 제어판> 예약된 작업 확인

※ 2008, 2012 는 제어판> 관리도구> 작업 스케줄러 에서 확인

Step 2) 등록된 예약 작업을 선택하여 상세내역 확인

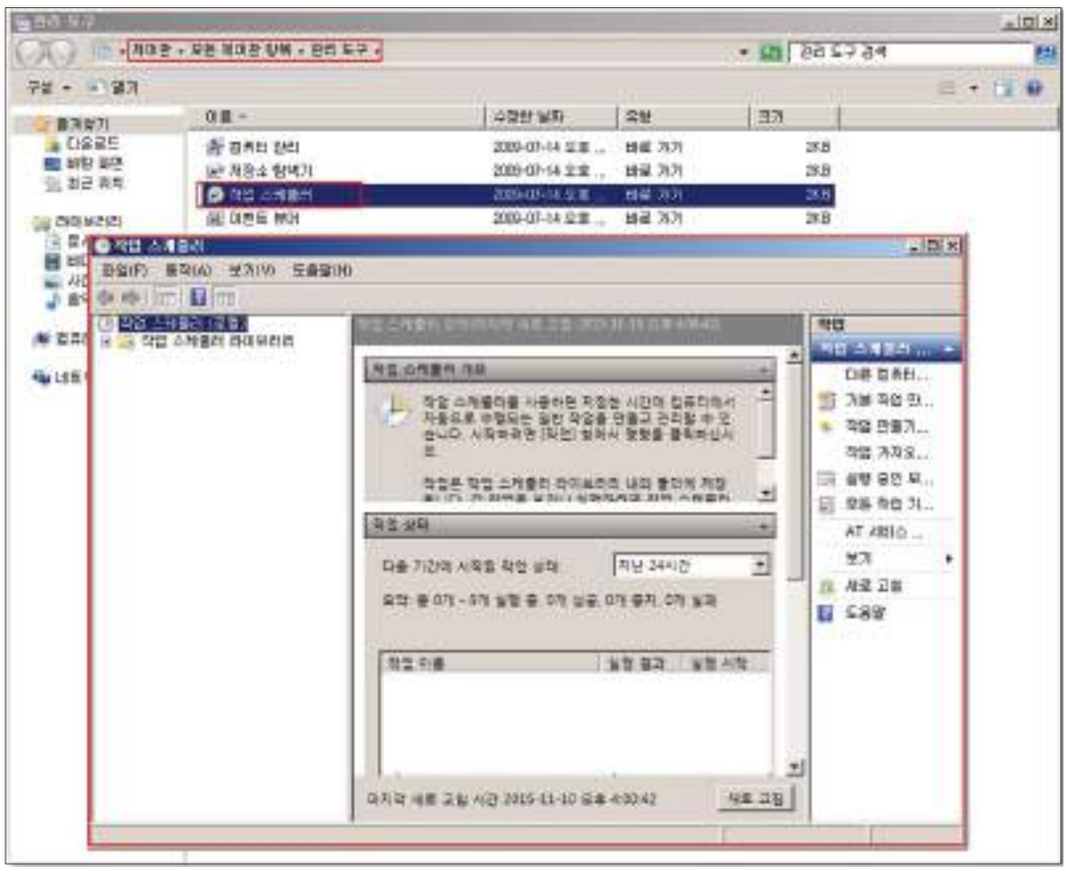
Step 3) 불필요한 파일 존재 시 삭제



[Windows 2000, 2003]

Windows 서버

W-68 (중)	2. 서비스 관리 > 2.36 예약된 작업에 의심스러운 명령이 등록되어 있는지 점검



[Windows 2008, 2012]

< CLI 확인 방법 >

Step 1) 시작> 실행> cmd 입력

Step 2) cmd 창에서 C:₩>at 명령어를 실행하여 확인 (2012 는 schtasks 명령어로 확인)

조치 시 영향	예약작업을 잘못 삭제하는 경우 관련된 작업이 실행되지 않을 수 있음

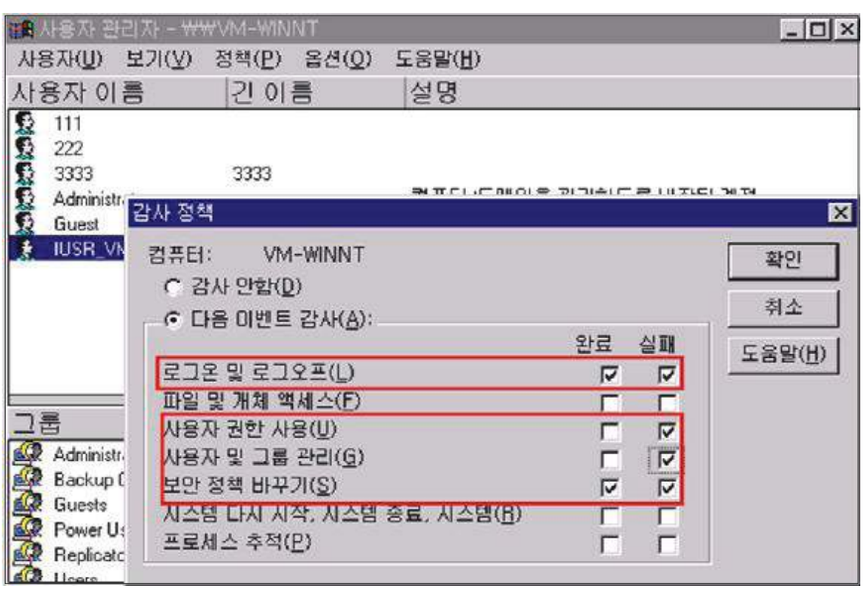
W-69 (중)	3. 패치 관리 > 3.3 정책에 따른 시스템 로깅 설정
취약점 개요	
점검내용	■ 시스템 로깅 설정 여부 및 적절성 점검
점검목적	■ 적절한 로깅 설정으로 유사 시 책임 추적을 위한 로그가 확보될 수 있게 하기 위함
보안위협	■ 감사 설정이 구성되어 있지 않거나 감사 설정 수준이 너무 낮은 경우 보안 관련 문제 발생 시 원인을 파악하기 어려우며 법적 대응을 위한 충분한 증거 확보가 어려움
참고	※ 감사 정책을 너무 강하게 설정할 경우, 보안 로그에 불필요한 항목이 많이 기록되므로 중요한 감사 항목 식별이 어려울 수 있으며, 시스템 성능에도 심각한 영향을 줄 수 있기 때문에 법적 요구 사항과 조직의 정책에 따라 꼭 필요한 로그를 남기도록 설정하여야 함 ※ 윈도우 시스템은 보안 로그가 가득 차게 되는 경우 가장 오래된 감사 항목이 덮어 씌워짐 ※ 관련 점검 항목 : A-20(상), A-85(하)
점검대상 및 판단기준	
대상	■ Windows NT, 2000, 2003, 2008, 2012
판단기준	**양호 :** 감사 정책 권고 기준에 따라 감사 설정이 되어 있는 경우
	취약 : 감사 정책 권고 기준에 따라 감사 설정이 되어 있지 않는 경우
조치방법	위와 같은 이벤트에 대한 추가적인 감사 설정
점검 및 조치 사례	

■ **Windows NT**

Step 1) 시작> 프로그램> 관리 도구> 도메인 사용자 관리자> 정책> 감사

< 설정 예시 >

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



Windows 서버

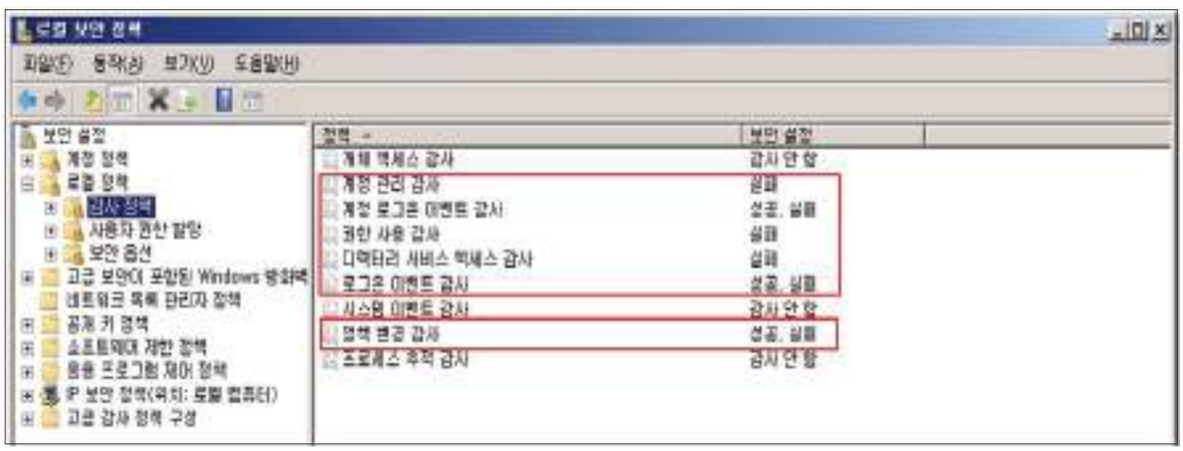
W-69 (중)	3. 패치 관리 > 3.3 정책에 따른 시스템 로깅 설정

■ **Windows 2000, 2003, 2008, 2012**

< 설정 예시 >

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

- 로그온 이벤트, 계정 로그온 이벤트, 정책 변경 : 성공/실패 감사
- 계정 관리, 디렉토리 서비스 액세스, 권한 사용 : 실패 감사



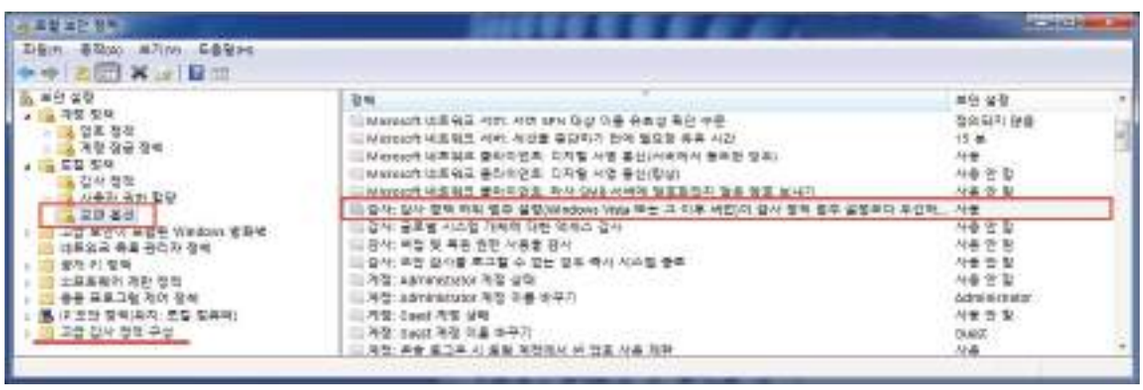
< 감사 정책 권고 기준 >

감사 정책	설정	고급 감사 정책	설정
개체 액세스 감사	감사 안 함	-	감사 안 함
계정 관리 감사	성공	사용자 계정 관리 컴퓨터 계정 관리 보안 그룹 관리	성공 성공 성공
계정 로그온 이벤트 감사	성공	자격 증명 유효성 검사 Kerberos 서비스 티켓 작업 Kerberos 인증서비스	성공 성공 성공
권한 사용 감사	감사 안 함	-	감사 안 함
디렉토리 서비스 액세스 감사	성공	디렉토리 서비스 액세스	성공
로그온 이벤트 감사	성공, 실패	로그온 로그오프 계정 잠금 특수 로그온 네트워크 정책 서버	성공, 실패 성공 성공 성공 성공, 실패
시스템 이벤트 감사	성공, 실패	보안 상태 변경 시스템 무결성 기타 시스템 이벤트	성공 성공, 실패 성공, 실패
정책 변경 감사	성공	감사 정책 변경 인증 정책 변경	성공 성공
프로세스 추적 감사	감사 안 함	-	감사 안 함

W-69 (중)	3. 패치 관리 > 3.3 정책에 따른 시스템 로깅 설정

※ 위에서 권고하는 감사 정책은 운영체제 제조사에서 서버 시스템의 보안 수준 유지를 위해 일반적으로 권장하는 설정값임. 감사 이벤트 생성하도록 허가된 작업이 너무 많거나, 많은 수의 개체에 대해 감사 정책을 구성할 경우 과도한 불필요한 이벤트 로그 생성으로 인해 전체 시스템의 성능에 영향을 줄 수 있으므로 책임 추적성을 확보하는 범위 내에서 적절한 감사 정책 수립이 필요함

※ 고급 감사 정책을 지원하는 시스템에서 고급 감사 정책을 활용 할 경우, **로컬 보안 정책** > **로컬 정책** > **보안 옵션** > "감사: 감사 정책 하위 범주 설정(Windows Vista 또는 그 이후 버전)이 감사 정책 범주 설정 보다 우선하도록 강제로 설정합니다" 정책을 먼저 사용하도록 설정하여야 함



< 감사정책 설명 >

정 책	설 명
로그온 이벤트	사용자가 컴퓨터에 로그온하거나 로그오프 할 때마다 로그온이 시도된 컴퓨터의 보안 로그에 이벤트 생성
계정 로그온 이벤트	사용자가 도메인에 로그온하면 도메인 컨트롤러에 로그온 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
디렉토리 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

Windows 서버

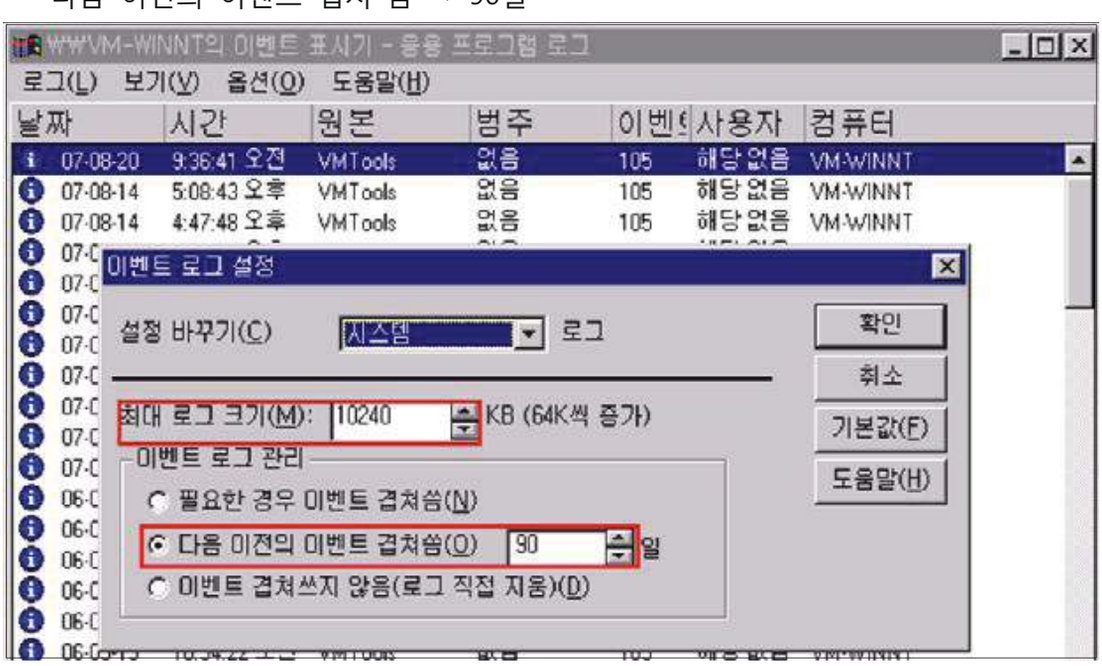
W-70 (하)	4. 로그 관리 > 4.3 이벤트 로그 관리 설정
취약점 개요	
점검내용	■ 이벤트 로그 파일 용량 및 보관 기간 설정 점검
점검목적	■ 유사 시 책임추적을 위해 주요 이벤트가 누락되지 않도록 이벤트 로그 파일의 크기 및 보관 기간을 적절하게 유지하기 위함
보안위협	■ 이벤트 로그 파일의 크기가 충분하지 않을 경우 중요 로그가 저장되지 않을 위험이 있으며, 최대 보존 크기를 초과하는 경우 자동으로 덮어 씀으로써 중요 로그의 손실의 우려가 있음
참고	-
점검대상 및 판단기준	
대상	■ Windows NT, 2000, 2003, 2008, 2012
판단기준	**양호 :** 최대 로그 크기 "10,240KB 이상"으로 설정, "90일 이후 이벤트 덮어씀" 을 설정한 경우
	취약 : 최대 로그 크기 "10,240KB 미만"으로 설정, 이벤트 덮어씀 기간이 "90일 이하"로 설정된 경우
조치방법	최대 로그 크기 "10,204KB", "90일 이후 이벤트 덮어씀" 설정
점검 및 조치 사례	

■ **Windows NT**

Step 1) 프로그램> 관리 도구> 이벤트 표시기> 로그> 로그 설정

Step 2) 최대 로그 크기 → 10240

다음 이전의 이벤트 겹쳐 씀 → 90일



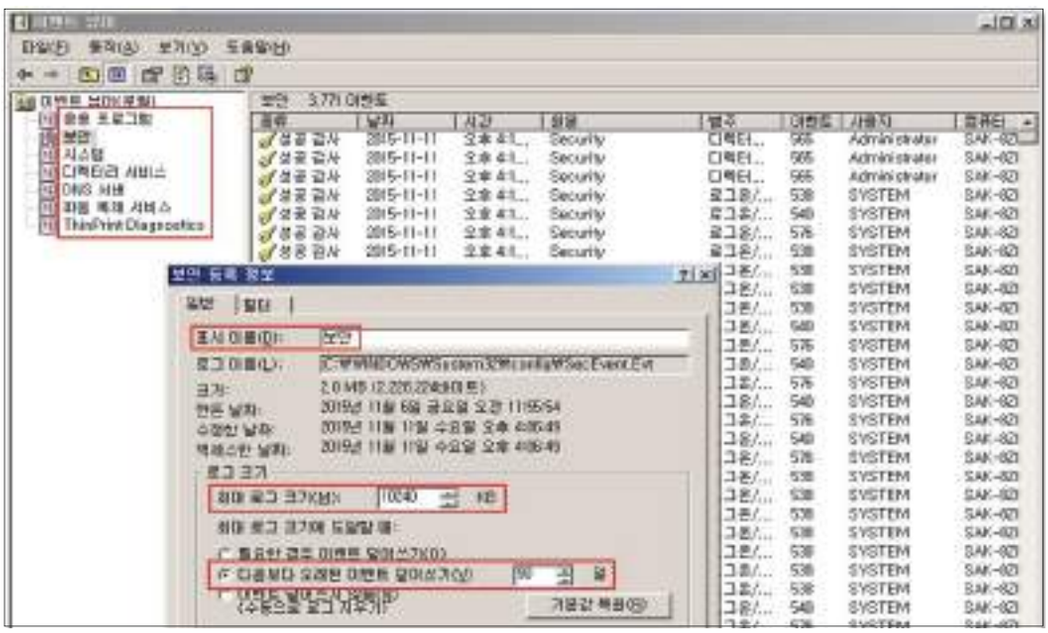
W-70 (하)	4. 로그 관리 > 4.3 이벤트 로그 관리 설정

■ **Windows 2000, 2003, 2008, 2012**

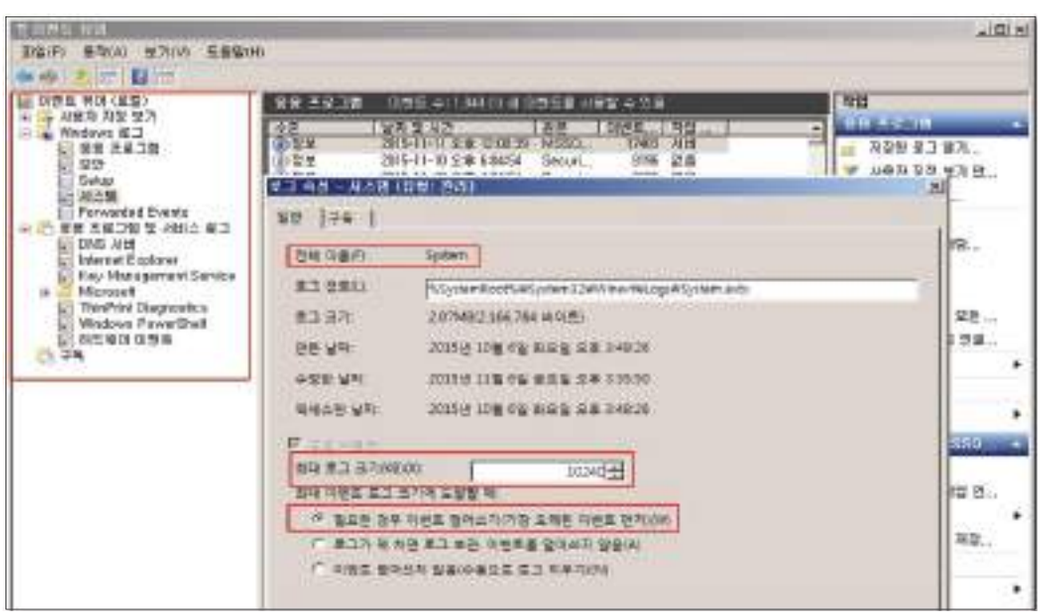
Step 1) 시작> 실행> EVENTVWR.MSC> 해당 로그> 속성> 일반

Step 2) 최대 로그 크기 → 10240

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



[Windows 2000, 2003]



[Windows 2008, 2012]

※ Windows 2008, 2012 서버의 경우 덮어쓰기 날짜 지정 불가능

조치 시 영향	일반적인 경우 영향 없음

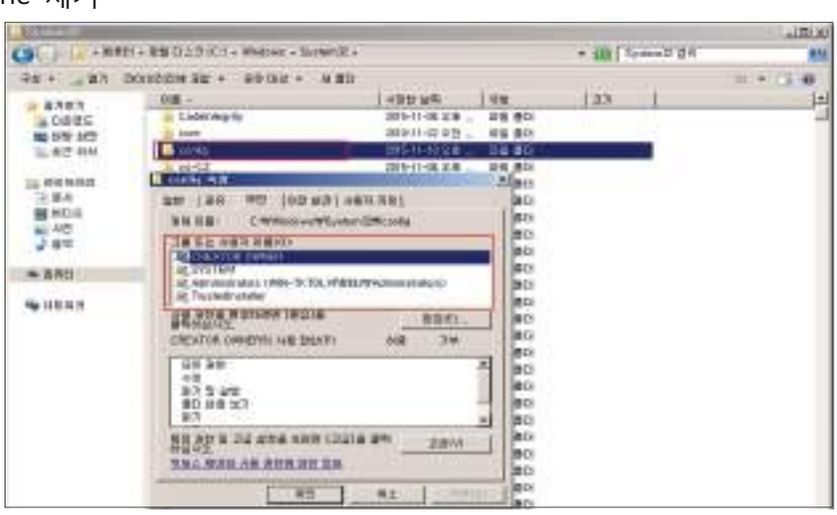
Windows 서버

W-71 (중)	4. 로그 관리 > 4.4 원격에서 이벤트 로그 파일 접근 차단
취약점 개요	
점검내용	■ 원격에서 로그 파일의 접근을 차단하기 위한 권한 적절성 점검
점검목적	■ 원격에서 로그 파일을 접근하는 것을 차단하여 로그 파일의 훼손 및 변조를 차단하기 위함
보안위협	■ 원격 익명 사용자의 시스템 로그 파일에 접근이 가능한 경우 '중요 시스템 로그' 파일 및 '애플리케이션 로그' 등 중요 보안 감사 정보의 변조·삭제·유출의 위험이 존재
참고	※ 로그 디렉토리 위치 • 시스템 로그 디렉토리: %systemroot%₩system32₩config • IIS 로그 디렉토리: %systemroot%₩system32₩LogFiles
점검대상 및 판단기준	
대상	■ Windows NT, 2000, 2003, 2008, 2012
판단기준	**양호 :** 로그 디렉토리의 접근권한에 Everyone 권한이 없는 경우
	취약 : 로그 디렉토리의 접근권한에 Everyone 권한이 있는 경우
조치방법	로그 디렉토리의 접근권한에 Everyone 제거
점검 및 조치 사례	

■ **Windows NT, 2000, 2003, 2008, 2012**

Step 1) 탐색기> 로그 디렉토리> 속성> 보안

Step 2) Everyone 제거



※ 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.

조치 시 영향	일반적인 경우 영향 없음

W-72 (상)	5. 보안 관리 > 5.11 DoS 공격 방어 레지스트리 설정
취약점 개요	
점검내용	■ DoS 공격 방어 레지스트리 설정 여부 점검
점검목적	■ TCP/IP 스택(Stack)을 강화하는 레지스트리 값 변경을 통하여 DoS 공격을 방어하기 위함
보안위협	■ DoS 방어 레지스트리를 설정하지 않은 경우, DoS 공격에 의한 시스템 다운으로 서비스 제공이 중단될 수 있음
참고	※ **DoS(서비스 거부 공격):** 네트워크 사용자가 컴퓨터나 컴퓨터의 특정 서비스를 사용할 수 없도록 만들기 위한 네트워크 공격
점검대상 및 판단기준	
대상	■ Windows NT, 2000, 2003, 2008, 2012
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

점검 및 조치 사례

레지스트리 값 이름	설 명
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 Gateway을 검색할 수 없음 • 1 => (True) 작동하지 않는 Gateway을 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

Windows 서버

W-72 (상)	5. 보안 관리 > 5.11 DoS 공격 방어 레지스트리 설정

■ **Windows NT, 2000, 2003, 2008, 2012**

Step 1) 시작> 실행> REGEDIT

Step 2) HKLM₩System₩CurrentControlSet₩Services₩Tcpip₩Parameters₩ 검색

Step 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)

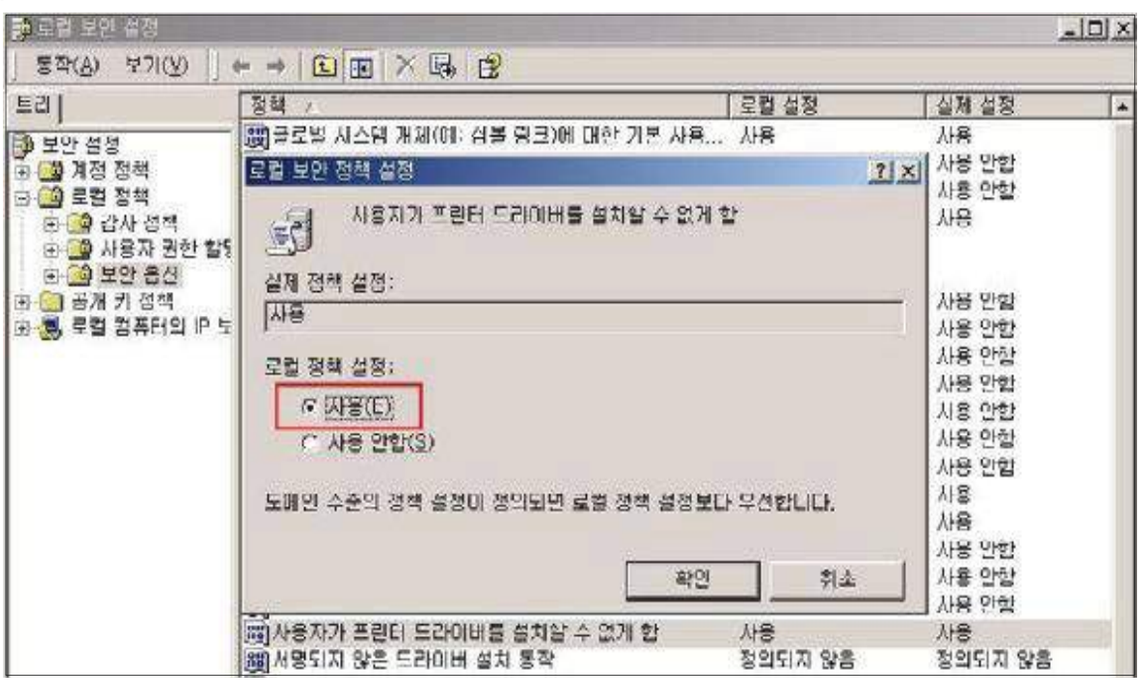
조치 시 영향	잘못된 값을 설정할 경우 OS 재설치를 요구할 수 있음

W-73 (중)	5. 보안 관리 > 5.12 사용자가 프린터 드라이버를 설치할 수 없게 함
취약점 개요	
점검내용	■ 사용자의 프린터 드라이버 설치 차단 여부 점검
점검목적	■ 일반 사용자를 통한 프린터 드라이버 설치를 차단하여 의도하지 않은 시스템 손상을 방지하기 위함
보안위협	■ 서버에 프린터 드라이버를 설치하는 경우 악의적인 사용자가 고의적으로 잘못된 프린터 드라이버를 설치하여 컴퓨터를 손상시킬 수 있으며, 프린터 드라이버로 위장한 악성 코드를 설치할 수 있음
참고	-
점검대상 및 판단기준	
대상	■ Windows NT, 2000, 2003, 2008, 2012
판단기준	**양호 :** "사용자가 프린터 드라이버를 설치할 수 없게 함" 정책
	취약 : "사용자가 프린터 드라이버를 설치할 수 없게 함" 정책이 "사용 안 함"인 경우
조치방법	사용자가 프린터 드라이버를 설치할 수 없게 함 → 사용
점검 및 조치 사례	

■ **Windows NT, 2000**

Step 1) 시작> 실행> SECPOL.MSC> 로컬 정책> 보안 옵션

Step 2) "사용자가 프린터 드라이버를 설치할 수 없게 함" 정책을 "사용" 으로 설정



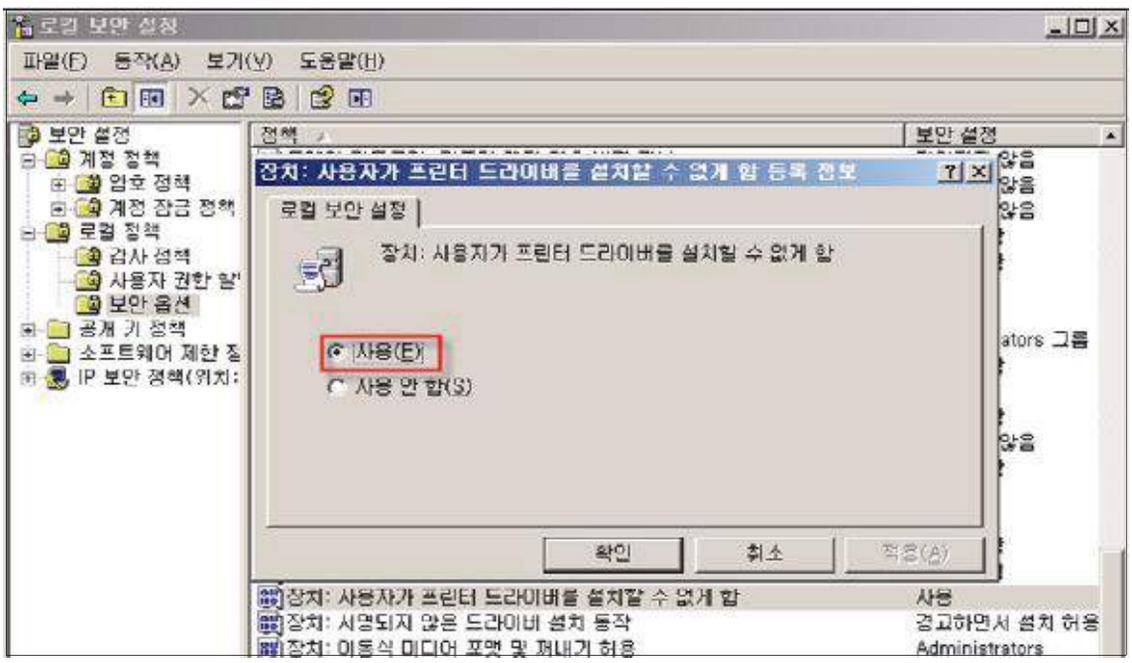
Windows 서버

W-73 (중)	5. 보안 관리 > 5.12 사용자가 프린터 드라이버를 설치할 수 없게 함

■ **Windows 2003, 2008, 2012**

Step 1) 시작> 실행> SECPOL.MSC> 로컬 정책> 보안 옵션

Step 2) "장치: 사용자가 프린터 드라이버를 설치할 수 없게 함" 정책을 "사용" 으로 설정

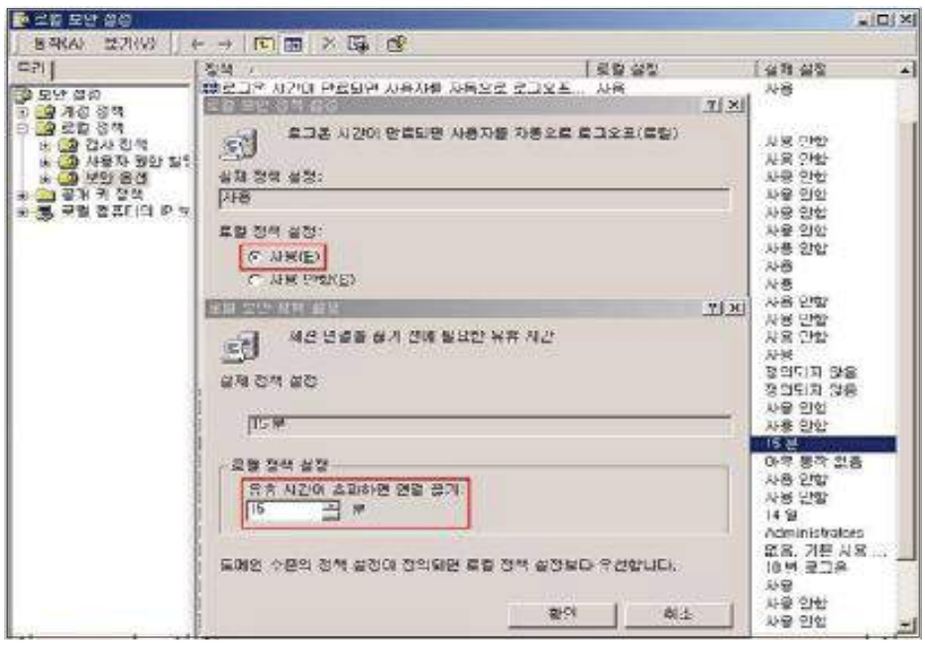


조치 시 영향	일반적인 경우 영향 없음

W-74 (중)	5. 보안 관리 > 5.13 세션 연결을 중단하기 전에 필요한 유휴시간
취약점 개요	
점검내용	■ 세션 연결 중단 시 유휴시간 설정 여부 점검
점검목적	■ 세션이 중단되기 전에 SMB(서버 메시지 블록) 세션에서 보내야 하는 연속 유휴 시간을 결정하여 서비스 거부 공격 등에 악용되지 않도록 하기 위함
보안위협	■ SMB 세션에서는 서버 리소스를 사용하며, null(공백) 세션수가 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
참고	※ 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
점검대상 및 판단기준	
대상	■ Windows NT, 2000, 2003, 2008, 2012
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
점검 및 조치 사례	
■ **Windows NT, 2000** Step 1) 시작> 실행> SECPOL.MSC> 로컬 정책> 보안 옵션 Step 2) "로그인 시간이 만료되면 클라이언트 연결 끊기" 정책 "사용" 설정 "세션 연결을 중단하기 전에 필요한 유효 시간" 정책 "15분" 설정	

Windows 서버

W-74 (중)	5. 보안 관리 > 5.13 세션 연결을 중단하기 전에 필요한 유휴시간

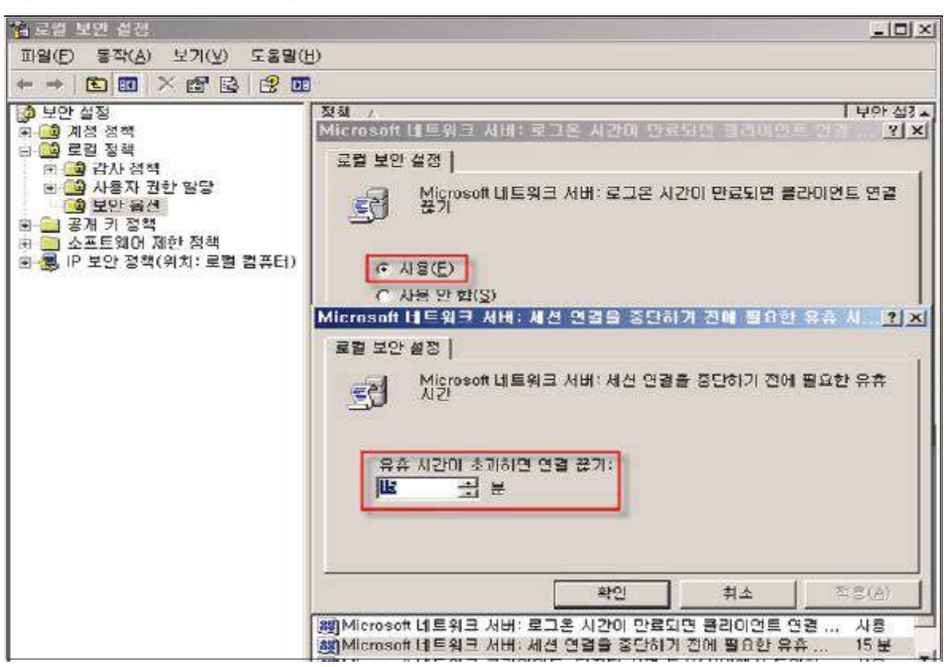


■ **Windows 2003, 2008, 2012**

Step 1) 시작> 실행> SECPOL.MSC> 로컬 정책> 보안 옵션

Step 2) "로그온 시간이 만료되면 클라이언트 연결 끊기" 정책 "사용" 설정

"세션 연결을 중단하기 전에 필요한 유휴 시간" 정책 "15분" 설정



조치 시 영향	일반적인 경우 영향 없음

W-75 (하)	5. 보안 관리 > 5.14 경고 메시지 설정
취약점 개요	
점검내용	■ 로그온 시 경고 메시지 출력 여부 점검
점검목적	■ 로그온 시 경고 메시지를 설정하여 시스템에 로그온을 시도하는 사용자들에게 관리자는 시스템의 불법적인 사용에 대하여 경고 창을 띄움으로써 경각심을 주기 위함
보안위협	■ 로그온 경고 메시지가 없는 경우 악의적인 사용자에게 관리자가 적절한 보안수준으로 시스템을 보호하고 있으며, 공격자의 활동을 주시하고 있다는 생각을 상기 시킬 수 없어 간접적인 공격 기회를 제공할 우려 있음
참고	-
점검대상 및 판단기준	
대상	■ Windows NT, 2000, 2003, 2008, 2012
판단기준	**양호 :** 로그인 경고 메시지 제목 및 내용이 설정되어 있는 경우
	취약 : 로그인 경고 메시지 제목 및 내용이 설정되어 있지 않은 경우
조치방법	로그인 메시지 제목 및 메시지 내용에 경고 문구 삽입
점검 및 조치 사례	

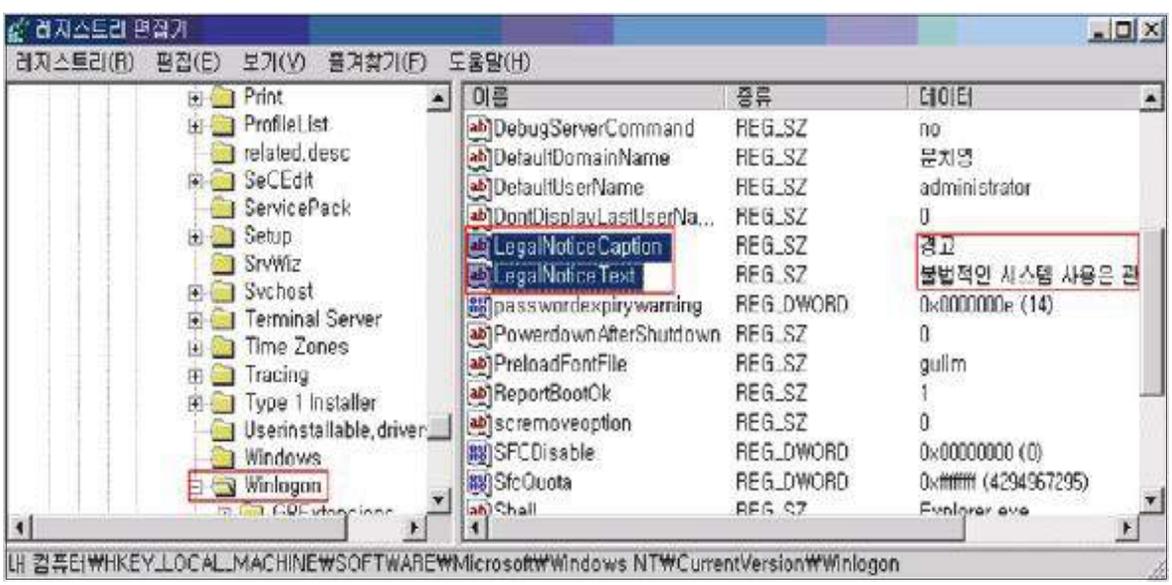
■ **Windows NT**

Step 1) HKEY_LOCAL_MACHINE₩SOFTWARE₩Microsoft₩WindowsNT₩CurrentVersion ₩Winlogon

Step 2) LegalNoticeCaption: 제목

Step 3) LegalNoticeText: 메시지 내용

※ 이처럼 변경된 레지스트리 키의 내용은 시스템을 로그오프 한 후 반영됨



Windows 서버

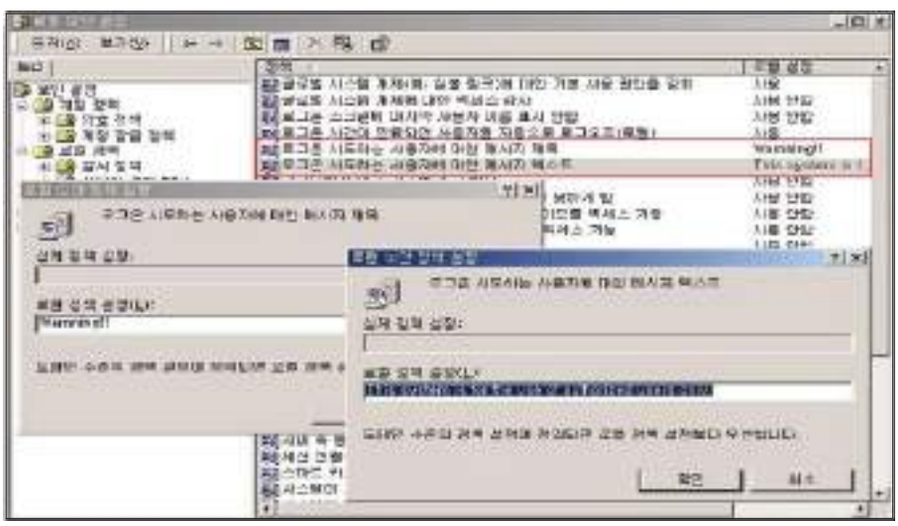
W-75 (하)	5. 보안 관리 > 5.14 경고 메시지 설정

■ **Windows 2000**

Step 1) 시작> 실행> SECPOL.MSC> 로컬 정책> 보안 옵션

Step 2) 로그온 시도하는 사용자에 대한 메시지 제목: 배너 제목 입력

Step 3) 로그온 시도하는 사용자에 대한 메시지 텍스트: 배너 내용 입력

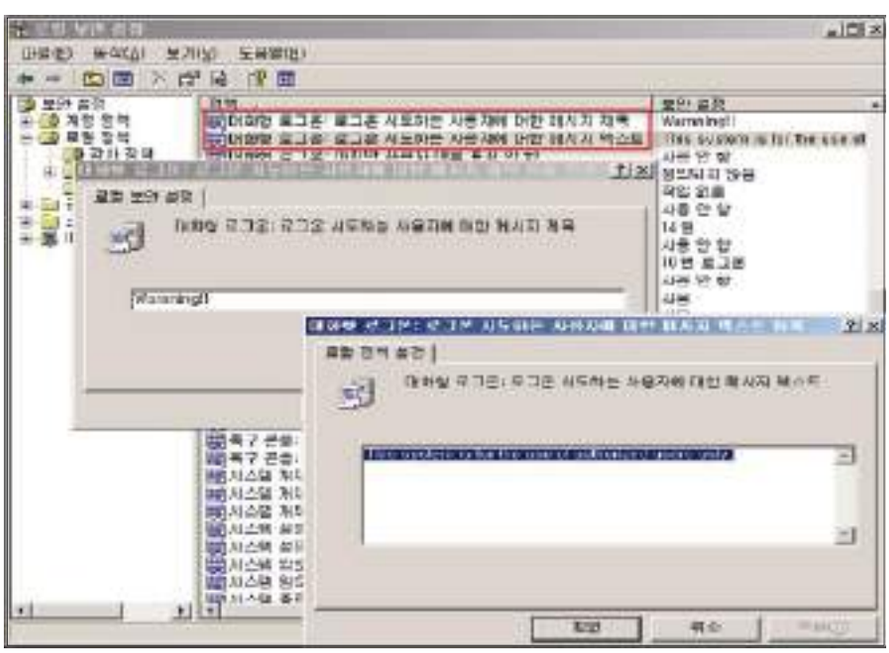


■ **Windows 2003, 2008, 2012**

Step 1) 시작> 실행> SECPOL.MSC> 로컬 정책> 보안 옵션

Step 2) 대화형 로그온: 로그온 시도하는 사용자에 대한 메시지 제목: 배너 제목 입력

Step 3) 대화형 로그온: 로그온 시도하는 사용자에 대한 메시지 텍스트: 배너 내용 입력



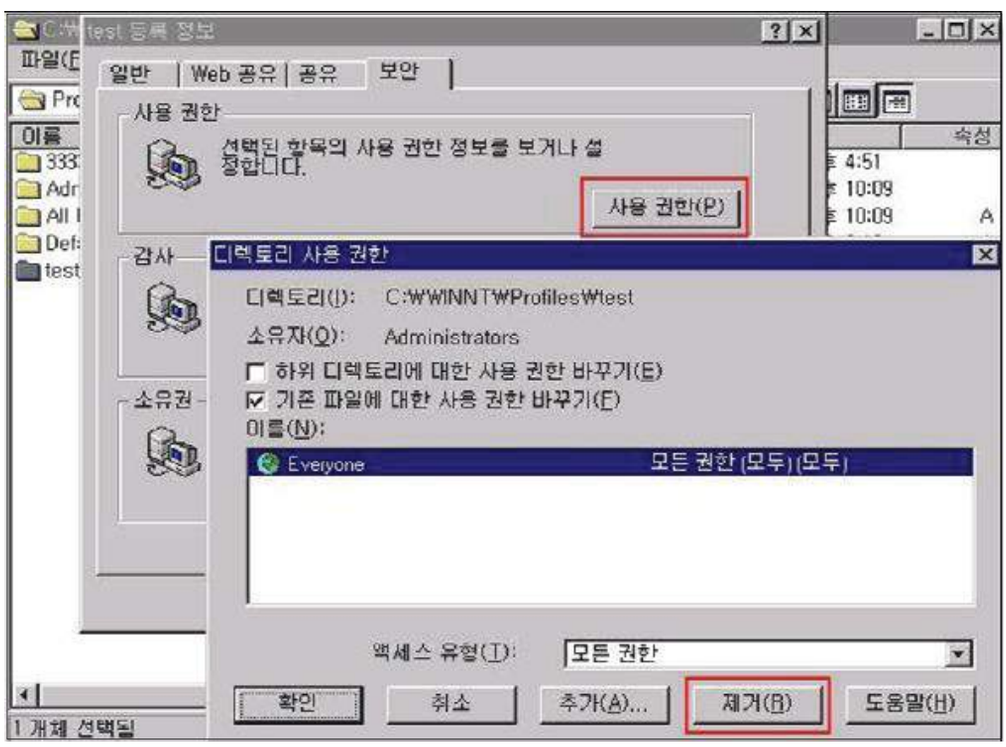
조치 시 영향	일반적인 경우 영향 없음

W-76 (중)	5. 보안 관리 > 5.15 사용자별 홈 디렉토리 권한 설정
취약점 개요	
점검내용	■ 사용자 홈 디렉토리 권한 적절성 점검
점검목적	■ 사용자 홈 디렉토리에 적절한 권한을 부여하여 비인가 사용자에 의한 불필요한 정보 노출을 방지하기 위함
보안위협	■ 사용자 계정별 홈 디렉토리의 권한이 제한되어 있지 않은 경우 임의의 사용자나 다른 사용자의 홈 디렉토리에 악의적인 목적으로 접근할 수 있으며, 접근 후 의도 또는, 의도하지 않은 행위로 시스템에 악영향을 미칠 수 있음
참고	-
점검대상 및 판단기준	
대상	■ Windows NT, 2000, 2003, 2008, 2012
판단기준	**양호 :** 홈 디렉토리에 Everyone 권한이 없는 경우 (All Users, Default User 디렉토리 제외)
	취약 : 홈 디렉토리에 Everyone 권한이 있는 경우
조치방법	Everyone 권한 제거
점검 및 조치 사례	

■ **Windows NT**

Step 1) Windows NT: C:₩WinNT₩Profiles₩사용자 홈 디렉토리> 등록 정보> 보안

Step 2) Everyone 권한 제거(All Users, Default User 디렉토리는 제외)



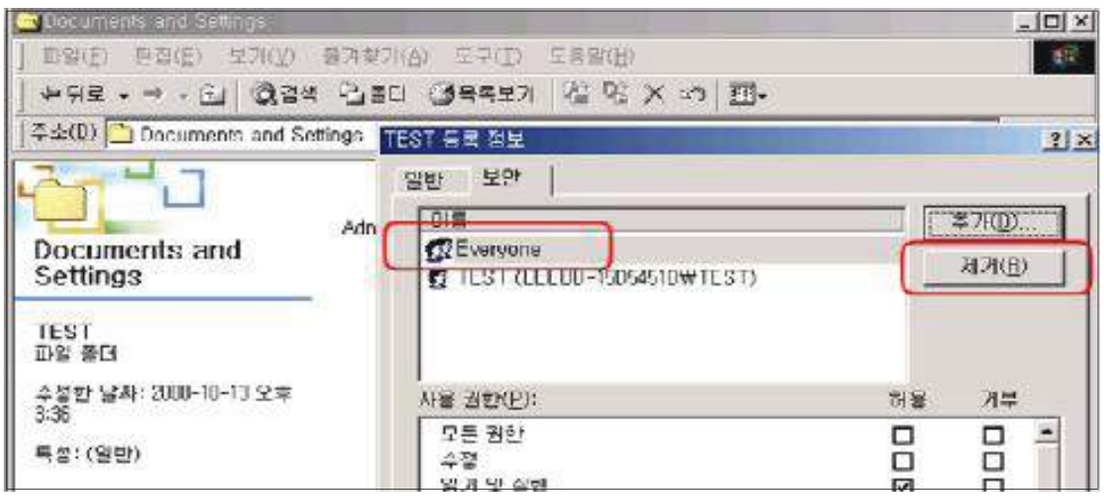
Windows 서버

W-76 (중)	5. 보안 관리 > 5.15 사용자별 홈 디렉토리 권한 설정

■ **Windows 2000, 2003**

Step 1) C:₩Documents and Settings₩사용자 홈 디렉토리> 속성> 보안

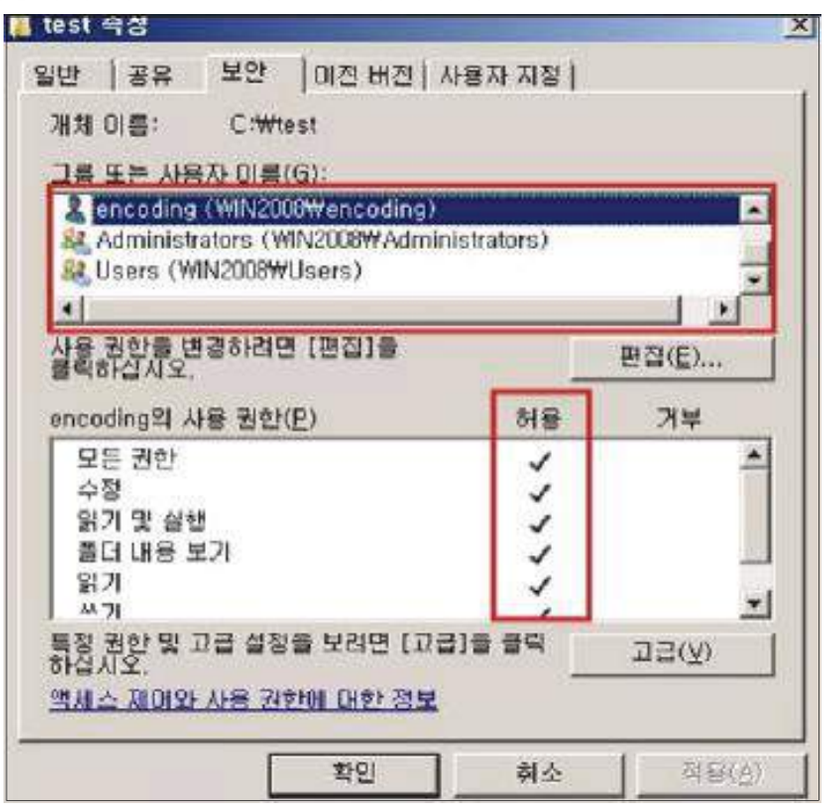
Step 2) Everyone 권한 제거(All Users, Default User 디렉토리는 제외)



■ **Windows 2008**

Step 1) C:₩사용자₩<사용자 계정>

Step 2) 해당 사용자에 대한 권한 외 일반 계정 삭제

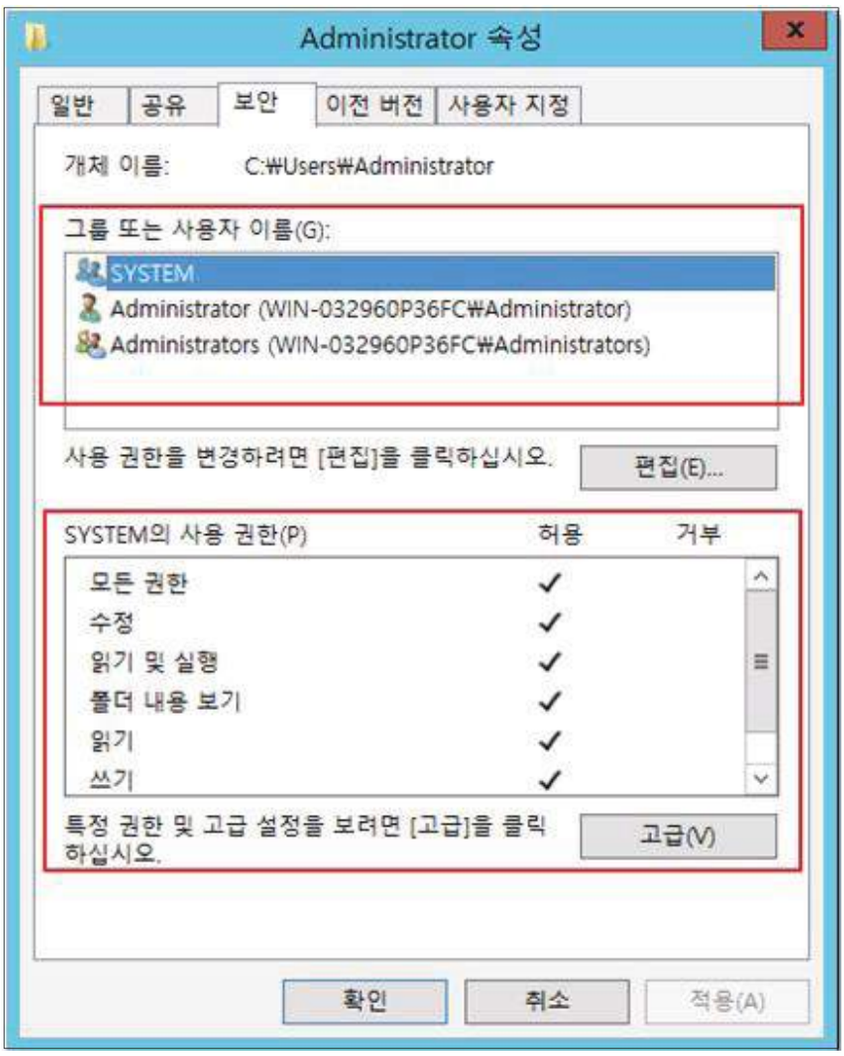


W-76 (중)	5. 보안 관리 > 5.15 사용자별 홈 디렉토리 권한 설정

■ **Windows 2012**

Step 1) C:₩사용자₩<사용자 계정>

Step 2) 해당 사용자에 대한 권한 외 일반 계정 삭제



조치 시 영향	일반적인 경우 영향 없음

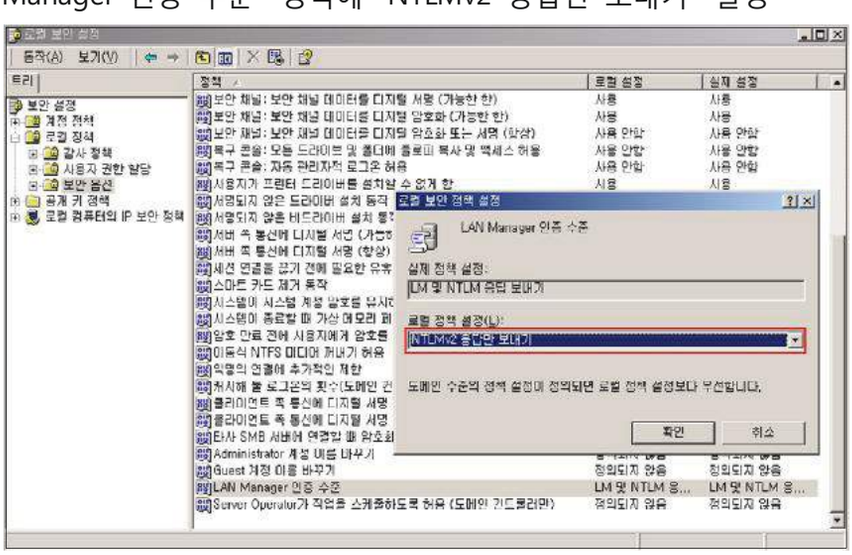
Windows 서버

W-77 (중)	5. 보안 관리 > 5.16 LAN Manager 인증 수준
취약점 개요	
점검내용	■ LAN Manager 인증 수준 적절성 점검
점검목적	■ Lan Manager 인증 수준 설정을 통해 네트워크 로그온에 사용할 Challenge/Response 인증 프로토콜을 결정하며, 안전한 인증 절차를 적용하기 위함
보안위협	■ 안전하지 않은 LAN Manager 인증 수준을 사용하는 경우 인증 트래픽을 가로채기를 통해 악의적인 계정 정보 노출을 허용할 수 있음
참고	※ LAN Manager는 네트워크를 통한 파일 및 프린터 공유 등과 같은 작업 시 인증을 담당. NTLMv2는 Windows 2000, 2003, XP 이상에서 지원되며, Windows 98, NT 버전과 통신할 경우 패치를 설치하여야 함
점검대상 및 판단기준	
대상	■ Windows NT, 2000, 2003, 2008, 2012
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 Windows 2012: 네트워크 보안: LAN Manager 인증 수준 -> NTMLv2 응답만 보냄
점검 및 조치 사례	

■ **Windows NT, 2000**

Step 1) 시작> 실행> SECPOL.MSC> 로컬 정책> 보안 옵션

Step 2) "LAN Manager 인증 수준" 정책에 "NTLMv2 응답만 보내기" 설정

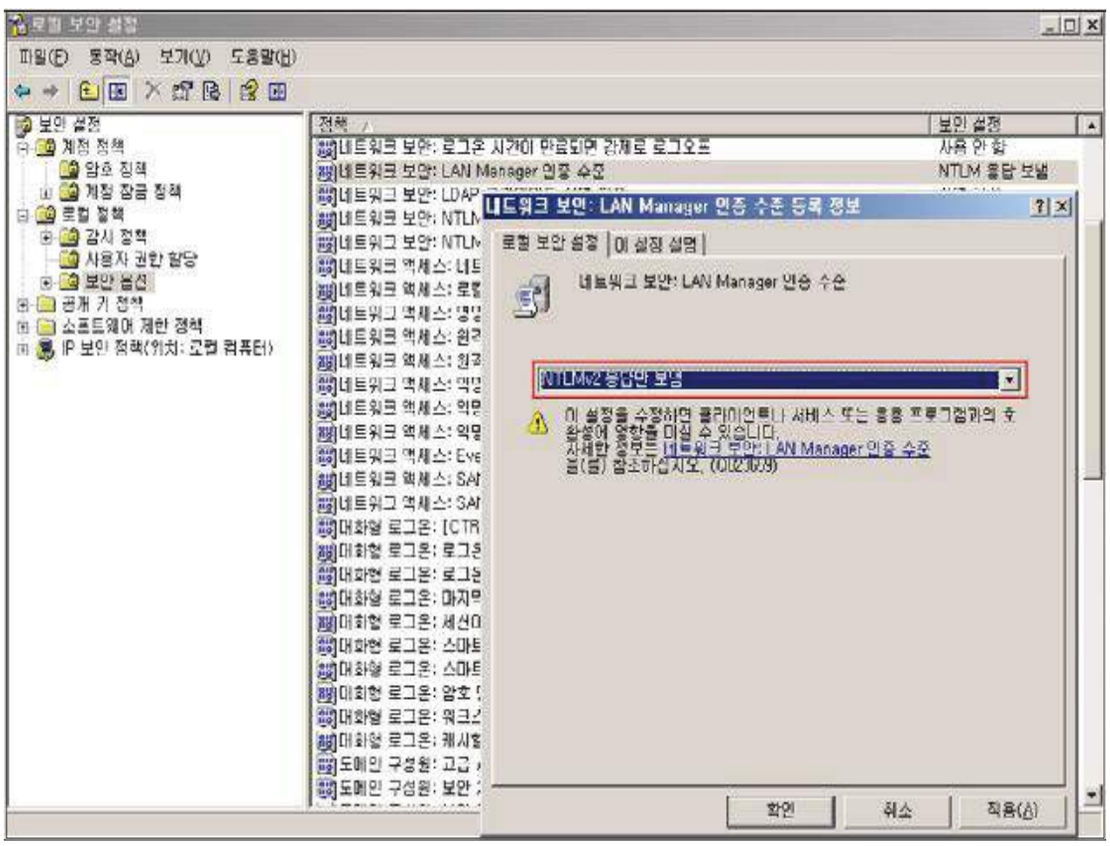


W-77 (중)	5. 보안 관리 > 5.16 LAN Manager 인증 수준

■ **Windows 2003, 2008, 2012**

Step 1) 시작> 실행> SECPOL.MSC> 로컬 정책> 보안 옵션

Step 2) "네트워크 보안: LAN Manager 인증 수준" 정책에 NTLMv2 응답만 보냄" 설정



조치 시 영향	일반적인 경우 영향 없음

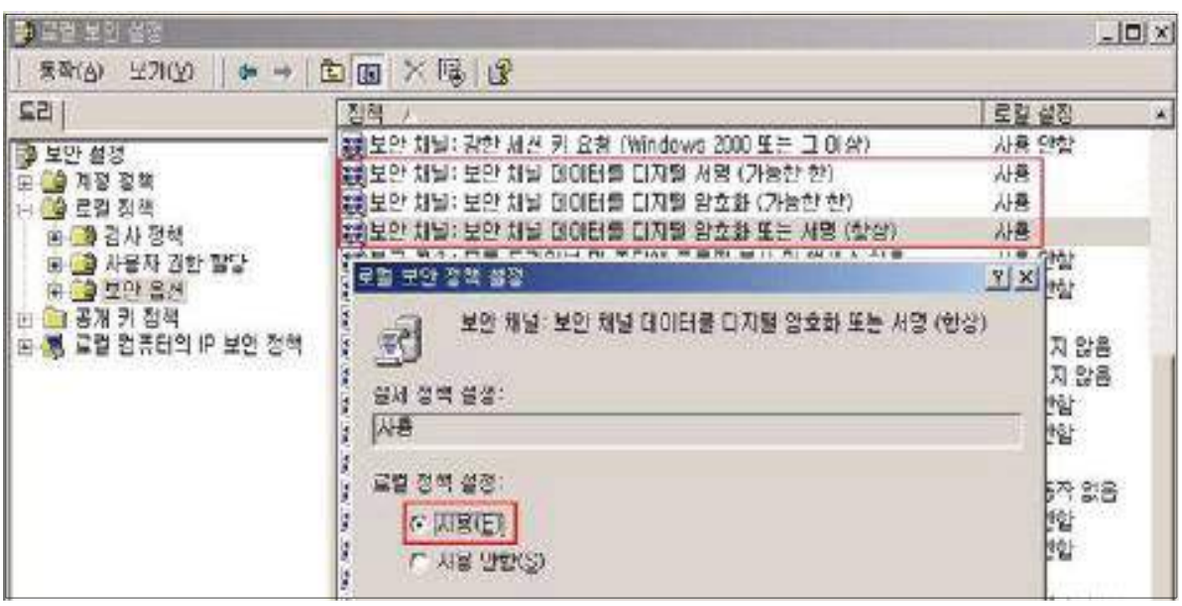
Windows 서버

W-78 (중)	5. 보안 관리 > 5.17 보안 채널 데이터 디지털 암호화 또는 서명
취약점 개요	
점검내용	■ '보안 채널 데이터 디지털 암호화 또는 서명' 정책 적절성 점검
점검목적	■ 해당 정책을 활성화하여 보안 채널의 서명 또는 암호화가 협상되지 않는 한 보안 채널을 확립하지 않기 위함
보안위협	■ 보안 채널이 암호화 되지 않은 경우 인증 트래픽 끼어들기 공격, 반복 공격 및 기타 유형의 네트워크 공격 등의 위험 존재
참고	-
점검대상 및 판단기준	
대상	■ Windows NT, 2000, 2003, 2008, 2012
판단기준	**양호 :** 아래 3가지 정책이 "사용"으로 되어 있는 경우
	취약 : 아래 3가지 정책이 "사용 안 함" 으로 되어 있는 경우 • 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
점검 및 조치 사례	

■ **Windows NT, 2000**

Step 1) 시작> 실행> SECPOL.MSC> 로컬 정책> 보안 옵션

Step 2) 위 3가지 정책을 모두 "사용"으로 설정



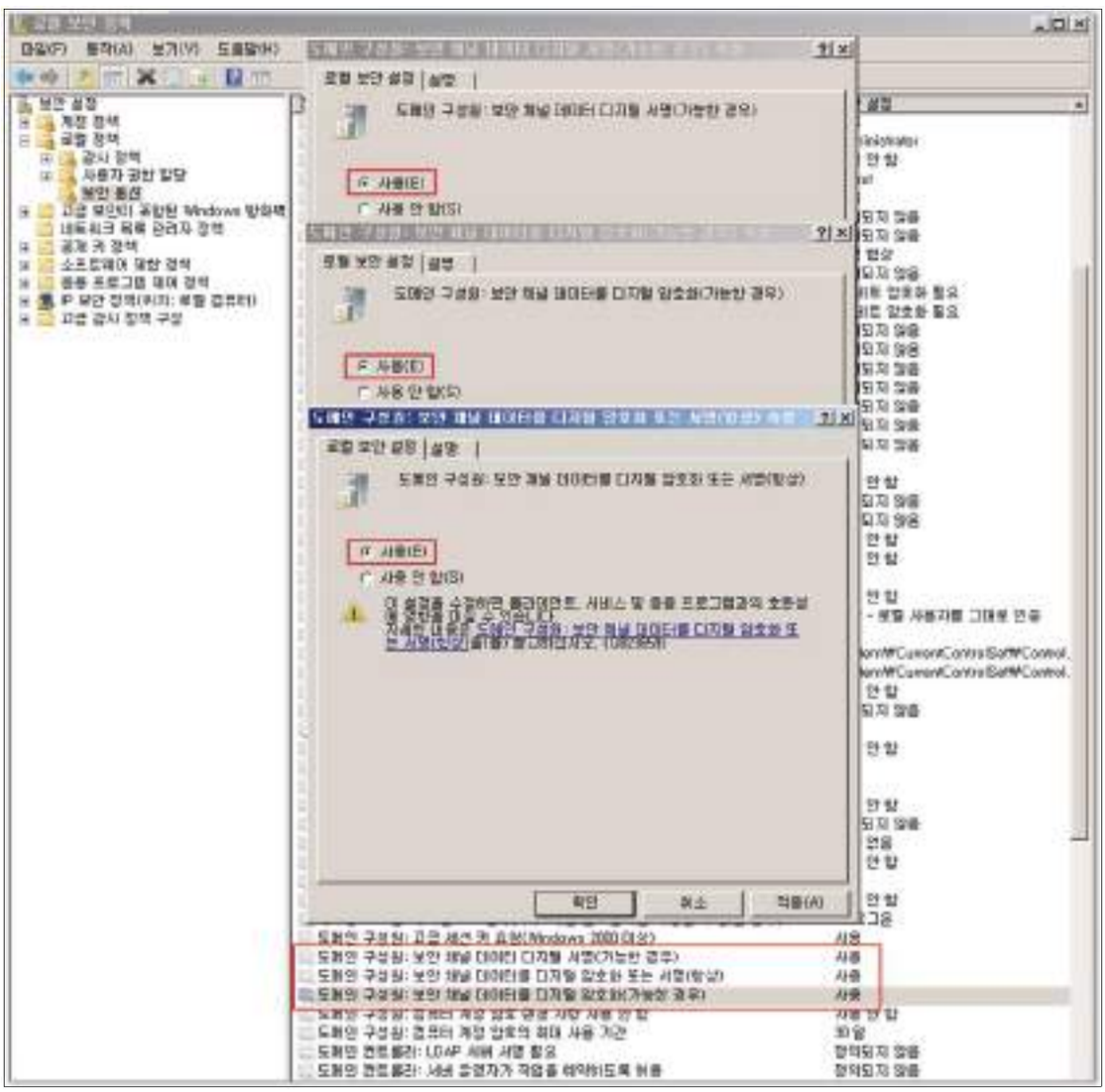
W-78 (중)	5. 보안 관리 > 5.17 보안 채널 데이터 디지털 암호화 또는 서명

■ **Windows 2003, 2008, 2012**

Step 1) 시작> 실행> SECPOL.MSC> 로컬 정책> 보안 옵션

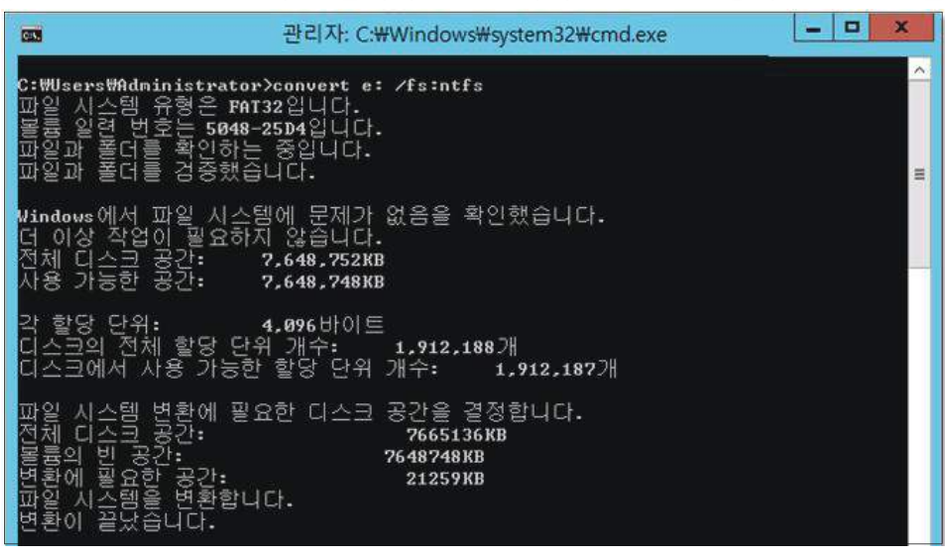
Step 2) 아래 3가지 정책을 모두 "사용" 으로 설정

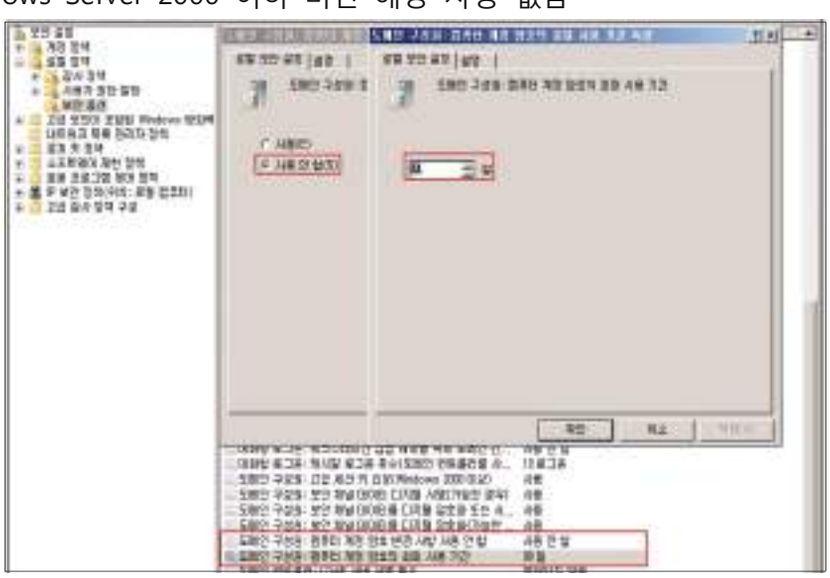
- 도메인 구성원: 보안 채널 데이터를 디지털 암호화 또는, 서명 (항상)
- 도메인 구성원: 보안 채널: 보안채널 데이터를 디지털 서명 (가능하면)
- 도메인 구성원: 보안 채널: 보안채널 데이터를 디지털 암호화 (가능하면)



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

Windows 서버

W-79 (중)	5. 보안 관리 > 5.18 파일 및 디렉토리 보호
취약점 개요	
점검내용	■ NTFS 파일 시스템 사용 여부 점검
점검목적	■ FAT 파일 시스템에 비해 보다 강화된 보안 기능을 제공하는 파일 시스템을 사용하기 위함 (파일과 디렉토리에 소유권과 사용 권한 설정이 가능하고 ACL(접근 통제 목록)을 제공)
보안위협	■ FAT 파일 시스템 사용 시 사용자별 접근 통제를 적용할 수 없어 중요 정보에 대한 책임 추적성 확보가 어려움
참고	※ 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 ※ 최근 운영체제 버전에서는 FAT32 파일 시스템을 지원하지 않으나 기존 FAT32 에서 NTFS 변환 가능 ※ 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.
점검대상 및 판단기준	
대상	■ Windows NT, 2000, 2003, 2008, 2012
판단기준	**양호 :** NTFS 파일 시스템을 사용하는 경우
	취약 : FAT파일 시스템을 사용하는 경우
조치방법	FAT파일 시스템을 사용하고 있다면, 가급적 NTFS 파일 시스템으로 변환
점검 및 조치 사례	
■ **Windows 2003, 2008, 2012** Step 1) 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

W-80 (중)	5. 보안 관리 > 5.19 컴퓨터 계정 암호 최대 사용 기간
취약점 개요	
점검내용	■ 컴퓨터 계정 암호 최대 사용 기간 설정 여부 점검
점검목적	■ 컴퓨터 계정 암호 최대 사용 기간을 설정하기 위함
보안위협	■ 기본적으로 도메인 구성원은 도메인 암호 변경 주기가 적절하지 않은 경우공격자가 무단 공격을 실행하여 하나 이상의 컴퓨터 계정 암호를 추측하기에 충분한 시간을 제공할 수 있음
참고	※ 도메인 구성원이 해당 컴퓨터 계정 암호를 정기적으로 변경할지를 결정할 수 있으며, 기본적으로 도메인 구성원이 사용하는 도메인 암호 변경 기간은 '자동'으로 설정되어 있음
점검대상 및 판단기준	
대상	■ Windows 2000, 2003, 2008, 2012
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 안 함 → 사용 안 함 컴퓨터 계정 암호 최대 사용 기간 → 90일
점검 및 조치 사례	
■ **Windows 2003, 2008, 2012** Step 1) 시작> 실행> SECPOL.MSC> 로컬 정책> 보안 옵션 Step 2) 컴퓨터 계정 암호 변경 사용 안 함 → 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

Windows 서버

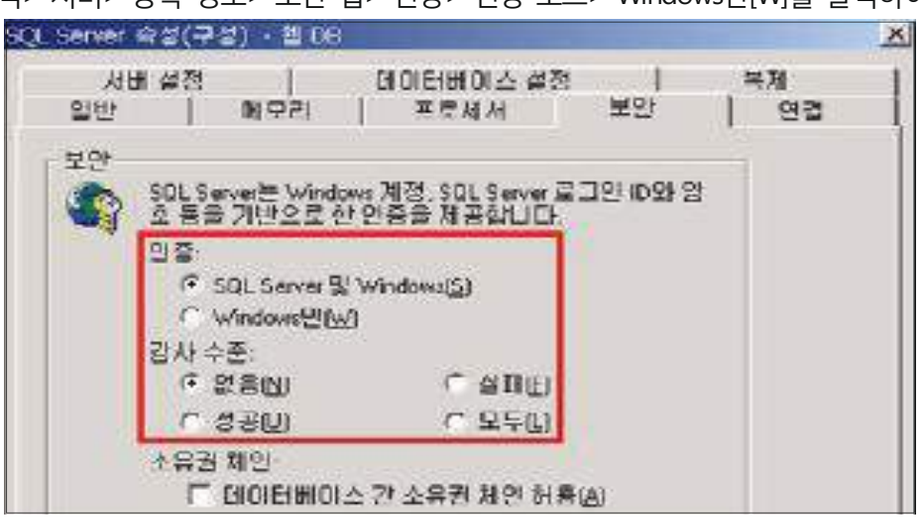
W-81 (중)	5. 보안 관리 > 5.20 시작프로그램 목록 분석
취약점 개요	
점검내용	■ 시작프로그램 목록 내 불필요한 항목 존재 여부 점검
점검목적	■ 불필요한 시작 프로그램을 삭제하거나 비활성화 하여 악의적인 공격을 차단하기 위함
보안위협	■ 윈도우 부팅 시 너무 많은 시작프로그램이 동시에 실행되면 속도가 저하되는 문제가 발생하며, 공격자가 심어놓은 악성 프로그램이나 해킹 툴이 실행되어 시스템에 피해를 줄 수 있음
참고	-
점검대상 및 판단기준	
대상	■ Windows 2000, 2003, 2008, 2012
판단기준	**양호 :** 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
점검 및 조치 사례	
■ **Windows 2000, 2003, 2008** Step 1) 시작> 검색> msconfig 명령어 입력 Step 2) 시작 프로그램 탭 클릭> 시작 프로그램 목록 중 불필요하거나 의심스러운 항목 체크 표시 해제 ■ **Windows 2012** Step 1) 2012 서버의 경우 시작프로그램 목록 편집이 불가능하며 별도의 편집이나 등록을 위해서는 배치파일이나 레지스트리 값 추가를 이용해서 개인화를 통해 사용할 수 있으나 보안상 권장하지 않음.	
조치 시 영향	일반적인 경우 영향 없음

W-82 (중)	6. DB 관리 > 6.1 Windows 인증 모드 사용
취약점 개요	
점검내용	■ DB 로그인 시 Windows 인증 모드 적절성 점검
점검목적	■ 적절한 Windows 인증 모드를 적용하여 적합한 복잡성 수준을 유지하기 위함
보안위협	■ 혼합 인증모드를 사용하고 sa 계정이 활성화 되어 있는 경우, 잘 알려진 sa 계정에 대한 계정 추측 공격의 우려 존재
참고	※ 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 계정 ※ **kerberos 보안프로토콜:** 개방된 컴퓨터 네트워크 내에서 서비스 요구를 인증하기 위한 보안 시스템
점검대상 및 판단기준	
대상	■ Windows 2003, 2008, 2012
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
점검 및 조치 사례	

■ Windows 만 인증 활성화

< SQL Server 2005>

Step 1) 우클릭> 서버> 등록 정보> 보안 탭> 인증> 인증 모드> Windows만[W]를 클릭하여 활성화시킴

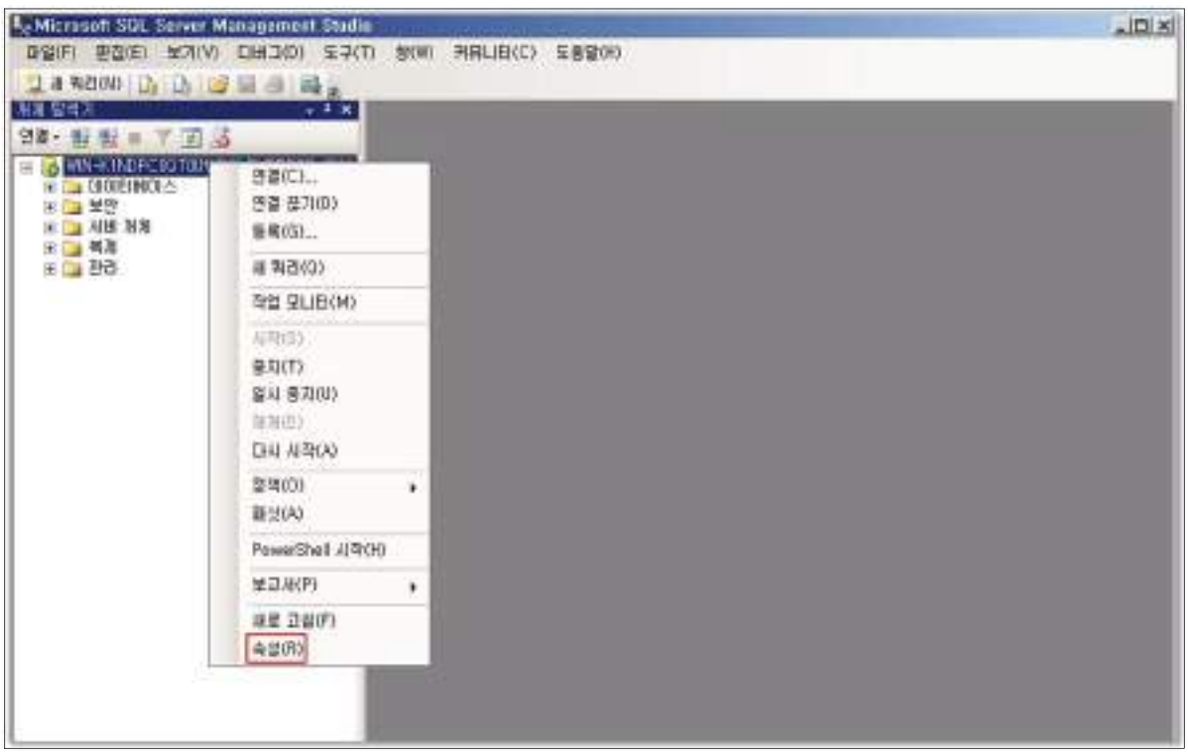


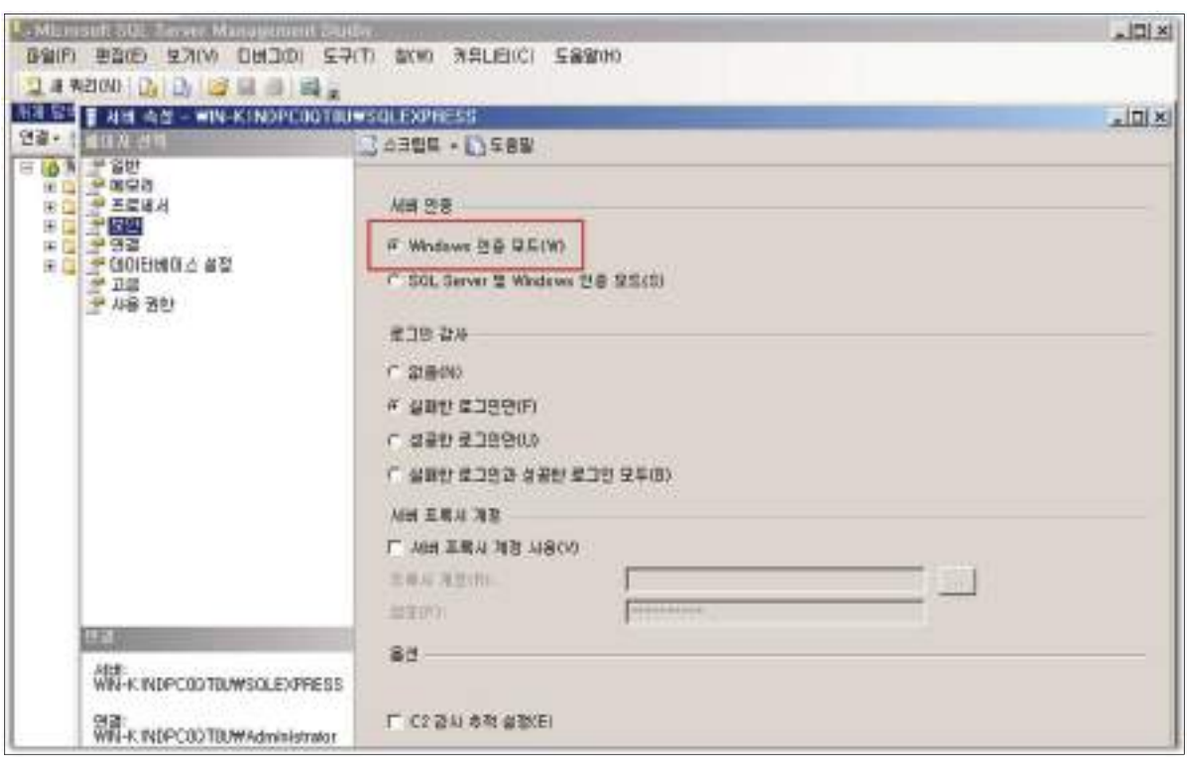
Windows 서버

W-82 (중)	6. DB 관리 > 6.1 Windows 인증 모드 사용

< SQL Server 2008>

Step 1) SQL Server 매니저 스튜디오> 해당 서버 우클릭> 속성> 보안> Windows 인증 활성화

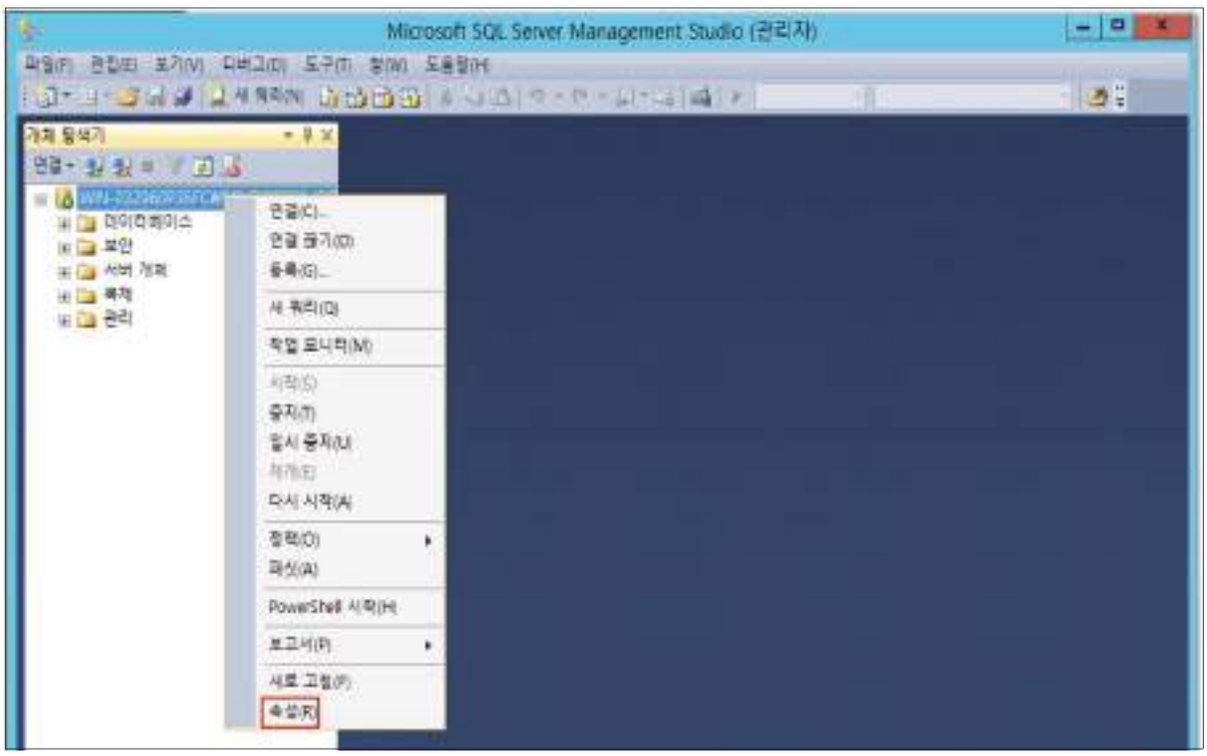


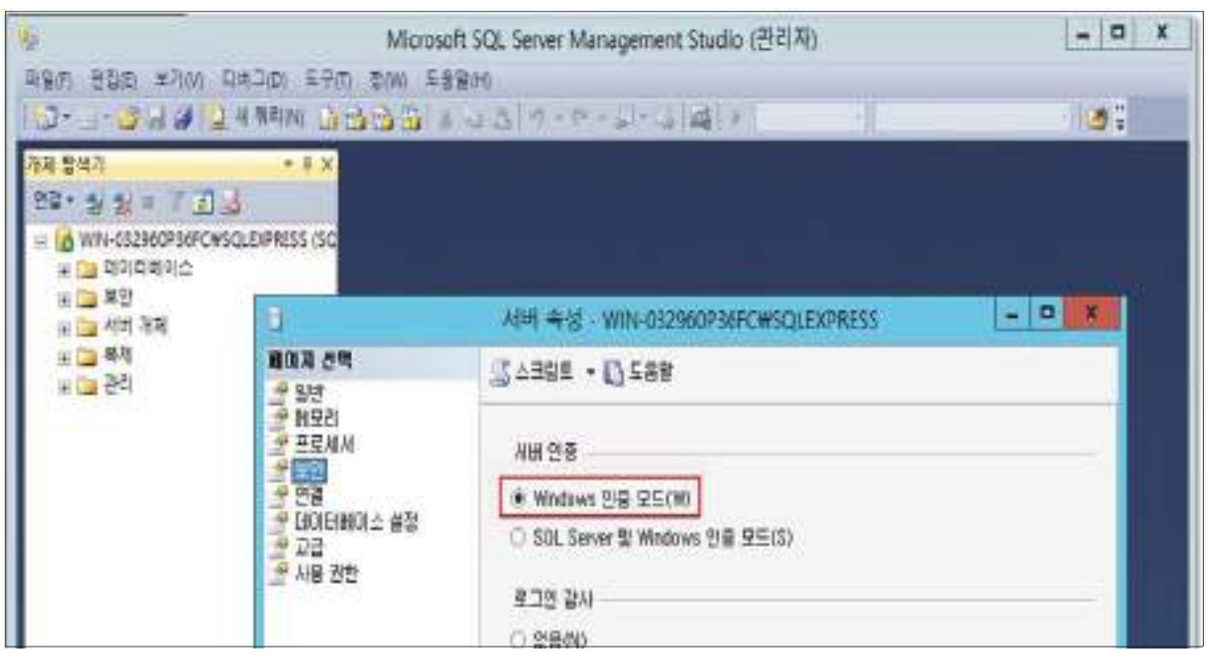


W-82 (중)	6. DB 관리 > 6.1 Windows 인증 모드 사용

< SQL Server 2012>

Step 1) SQL Server 매니저 스튜디오> 해당서버 우클릭> 속성> 보안 탭> 서버 인증> Windows 인증 모드(W)를 클릭하여 활성화시킴

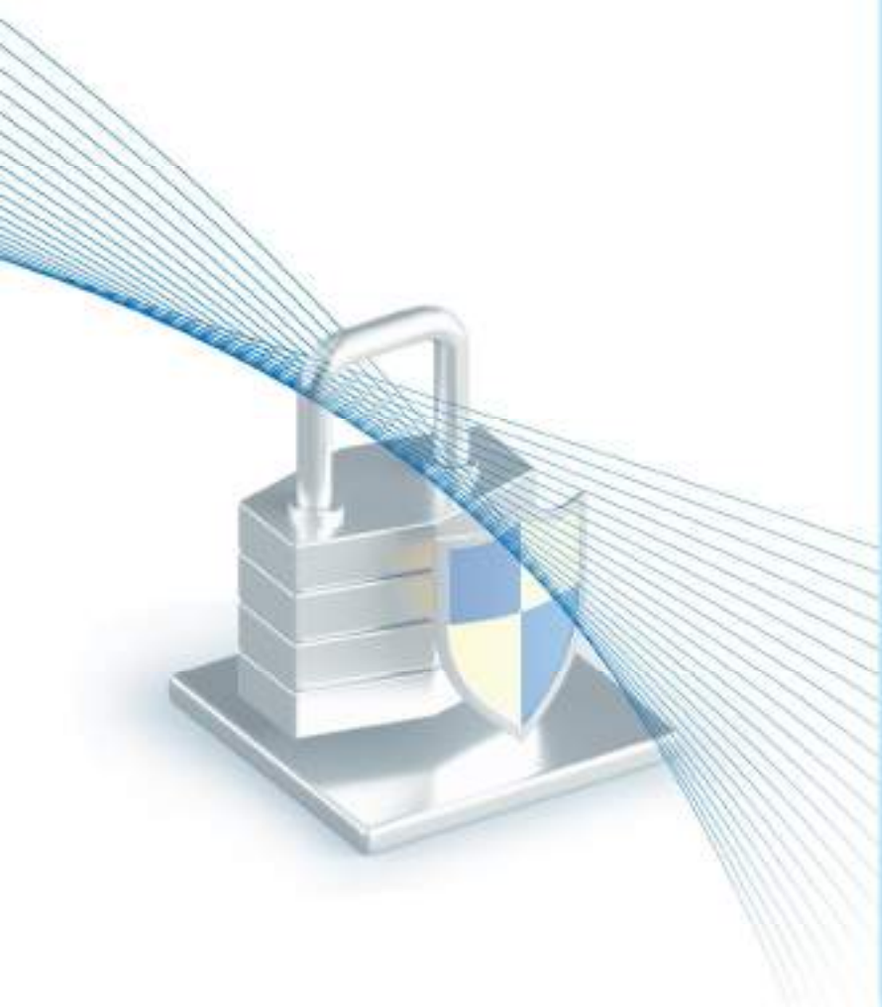




조치 시 영향	일반적인 경우 영향 없음

Ⅱ

보안장비



보안장비 취약점 분석·평가 항목

분류	점검항목	항목 중요도	항목코드
1. 계정관리	보안장비 Default 계정 변경	상	S-01
	보안장비 Default 패스워드 변경	상	S-02
	보안장비 계정별 권한 설정	상	S-03
	보안장비 계정 관리	상	S-04
2. 접근관리	로그인 실패횟수 제한	중	S-17
	보안장비 원격 관리 접근 통제	상	S-05
	보안장비 보안 접속	상	S-06
3. 패치관리	Session timeout 설정	상	S-07
4. 로그관리	벤더에서 제공하는 최신 업데이트 적용	상	S-08
	보안장비 로그 설정	중	S-18
	보안장비 로그 정기적 검토	중	S-19
	보안장비 로그 보관	중	S-20
	보안장비 정책 백업 설정	중	S-21
	원격 로그 서버 사용	중	S-22
	로그 서버 설정 관리	하	S-23
	NTP 서버 연동	중	S-24
5. 기능관리	정책 관리	상	S-09
	NAT 설정	상	S-10
	DMZ 설정	상	S-11
	최소한의 서비스만 제공	상	S-12
	이상징후 탐지 경고 기능 설정	상	S-13
	장비 사용량 검토	상	S-14
	SNMP 서비스 확인	상	S-15
	SNMP Community String 복잡성 설정	상	S-16
	부가 기능 설정	중	S-25
	유해 트래픽 차단 정책 설정	중	S-26

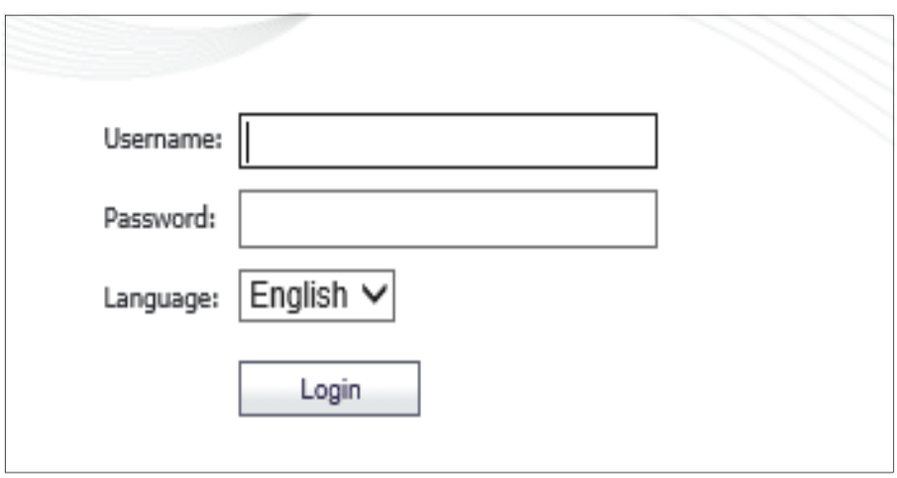
S-01 (상)	1. 계정관리 > 1.1 보안장비 Default 계정 변경
취약점 개요	
점검내용	■ 보안장비에 기본적으로 설정되어 있는 관리자 계정의 변경 여부 점검
점검목적	■ 보안장비의 기본 관리자 계정 패스워드는 인터넷이나 매뉴얼 등에 공개되어 있으므로 보안장비의 기본 관리자 계정을 변경하여 공격자가 기본 관리자 계정 정보를 통해 보안장비를 장악하지 못하게 하기 위함
보안위협	■ 보안장비의 기본 관리자 계정을 변경하지 않을 경우, 공격자가 공개된 기본 관리자 계정의 정보들을 통하여 보안장비에 불법적인 접근을 시도해 보안장비 설정 값을 변경함으로써 시스템 침입 경로 제공 및 보안장비를 무력화 할 수 있는 위험이 존재함
참고	※ **Default 계정:** 장비 제조업체에서 출고 시 설정되어 나오는 기본 관리자 계정정보
점검대상 및 판단기준	
대상	■ 방화벽, IPS, VPN 등
판단기준	**양호 :** 장비에서 제공하고 있는 디폴트 계정을 변경하여 사용하는 경우 (Default 계정 변경이 불가능 할 경우 기본 패스워드 변경으로 보완 필요)
	취약 : 장비에서 제공하고 있는 디폴트 계정을 변경이 가능함에도 변경하지 않고 사용하는 경우
조치방법	디폴트 계정 변경
점검 및 조치 사례	

■ **점검방법**

Step 1) Web을 통한 접속

Step 2) 디폴트 계정, 비밀번호 입력

Step 3) 접속 확인



보안장비

S-01 (상)	1. 계정관리 > 1.1 보안장비 Default 계정 변경

■ **조치방법**

Step 1) 보안장비에서 제공하고 있는 계정 메뉴에서 Default 계정 변경

Step 2) Default 계정 변경이 불가능 할 경우 기본 패스워드 변경으로 보완 필요

조치 시 영향	일반적인 경우 영향 없음

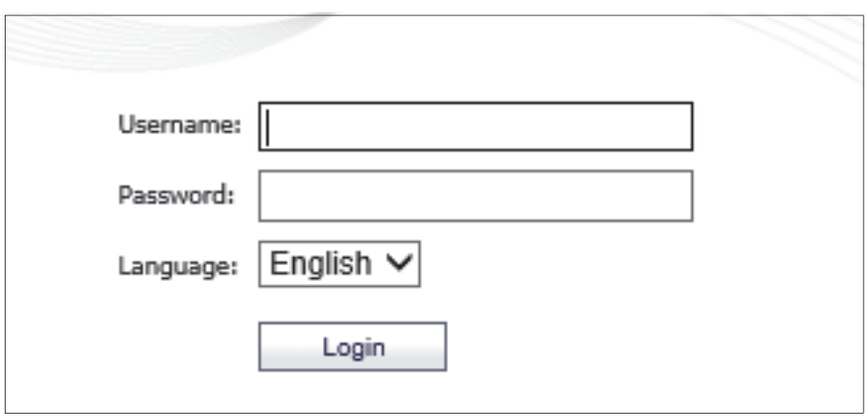
S-02 (상)	1. 계정관리 > 1.2 보안장비 Default 패스워드 변경
취약점 개요	
점검내용	■ 보안장비에 기본적으로 설정되어 있는 관리자 계정의 패스워드를 변경 없이 사용하고 있는지 점검
점검목적	■ 보안장비의 기본 관리자 계정 패스워드는 인터넷이나 매뉴얼 등에 공개되어 있으므로 보안장비의 기본 관리자 계정 패스워드를 변경하여 공격자가 기본 관리자 계정 정보를 통해 보안장비를 장악하지 못하게 하기 위함
보안위협	■ 보안장비의 기본 관리자 계정 패스워드를 변경하지 않을 경우, 공격자가 공개된 기본 관리자 계정의 정보를 이용하여 보안장비에 불법적인 접근을 시도해 보안장비 설정 값을 변경함으로써 시스템 침입 경로 제공 및 보안장비를 무력화 할 수 있는 위험이 존재함
참고	※ **Default 패스워드:** 장비 제조업체에서 출고 시 설정되어 나오는 기본 관리자 계정의 패스워드 정보
점검대상 및 판단기준	
대상	■ 방화벽, IPS, VPN 등
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
점검 및 조치 사례	

■ **점검방법**

Step 1) Web을 통한 접속

Step 2) 디폴트 계정, 비밀번호 입력

Step 3) 접속 확인

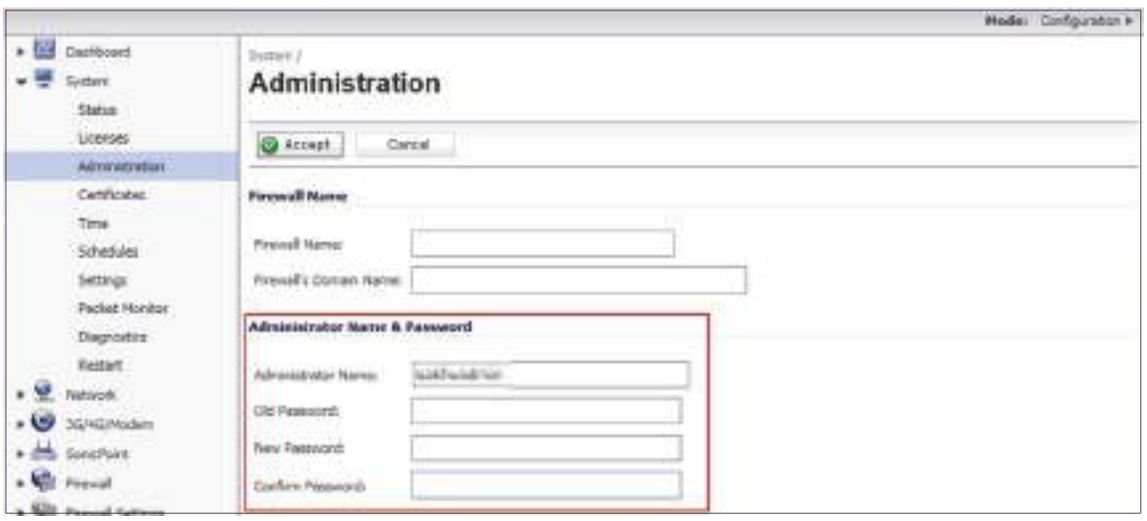


보안장비

S-02 (상)	1. 계정관리 > 1.2 보안장비 Default 패스워드 변경

■ **조치방법**

Step 1) 패스워드 메뉴에서 패스워드 변경



Step 2) 보안장비가 제공하는 범위에서 패스워드 설정
(특수문자, 숫자, 영소문자 포함 8자리 이상)

조치 시 영향	일반적인 경우 영향 없음

보안장비

S-03 (상)	1. 계정관리 > 1.3 보안장비 계정별 권한 설정
취약점 개요	
점검내용	■ 보안장비에 등록한 계정들에 대해 업무에 불필요한 권한 여부 점검
점검목적	■ 보안장비에 등록한 계정의 용도별 권한부여를 함으로써 권한 없는 사용자의 설정 변경으로 인한 시스템 침입 경로 유출 위험을 줄이고 관리자 계정이 아닌 일반계정이 공격자에게 탈취되었을 때 보안장비를 장악하지 못하게 하기 위함
보안위협	■ 보안장비 계정별 권한 설정이 없을 경우, 권한 없는 사용자의 의도하지 않은 보안정책 수정이나 보안장비 설정 값 변경을 통하여 공격자에게 시스템 침입 경로를 제공할 수 있음
참고	※ 관리자 권한은 최소한의 계정에만 부여
점검대상 및 판단기준	
대상	■ 방화벽, IPS, VPN 등
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
점검 및 조치 사례	

■ 점검방법

Step 1) 보안장비에서 제공하고 있는 계정 메뉴에서 계정별 권한 확인

■ 조치방법

Step 1) 보안장비에서 제공하고 있는 계정 메뉴에서 기존 계정의 권한 검토(불필요한 권한 삭제)

Step 2) 단일 계정을 여러 사용자가 공유 시 사용자별 계정 생성 및 권한 차등 부여

조치 시 영향	일반적인 경우 영향 없음

보안장비

S-04 (상)	1. 계정관리 > 1.4 보안장비 계정 관리
취약점 개요	
점검내용	■ 보안장비에 등록되어 있는 계정 중 사용하지 않는 계정을 제거 또는 관리하고 있는지 점검
점검목적	■ 사용하지 않는 불필요한 계정을 관리함으로써 관리되지 않은 계정을 통한 공격을 차단하기 위함
보안위협	■ 보안장비에 등록되어 있는 불필요한 계정을 관리하지 않을 경우, 공격자의 무작위 대입 방법이나 사전 대입 공격에 의해 불필요한 계정을 통한 접근 위험이 존재하며 공용계정 및 휴면계정이 존재할 경우 계정 탈취 시 침해사고 발생 때 사후 추적이 어려움
참고	※ 계정은 1인 1계정 사용을 원칙으로 운영해야 하며, 계정의 공용을 금지하여야 함
점검대상 및 판단기준	
대상	■ 방화벽, IPS, VPN 등
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
점검 및 조치 사례	

■ 점검방법

Step 1) 보안장비에서 제공하고 있는 계정 메뉴에서 계정 확인 및 담당자 인터뷰

■ 조치방법

Step 1) 사용하지 않는 계정 삭제

Step 2) 공용계정 사용 시 사용자별 계정 생성 및 시스템 접근 이력을 관리하여 책임 추적성 확보

※ 시스템이 아닌 사람을 중심으로 하는 통합된 계정관리가 중요함

조치 시 영향	일반적인 경우 영향 없음

S-05 (상)	2. 접근 관리 > 2.1 보안장비 원격 관리 접근 통제
취약점 개요	
점검내용	■ 보안장비 원격 관리 시 관리자 IP 또는 특정 IP 만 접근이 가능하도록 설정하였는지 점검
점검목적	■ 보안장비에 원격으로 접근할 수 있는 IP를 등록함으로써 비인가자의 보안장비 접근을 차단하고 보안장비에 접근이 허용된 특정인들만 보안장비에 접근을 가능하도록 하기 위함
보안위협	■ 보안장비 원격 관리 시 특정 IP만 접근 가능하도록 설정하지 않을 경우, 외부에 있는 공격자에 의해 계정이 탈취 당하였을 때 보안장비 접근이 가능하게 되어 보안장비 설정 값을 변경하여 보안장비를 무력화 시킬 수 있음
참고	※ 보안장비에서 제공하는 관리자 접근제한 기능을 통해 관리자 단말기 또는 콘솔 장비의 허용된 IP만을 등록하고 접근을 제한할 수 있음 ※ 보안장비 원격 관리를 원칙적으로 금지하나, 부득이 사용해야 하는 경우 원격접속을 허용할 IP나 계정을 제한하는 등 보안 대책을 강구하여 관리해야함
점검대상 및 판단기준	
대상	■ 방화벽, IPS, VPN 등
판단기준	**양호 :** 원격 관리 시 관리자 IP 또는 특정 IP만 접근 가능하도록 설정한 경우
	취약 : 원격 관리 시 관리자 IP 또는 특정 IP만 접근 가능하도록 설정하지 않은 경우
조치방법	원격 관리 시 관리자 및 특정 IP만 접근 가능하도록 함
점검 및 조치 사례	
■ 점검방법 Step 1) 보안장비에서 제공하고 있는 메뉴에서 접속 IP나 계정 제한 확인 **■ 조치방법** Step 1) 관리자 IP 또는 특정 IP 및 계정에서만 접속할 수 있도록 설정  	
조치 시 영향	일반적인 경우 영향 없음

보안장비

S-06 (상)	2. 접근 관리 > 2.2 보안장비 보안 접속
취약점 개요	
점검내용	■ 보안장비에 접속할 때 암호화 프로토콜을 이용하여 접속하는지 여부를 점검
점검목적	■ 보안장비 접속 시 평문 전송하는 Telnet, HTTP 접속을 사용하지 않고 데이터가 암호화되는 SSH, SSL 인증 등의 암호화 접속을 통하여 공격자의 데이터 스니핑에 대비하기 위함
보안위협	■ Telnet 또는 HTTP 통신은 암호화 전송이 아닌 평문 전송을 하므로 공격자가 스니핑을 시도 할 경우 관리자의 ID, 패스워드가 노출되어 악의적인 사용자가 관리자 계정을 탈취 할 수 있음
참고	※ **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 ※ **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 ※ 보안장비에 대한 원격 접속을 원칙적으로 금지하나, 부득이 원격 접속을 해야 하는 경우 암호화 통신 프로토콜 사용 등 보안 대책을 강구하여 접속해야함
점검대상 및 판단기준	
대상	■ 방화벽, IPS, VPN 등
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
점검 및 조치 사례	

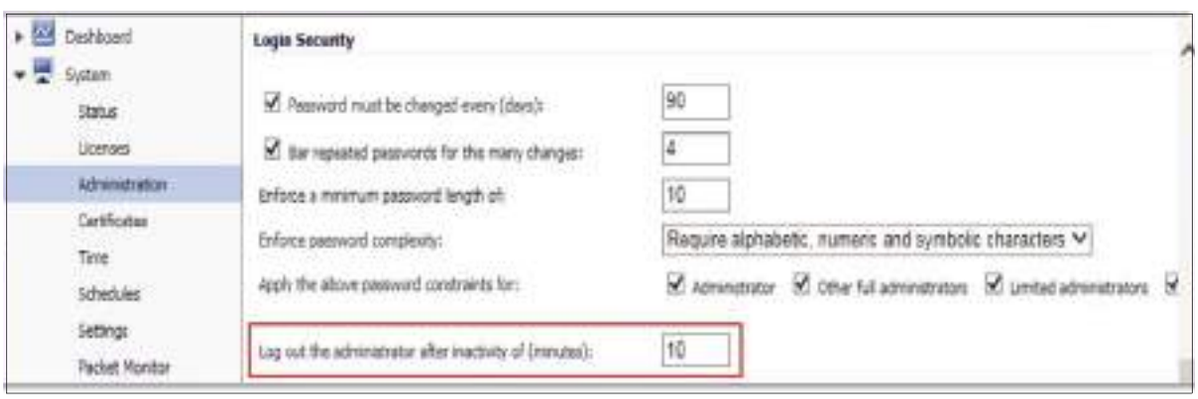
■ 점검방법

Step 1) HTTPS 또는 SSH 등 암호화 통신을 통한 접속 확인

■ 조치방법

Step 1) 보안장비 접속 시, 가능하다면 SSL 등의 암호화 접속 활용
(제품마다 상이하므로 벤더사에 문의)

조치 시 영향	일반적인 경우 영향 없음

S-07 (상)	2. 접근 관리 > 2.3 Session timeout 설정
취약점 개요	
점검내용	■ 보안장비의 정책에 Session timeout 설정을 적용하였는지 점검
점검목적	■ 보안장비 관리 작업을 완료 후 사용자의 부주의로 계정이 접속한 상태로 방치되는 경우를 방지하며 사용하지 않는 세션을 종료하여 가용성을 높이기 위함
보안위협	■ 보안장비에 접속한 사용자가 자리 이석을 하거나 불완전한 세션 종료를 했을 경우, 이석한 자리는 이미 보안장비에 접속한 상태이므로 권한 없는 사용자가 이석한 자리에서 보안정책 삭제나 변경 등 악의적인 행위를 하거나 불완전한 세션 종료를 한 세션 정보를 재사용하여 인증 없이 보안장비에 접근 할 수 있음
참고	※ **Session timeout**: 로컬 또는 원격에서 보안장비에 접속한 사용자가 일정시간 동안 통신이 없을 시 해당 세션을 종료시키는 설정 ※ 보안장비에 접속하여 이행하는 업무 특성을 고려하여 시간을 설정하도록 함
점검대상 및 판단기준	
대상	■ 방화벽, IPS, VPN 등
판단기준	**양호 :** Session Timeout 시간을 설정한 경우
	취약 : Session Timeout 시간을 설정하지 않은 경우
조치방법	Session Timeout 시간을 설정
점검 및 조치 사례	
■ **점검방법** Step 1) 벤더별 설정 값 확인. 대부분의 보안장비는 디폴트로 설정 되어 있음 Step 2) Console, SSL, VPN, SSH 등의 모든 원격 접근에 대한 Session Timeout 설정 확인  ■ **조치방법** Step 1) 보안장비가 제공하는 Session Timeout 기능 활성화 설정	
조치 시 영향	일반적인 경우 영향 없음

보안장비

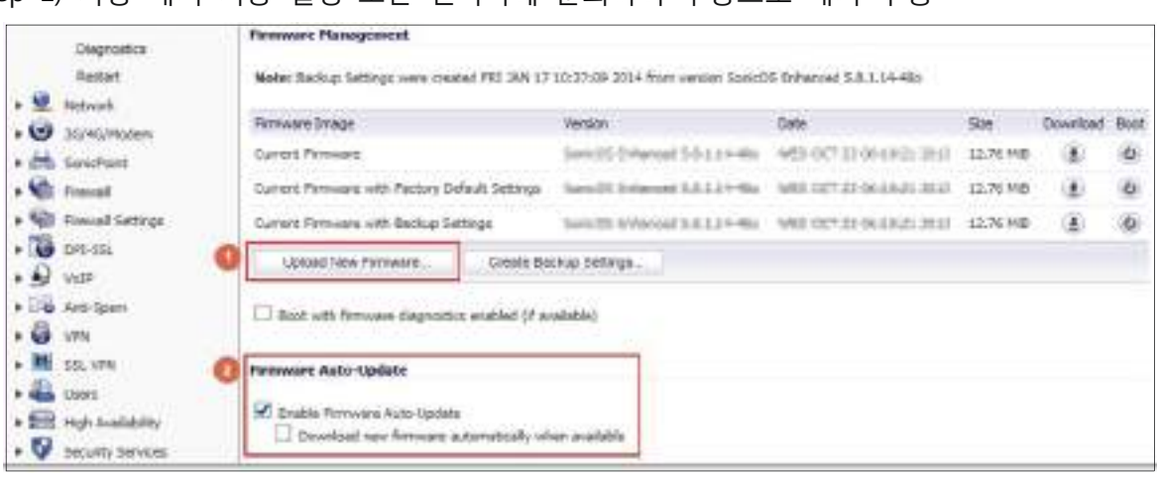
S-08 (상)	3. 패치 관리 > 3.1 벤더에서 제공하는 최신 업데이트 적용
취약점 개요	
점검내용	■ 보안장비 OS 및 보안 기능(IPS, 안티바이러스 등)의 버전을 최신 버전으로 유지하고 있는지 점검
점검목적	■ 최신 업데이트를 적용하여 보안장비 OS 취약점으로 발생하는 공격이나 보안장비로 유입되는 최신 유해 트래픽에 대한 탐지 및 차단을 하기 위함
보안위협	■ 보안장비 OS 및 보안 기능(IPS, 안티바이러스 등)의 버전을 최신 버전으로 유지하지 않을 경우 보안장비 OS 취약점을 이용한 공격이나 최신 유해 트래픽에 대한 탐지 및 차단이 제대로 이루어지지 않아 내부 정보시스템의 침해 위험이 존재함
참고	-
점검대상 및 판단기준	
대상	■ 방화벽, IPS, VPN 등
판단기준	**양호 :** 패치 적용 정책을 수립하여 주기적으로 패치를 관리하고 있을 경우
	취약 : 패치 적용 정책을 수립하여 주기적으로 패치를 관리하고 있지 않을 경우
조치방법	벤더사에서 주기적으로 제공하는 장비별 최신 취약점 정보를 파악 후 최신 패치 및 업그레이드를 수행
점검 및 조치 사례	

■ 점검방법

Step 1) 보안장비의 최신 패치 현황 파악 또는 벤더사에 문의하여 최신 패치 현황 파악

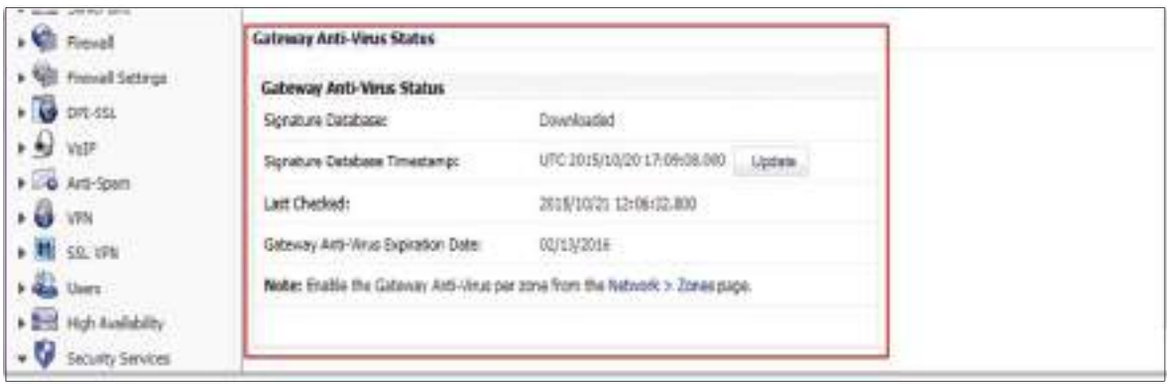
■ 조치방법

Step 1) 자동 패치 기능 설정 또는 벤더사에 문의하여 수동으로 패치 수행

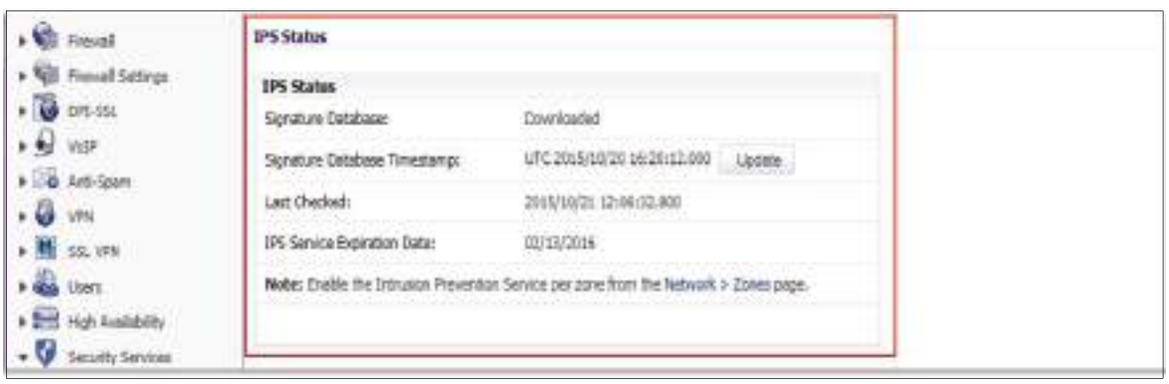


[No1. 수동으로 패치 수행, No2. 자동으로 패치 기능 설정]

S-08 (상)	3. 패치 관리 > 3.1 벤더에서 제공하는 최신 업데이트 적용



[Anti-virus 패치]



[IPS 패치]

조치 시 영향	최신 업데이트 적용 시 시스템 재시작 등의 서비스 영향도 검토 필요

보안장비

S-09 (상)	5. 기능관리 > 5.1 정책 관리
취약점 개요	
점검내용	■ 보안장비 정책에 미사용 및 중복된 정책이 존재하는지 점검
점검목적	■ 주기적인 정책 검토를 통해 미사용 및 중복된 정책을 제거하여 향후 발생 가능한 보안 위협을 제거하고 보안장비의 고가용성을 유지하기 위함
보안위협	■ 미사용 및 중복된 정책을 제거하지 않는 경우, 보안장비 관리자의 업무 편의성 및 효율성이 저하되며 설정되어 있는 정책 중 관리자가 인지하지 못한 정책으로 인해 네트워크 보안 체계가 약화될 수 있음
참고	※ **발생 가능한 보안 위협:** 비인가자의 네트워크 접근 및 내부 정보 유출, 악성코드 삽입 등 ※ 관련 점검 항목 : A-92(하)
점검대상 및 판단기준	
대상	■ 방화벽, IPS 등
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
점검 및 조치 사례	
■ **점검방법** Step 1) 정책에 대한 주기적인 검사로 미사용 & 중복된 정책 확인 ■ **조치방법** Step 1) 보안장비 정책의 주기적인 검사 및 미사용 & 중복된 정책 제거 Step 2) 정책 관리 방법 1. 보안장비 정책 입력 시 IP 대신 이름을 사용하도록 함(예. 그룹명: OOO 부서, OOO 팀, OOO 팀의 OOO 등) 2. 공통 정책은 그룹으로 관리하도록 함 3. 사용빈도가 높은 정책은 정책 설정 시 상단에 위치하도록 함 4. 위 내용을 포함한 정책에 대해 주기적으로 점검하도록 함	
조치 시 영향	일반적인 경우 영향 없음

보안장비

S-10 (상)	5. 기능관리 > 5.2 NAT 설정
취약점 개요	
점검내용	■ 외부 공개 필요성이 없는 정보시스템에 NAT 설정 여부를 점검
점검목적	■ 외부 침입자가 내부 시스템을 공격하기 위해서는 내부 사설 IP를 알아야 하므로 NAT 설정을 통해 내부 네트워크를 보호할 수 있음
보안위협	■ NAT 설정을 하지 않을 경우, 공인 IP를 통해 시스템에 접근 가능하여 정보 유출, 시스템 파괴, 악성코드 전파 등의 불법적 행위가 발생할 수 있음
참고	※ **NAT 사용 목적:** 1) 인터넷의 공인 IP 주소 절약 2) 공공망과 연결되는 사용자들의 고유한 사설망을 침입자들로부터 보호
점검대상 및 판단기준	
대상	■ 방화벽 등
판단기준	**양호 :** 외부 공개 필요성이 없는 서버, 단말기 등 정보시스템에 대해 NAT 설정을 적용한 경우
	취약 : 외부 공개 필요성이 없는 서버, 단말기 등 정보시스템에 대해 NAT 설정을 적용하지 않은 경우
조치방법	외부 공개 필요성이 없는 정보시스템에 대해 공인 IP 지정 여부를 확인하여 사설 IP 로 변경한 후 보안장비에서 NAT 설정을 적용
점검 및 조치 사례	

■ 점검방법

Step 1) 공인 IP 확인 사이트(포털 등)에 접속하여 사용 중인 단말의 IP 확인

■ 조치방법

Step 1) 대부분의 네트워크 보안 제품들은 NAT 기술을 기본으로 채택하고 있으므로 내부 사설 IP 부여 정책에 맞춰 적용하도록 함

[Source IP의 NAT 적용]

보안장비

S-10 (상)	5. 기능관리 > 5.2 NAT 설정

[Destination IP 의 NAT 적용]

조치 시 영향	일반적인 경우 영향 없음

보안장비

S-11 (상)	5. 기능관리 > 5.3 DMZ 설정
취약점 개요	
점검내용	■ 내부 네트워크와 외부 서비스 네트워크(DMZ)를 구분 하고 있는지 점검
점검목적	■ 외부 네트워크로 서비스를 제공하는 호스트에서 내부 네트워크로의 접근이 통제되고 있는지 확인하기 위함
보안위협	■ DMZ 설정을 통해 내부 네트워크와 외부 서비스 네트워크를 구분하도록 설정되어 있지 않은 경우, 외부 네트워크를 통해서 서비스를 제공받는 악의적인 사용자가 DMZ 내 호스트를 통해 내부 네트워크로 불법적 연결을 시도할 수 있음
참고	※ **DMZ:** 조직의 내부 네트워크와 외부 네트워크 사이에 위치하는 네트워크 망으로 DMZ 내 컴퓨터는 외부 네트워크에만 연결할 수 있도록 하고, 내부 네트워크로는 연결할 수 없도록 구성함
점검대상 및 판단기준	
대상	■ 방화벽 등
판단기준	**양호 :** DMZ를 구성하여 내부 네트워크를 보호하는 경우
	취약 : DMZ를 구성하지 않고 사설망에서 외부 공개 서비스를 제공하는 경우
조치방법	DMZ를 구성하여 내부 네트워크와 외부 서비스 네트워크 분리 ※물리적(망분리)으로 내부 네트워크와 외부 서비스 네트워크가 분리 되어 있을 경우 해당 없음
점검 및 조치 사례	

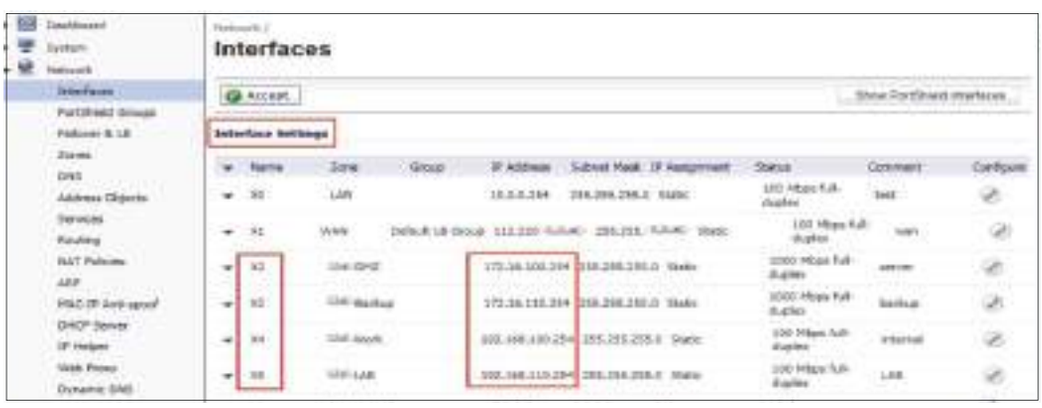
■ 점검방법

Step 1) 네트워크 구성도 또는 방화벽 설정 확인

■ 조치방법 1> 방화벽 옵션 설정

Step 1) 방화벽의 옵션 설정

각각의 네트워크는 방화벽에 서로 다른 포트를 사용하여 연결하는데 이를 삼각 방화벽 설정(three-legged firewall set-up)이라 함



보안장비

S-11 (상)	5. 기능관리 > 5.3 DMZ 설정
■ **조치방법 2> 두 개의 방화벽 사용** Step 1) 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(screened-subnet firewall)이라고 함	
조치 시 영향	일반적인 경우 영향 없음

보안장비

S-12 (상)	5. 기능관리 > 5.4 최소한의 서비스만 제공
취약점 개요	
점검내용	■ 방화벽에서 필요한 서비스만 제공하고 있는지 점검
점검목적	■ 방화벽 정책을 검토하여 사용하지 않는 IP와 Port를 제거하여 네트워크 및 시스템 운영의 보안성을 유지하기 위함
보안위협	■ 필요한 서비스를 제외한 다른 서비스가 활성화 될 경우, 이를 통해 해커의 침입 또는 악성 소프트웨어 전달 등의 보안 위험이 발생 할 수 있음
참고	※ **방화벽 기존 정책:** 방화벽은 기본적으로 all deny 설정을 적용하며 허용할 port와 IP만 추가함으로써 관리 포인트를 최소화 함
점검대상 및 판단기준	
대상	■ 방화벽, IDS 등
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 허용하도록 설정함
점검 및 조치 사례	

■ **점검방법**

Step 1) 방화벽에서 허용되지 않은 포트 접속 확인

■ **조치방법**

Step 1) 방화벽 기본 정책인 all deny에 최소 서비스만 허용 확인
(허용된 IP와 서비스 포트만 오픈, 모든 IP 및 서비스 허용 금지)

조치 시 영향	허용되지 않은 접속은 모두 차단됨

보안장비

S-13 (상)	5. 기능관리 > 5.5 이상징후 탐지 경고 기능 설정
취약점 개요	
점검내용	■ 보안장비에 이상 징후 탐지 경고 기능이 설정되어 있는지 점검
점검목적	■ 이상징후가 탐지되는 경우 사고 예방 및 신속한 조치를 이행하기 위함
보안위협	■ 이상징후 탐지 시 경고 기능이 설정되지 않을 경우, 보안사고 미연 방지 및 IT 컴플라이언스를 준수하기가 어려워 질 수 있음
참고	※ **보안사고 미연 방지 및 IT 컴플라이언스 준수** **예시 1)** 휴일 또는 업무 시간 이외에 비정상적인 패턴으로 중요 문서 또는 고객정보 DB에 접근한다면 정보유출 징후가 있다고 판단 가능함 **예시 2)** 퇴직 징후가 의심스러운 직원이 휴일이나 업무시간 외에 비정상적으로 중요 문서나 고객 DB에 접근하는 경우 정보유출 가능성이 높기 때문에 이를 사전에 탐지하고 예방할 수 있음
점검대상 및 판단기준	
대상	■ 방화벽, IPS 등
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
점검 및 조치 사례	

■ 점검방법

Step 1) 보안장비의 실시간 알람, 이메일, SMS 경고 기능 설정 확인

■ 조치방법

Step 1) 24시간 모니터링을 통한 검사가 여건상 어려울 경우 이메일이나 SMS를 통한 경고 기능 설정으로 대체

조치 시 영향	일반적인 경우 영향 없음

보안장비

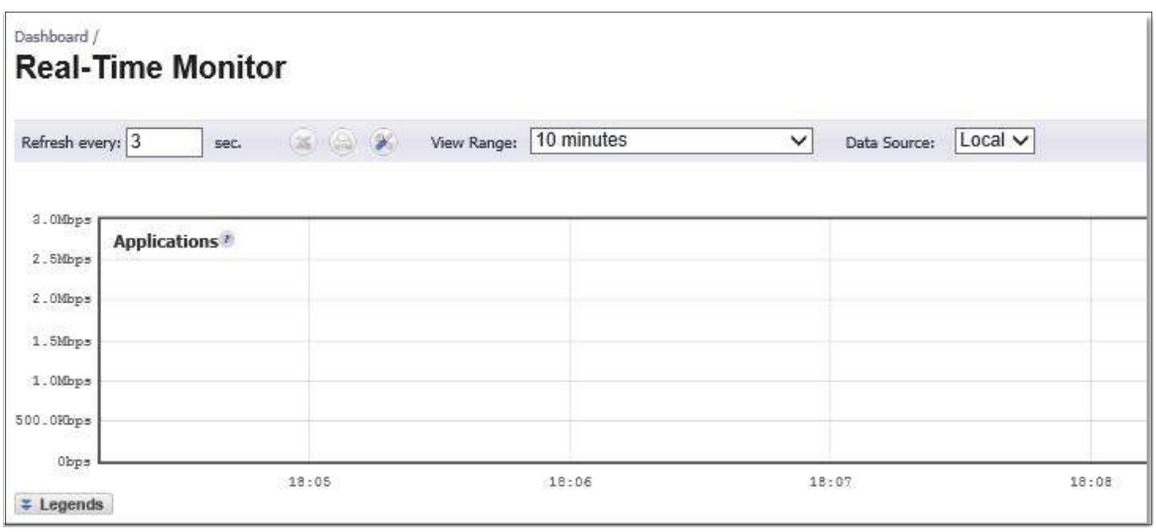
S-14 (상)	5. 기능관리 > 5.6 장비 사용량 검토
취약점 개요	
점검내용	■ 보안장비에서 제공하는 Dashboard를 통해 보안장비의 가용성에 대한 실시간 검토 여부 점검
점검목적	■ 보안장비의 가용성에 대한 검토로 인해 네트워크 트래픽의 수준을 파악하게 되고, 그에 따른 가용성 향상을 고려할 수 있음
보안위협	■ 정기적으로 가용성에 대한 검토를 하지 않을 경우, 성능 및 회선 상태를 파악할 수 없어 보안장비의 가용성 하락이 발생할 가능성이 존재함
참고	※ 내부 정책에 맞게 일, 주, 월 등의 주기를 정하여 정기적으로 이행하도록 하며 일반적으로 월 1회 검토를 권고함
점검대상 및 판단기준	
대상	■ 방화벽, IPS, VPN 등
판단기준	**양호 :** 보안장비 가용성을 정기적으로 모니터링 및 검토할 경우
	취약 : 보안장비 가용성을 정기적으로 모니터링 및 검토하지 않을 경우
조치방법	장비 사용량을 정기적으로 모니터링
점검 및 조치 사례	

■ 점검방법

Step 1) 보안장비의 실시간 알람, 이메일, SMS 경고 기능 설정 확인

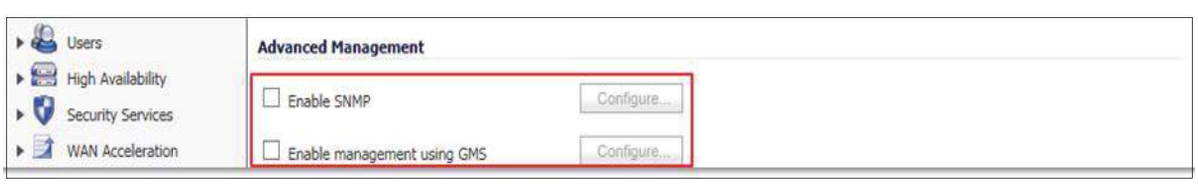
■ 조치방법

Step 1) 보안장비의 Web Dash Board 모니터링



조치 시 영향	일반적인 경우 영향 없음

보안장비

S-15 (상)	5. 기능관리 > 5.7 SNMP 서비스 확인
취약점 개요	
점검내용	■ SNMP 서비스 사용 여부 점검
점검목적	■ 보안장비 관리를 위해 NMS 솔루션과의 연동으로 SNMP 서비스 사용이 필요한 경우가 아니라면 서비스를 중지하도록 함
보안위협	■ UDP 프로토콜을 사용하는 SNMP 서비스를 활성화 할 경우 DoS공격, 보안장비 성능 저하, 크래쉬, 리로드 등의 여러 공격에 취약할 수 있음
참고	※ **SNMP 서비스:** 네트워크 관리를 위한 프로토콜로 네트워크 상의 서버, 프린터, 허브, 스위치, 라우터와 같은 네트워크 장치를 구성하고 정보를 수집하는데 사용됨 ※ SNMP 서비스를 이용해야 할 경우 Community String을 유추가 불가능하게 설정
점검대상 및 판단기준	
대상	■ 방화벽, IPS, VPN 등
판단기준	**양호 :** SNMP 서비스를 불필요하게 사용하지 않는 경우
	취약 : SNMP 서비스를 불필요하게 사용할 경우
조치방법	불필요한 경우 SNMP 서비스 중지
점검 및 조치 사례	
■ **점검방법** Step 1) 보안장비의 SNMP 설정 메뉴에서 확인 ■ **조치방법** Step 1) 불필요하다면 SNMP 서비스를 중지하고, 관리를 위해 NMS 솔루션과의 연동이 필요하다면 SNMP 설정  	
조치 시 영향	일반적인 경우 영향 없음

보안장비

S-16 (상)	5. 기능관리 > 5.8 SNMP Community String 복잡성 설정
취약점 개요	
점검내용	■ SNMP Community String 이 유추하기 어렵게 설정되어 있는지 점검
점검목적	■ SNMP Community String 을 유추하기 어렵도록 설정하여 네트워크상에서 시스템 정보가 비인가자에게 노출되지 않도록 함
보안위협	■ 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
참고	※ **SNMP 버전:** v1, v2 ,v3 이 존재하는데 v1, v2 는 community string을 평문 전송하지만 v3 은 암호화가 설정되어 해쉬 값으로 전송함
점검대상 및 판단기준	
대상	■ 방화벽, IPS, VPN 등
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
점검 및 조치 사례	

■ 점검방법

Step 1) 보안장비의 SNMP 설정 메뉴에서 커뮤니티 스트링 확인

■ 조치방법

Step 1) 보안 장비는 SNMP 취약성이 존재하므로 누구나 추측하기 어렵고 의미가 없는 문자열, 영문자 혼합으로 변경 권고

Step 2) 보안장비의 SNMP 설정에서 커뮤니티 이름 변경

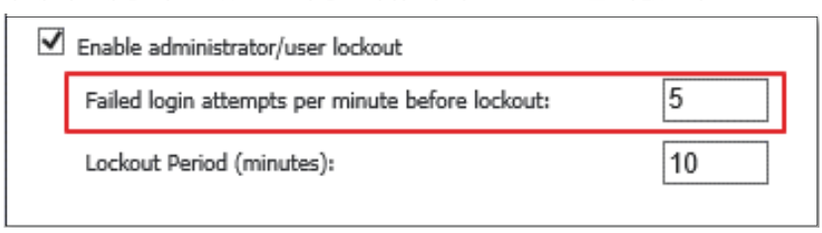
조치 시 영향	일반적인 경우 영향 없음

보안장비

S-17 (중)	1. 계정관리 > 1.5 로그인 실패횟수 제한
취약점 개요	
점검내용	■ 보안장비에서 제공하고 있는 로그인 임계값 설정의 활성화 여부 점검
점검목적	■ 보안장비에서 제공하는 로그인 실패횟수 제한 기능을 사용하여 공격자의 자동화 툴을 이용한 패스워드 대입 공격을 막기 위함
보안위협	■ 로그인 실패횟수 제한 기능을 활성화 하여 사용하지 않을 경우, 공격자는 자동화된 방법을 통하여 무작위 대입 공격이나 사전 대입 공격 등을 시도하여 계정의 패스워드를 탈취할 수 있음
참고	※ 기종에 따라 Limited/Lockout로 표시됨 ※ 보안장비에 계정 잠금시간 기능을 지원할 시 함께 설정하면 보안성이 향상됨
점검대상 및 판단기준	
대상	■ 방화벽, IPS, VPN 등
판단기준	**양호 :** 로그온 실패횟수를 5회 이하로 제한한 경우
	취약 : 로그온 실패횟수를 5회 이하로 제한하지 않은 경우
조치방법	로그온 실패횟수를 5회 이하로 제한
점검 및 조치 사례	

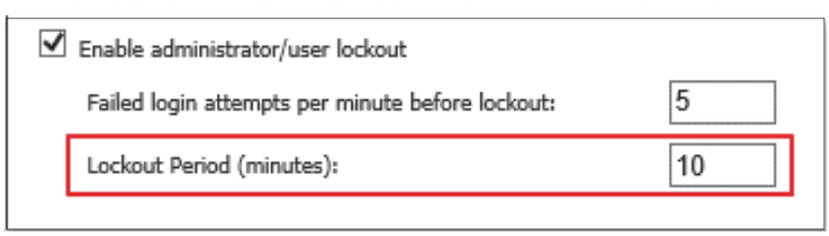
■ 점검방법

Step 1) 보안장비에서 제공하고 있는 계정 메뉴에서 로그인 임계값 확인



■ 조치방법

Step 1) 보안장비에서 제공하고 있는 계정 메뉴에서 Lockout 기능 설정



조치 시 영향	일반적인 경우 영향 없음

S-18 (중)	4. 로그 관리 > 4.1 보안장비 로그 설정
취약점 개요	
점검내용	■ 보안장비에 로그 설정이 적용되어 있는지 확인하고 로그 정책이 기관 정책에 맞게 적용 되어 있는지 점검
점검목적	■ 로그 설정을 점검하여 보안장비의 이상 유무와 보안장비 및 보안장비에 의해 보호받고 있는 정보시스템에 대한 비인가자의 침입 및 공격을 식별하고 있는지 확인하기 위함
보안위협	■ 로그 설정이 적용되어 있지 않을 경우 보안장비에 장애가 발생하거나 보안장비 및 보안장비에 의해 보호받고 있는 정보시스템에 대한 침해가 발생했을 경우 원인 분석이 어려움
참고	※ **로그 정책 설정:** 로그 정책 설정 시 보안장비에 대한 접근 이력(날짜, 시간, IP, ID, 명령어 이력 등), 보안 장비 성능 이상 유무(CPU, RAM 사용량 등), 보안장비를 통해 유입되거나 외부로 나가는 트래픽에 대해 로그가 남도록 설정하는 것을 권장 ※ 관련 점검 항목 : A-20(상), S-22(중)
점검대상 및 판단기준	
대상	■ 방화벽, IPS, VPN 등
판단기준	**양호 :** 기관 정책에 따른 로그 설정이 되어 있는 경우
	취약 : 기관 정책에 따른 로그 설정이 되어 있지 않은 경우
조치방법	기관 정책에 따른 로깅 설정
점검 및 조치 사례	

■ 점검방법

Step 1) 보안장비의 로그 설정 메뉴 확인

■ 조치방법

Step 1) 기관 정책에 따른 로깅 설정 (각 벤더별 설정 방법이 상이 함)

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

보안장비

S-19 (중)	4. 로그 관리 > 4.2 보안장비 로그 정기적 검토
취약점 개요	
점검내용	■ 로그 분석 도구(보안장비 로그 모니터링 기능, 로그 분석 프로그램 등)를 이용하여 보안장비 로그를 정기적으로 검토하는지 점검
점검목적	■ 정기적으로 로그 검토를 이행하는지 점검하여 보안장비의 이상 유무와 비인가자의 공격 및 침입을 식별하고 있는지 확인하기 위함
보안위협	■ 로그 검토를 이행하지 않을 경우 보안장비에 이상이 발생했을 경우와 보안장비 및 보안장비에 의해 보호받고 있는 정보시스템에 침해 사고가 발생했을 경우 원인 식별이 어려워지고 사전에 탐지할 수 없음
참고	※ **정기적 검토:** 정기적 검토 간격은 기관의 정책에 따라 달라질 수 있으나 매달 1번 이상 검토하는 것을 권고함
점검대상 및 판단기준	
대상	■ 방화벽, IPS, VPN 등
판단기준	**양호 :** 로그 검토를 정기적으로 이행하는 경우
	취약 : 로그 검토를 정기적으로 이행하지 않는 경우
조치방법	보안장비 로그를 정기적으로 분석하여 보관
점검 및 조치 사례	
■ 점검방법 Step 1) 보안장비의 로그를 정기적으로 분석하여 보관하는지 확인 **■ 조치방법** Step 1) 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

S-20 (중)	4. 로그 관리 > 4.3 보안장비 로그 보관
취약점 개요	
점검내용	■ 로그 보관 정책에 따라 적절하게 로그를 보관하는지 점검
점검목적	■ 로그 보관 설정을 점검하여 로그 검토나 보안장비 침해 사고 원인 분석에 필요한 (3개월 이상) 로그를 안전(삭제, 변경 불가)하게 보관하는지 확인하기 위함
보안위협	■ 로그 보관 기간이 적용되어 있지 않은 경우 보안장비에서 로그를 자동으로 삭제하여 로그 검토나 보안장비 침해 사고 원인 분석 시 필요한 로그가 남아 있지 않아 로그 검토나 사고 원인 분석이 어려워질 수 있음
참고	※ **로그 보관 기간:**「정보통신망 이용촉진 및 정보보호 등에 관한 법률」제45조 제2항에 따른 미래창조과학부 고시「정보보호조치에 관한 지침 [별표1] 보호조치의 구체적인 내용 2.2.10 로그관리」에 따라 최소 1개월 이상 로그기록 유지·관리(정보보호시스템은 3개월) 하도록 정함
점검대상 및 판단기준	
대상	■ 방화벽, IPS, VPN 등
판단기준	**양호 :** 정책에 따라 로그 보관 설정이 되어 있는 경우
	취약 : 로그 보관 정책이 없고, 관리되고 있지 않는 경우
조치방법	보안장비 로그 보관 설정에서 로그 저장기간 확인 및 변경 (별도의 장비에 보관하고 있다면 로그 보관 정책에 맞게 보관 설정)
점검 및 조치 사례	

■ 점검방법

Step 1) 보안장비의 보관된 로그 날짜 확인

■ 조치방법

Step 1) 보안장비 로그 보관 설정에서 로그 저장기간 확인 및 변경
(별도의 장비에 보관하고 있다면 로그 보관 정책에 맞게 보관 설정)

※ 각 벤더마다 설정 방법 상이

조치 시 영향	일반적인 경우 영향 없음.

보안장비

S-21 (중)	4. 로그 관리 > 4.4 보안장비 정책 백업 설정
취약점 개요	
점검내용	■ 보안장비 설정 정보가 저장되어 있는 파일을 백업하는지 점검
점검목적	■ 보안장비 설정 파일의 백업 유무를 점검하여 보안장비 또는 보안장비와 연결된 정보시스템에 문제(장비 이상으로 인해 장비를 교체할 경우, 보안장비 설정을 실수로 잘못 변경하여 문제가 생긴 경우, 비인가자의 공격 및 침입에 의한 설정 변경 및 삭제 등의 침해 사고가 발생했을 경우 등) 발생 시 백업된 설정 파일을 통해 즉시 복구 가능하도록 대비하고 있는지 확인하기 위함
보안위협	■ 설정 파일을 백업 해놓지 않을 경우 보안장비에 문제 발생 시 즉시 설정 복구가 되지 않아 보안장비에 연결된 정보시스템의 가용성(예: 웹서버 서비스 불가)에 영향을 미칠 수 있는 위험이 존재함
참고	※ **보안 장비 설정 파일:** 보안장비의 각종 설정 및 정책(룰셋)이 저장되어 있는 파일. 보안장비가 문제가 발생했을 경우 복구하는 용도로 활용
점검대상 및 판단기준	
대상	■ 방화벽, IPS, VPN 등
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
점검 및 조치 사례	

■ 점검방법

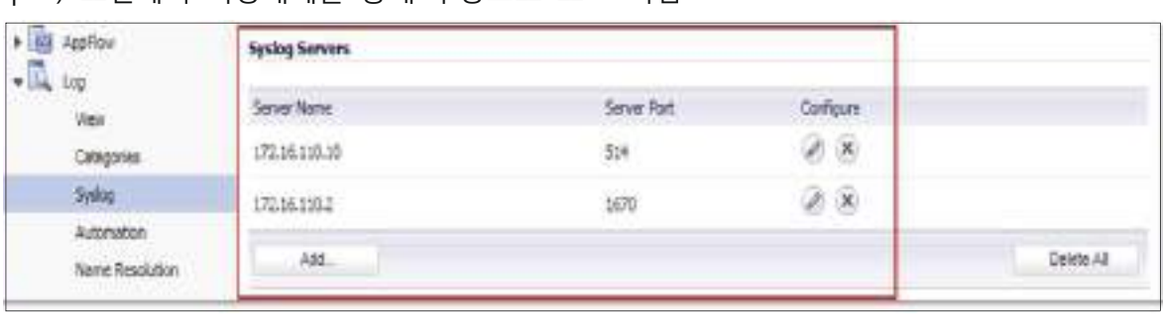
Step 1) 보안장비에 적용된 정책을 별도의 파일로 보관하는지 확인

■ 조치방법

Step 1) 보안장비 설정 메뉴에서 정책 백업 설정. 별도의 파일로 보관

※ 각 벤더마다 설정 방법 상이

조치 시 영향	일반적인 경우 영향 없음

S-22 (중)	4. 로그 관리 > 4.5 원격 로그 서버 사용
취약점 개요	
점검내용	■ 보안 장비 로그 설정(syslog)에 원격 로그 서버로 보안장비 로그를 별도 보관하도록 설정되어 있는지 점검
점검목적	■ 보안 장비 로그를 원격 로그 서버에 별도 보관하도록 설정되어 있는지 점검하여 보안장비에 문제(장비 이상, 비인가자의 공격 및 침해 등)가 생겨 발생할 수 있는 로그 삭제나 변조 위험에 대비하고 있는지 확인하기 위함
보안위협	■ 원격 로그 서버에 로그를 별도 보관하도록 설정되어 있지 않을 경우 보안장비 문제 발생 시 로그가 삭제되거나 변조되어 사고 원인 분석에 어려움이 발생함
참고	※ **원격 로그 서버:** 정보시스템(서버, 네트워크, 보안장비 등)의 로그를 통합적으로 보관하는 서버
점검대상 및 판단기준	
대상	■ 방화벽, IPS, VPN 등
판단기준	**양호 :** 별도의 로그 서버를 구축하여 통합 로그관리를 하는 경우
	취약 : 별도의 로그 서버가 없는 경우
조치방법	보안장비 로그 설정 메뉴에서 syslog 설정 또는 주기적으로 별도 저장매체에 백업(syslog 지원하지 않을 경우)
점검 및 조치 사례	
■ **점검방법** Step 1) 보안장비 로그 설정 메뉴에서 syslog 설정 확인 ■ **조치방법** Step 1) 원격 syslog 로그 수집 서버 설정 Step 2) 로컬에서 저장매체를 통해 수동으로 로그 백업 	
조치 시 영향	일반적인 경우 영향 없음

보안장비

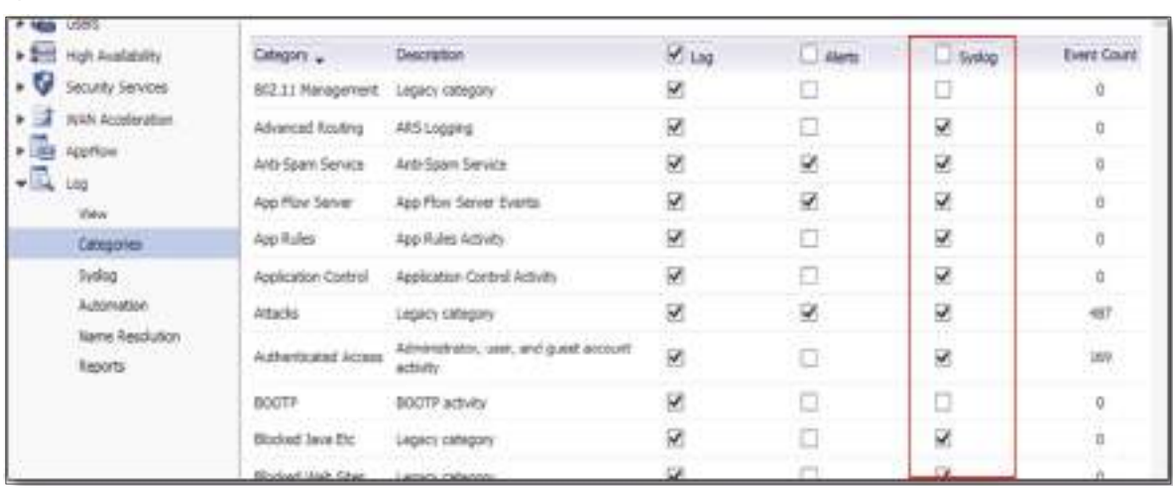
S-23 (하)	4. 로그 관리 > 4.6 로그 전송 설정 관리
취약점 개요	
점검내용	■ 로그 서버에 저장될 로그 설정이 기관의 정책에 맞게 설정되어 있는지 점검
점검목적	■ 보안장비와 연결된 로그 서버가 기관의 정책에 맞게 로그를 저장 할 수 있도록 설정되어 있는지 확인하기 위함
보안위협	■ 로그 서버에 기관의 정책에 맞는 로그를 보관하도록 설정되어 있지 않을 경우 비인가자의 공격 및 침입 사고가 발생했을 시 로그 검토나 사고 원인 분석이 어려워질 수 있음
참고	-
점검대상 및 판단기준	
대상	■ 방화벽, IPS, VPN 등
판단기준	**양호 :** 로그 서버에 저장될 로그가 기관 정책에 맞게 설정되어 있을 경우
	취약 : 로그 서버에 저장될 로그가 기관 정책에 맞게 설정되어 있지 않을 경우
조치방법	기관의 정책에 맞게 로그 서버에 저장될 로그를 설정
점검 및 조치 사례	

■ 점검방법

Step 1) 보안장비의 로그 설정 메뉴 확인

■ 조치방법

Step 1) 정책에 따른 원격 로그 서버에 저장될 로그 설정 (각 벤더별 설정 방법이 상이 함)



Step 2) 특정 내부 네트워크에서의 syslog 전송만 허용할 경우 ACL을 적용하여 제어할 수 있음

조치 시 영향	일반적인 경우 영향 없음

보안장비

S-24 (중)	4. 로그관리 > 4.7 NTP 서버 연동
취약점 개요	
점검내용	■ 보안장비의 NTP 서버 연동 설정 적용 여부 점검
점검목적	■ 시스템 운영 또는 보안사고 발생으로 인한 로그 분석 과정에서 이벤트 간의 인과 관계 파악에 도움을 주고 로그 자체의 신뢰성을 갖도록 함
보안위협	■ 시스템 간 시간 동기화 미흡으로 보안사고 및 장애 발생 시 로그에 대한 신뢰도 확보 미흡
참고	※ **NTP(Network Time Protocol):** 네트워크를 통해 컴퓨터 시스템 간의 시간을 정확하게 유지 시켜주기 위한 네트워크 프로토콜. NTP는 1985년 RFC958로 제안된 표준으로 현재 RFC5905 NTP version 4로 대체됨 ※ https://tools.ietf.org/html/rfc5905 NTP 관련 정보 참고 사이트
점검대상 및 판단기준	
대상	■ 방화벽, IPS, VPN 등
판단기준	**양호 :** NTP 서버 연동이 되어 있는 경우
	취약 : NTP 서버 연동이 되어 있지 않은 경우
조치방법	보안장비 시간 설정에서 NTP 프로토콜 연동 확인
점검 및 조치 사례	

■ 점검방법

Step 1) 보안장비 설정 메뉴에서 NTP 프로토콜 연동 확인 및 벤더사에 문의

■ 조치방법

Step 1) 보안장비 설정 메뉴에서 NTP 서버 연동 설정

조치 시 영향	일반적인 경우 영향 없음.

보안장비

S-25 (중)	5. 기능관리 > 5.9 부가 기능 설정
취약점 개요	
점검내용	■ 보안장비에서 지원하는 부가기능을 확인하여 필요한 부가 기능을 사용하고 있는지 점검
점검목적	■ 보안장비에서 부가 기능을 제공하는 경우, 이를 활용하여 보안성을 높이기 위함
보안위협	■ 부가기능을 사용하지 않는다고 보안 운영에 큰 영향을 미치지는 않지만, 사용함으로써 도움을 얻을 수 있음
참고	※ **부가기능:** 유해 사이트 차단, anti-spam, anti-virus 등 ※ 보안장비 부가기능을 사용할 시 비용이 발생할 수 있으므로 기관에 예산이나 여건에 따라 사용하지 않을 수 있음
점검대상 및 판단기준	
대상	■ 방화벽 등
판단기준	**양호 :** 보안장비에서 기본적으로 제공하는 부가기능 중 기관에서 필요한 기능을 사용할 경우
	취약 : 보안장비에서 기본적으로 제공하는 부가기능 중 기관에서 필요한 기능을 사용하지 않을 경우
조치방법	보안장비에서 제공하고 있는 부가기능을 확인하여 필요한 기능 사용
점검 및 조치 사례	

■ 점검방법

Step 1) 보안장비에서 제공하는 부가기능 설정 확인

■ 조치방법

Step 1) 벤더사에 문의하여 부가기능 설정 시 발생하는 영향을 고려하여 적용

조치 시 영향	부가기능 적용 시 방화벽 고유 기능에 발생하는 영향을 고려하여 적용

S-26 (중)	5. 기능관리 > 5.10 유해 트래픽 차단 정책 설정
취약점 개요	
점검내용	■ 유해 트래픽 차단 정책을 설정하고 있는지 점검
점검목적	■ 유해 트래픽을 차단하여 네트워크 운영 및 서비스의 장애 발생 가능성을 낮추고자 함
보안위협	■ 유해 트래픽 차단 정책이 설정되지 않을 경우, 악성코드가 네트워크 및 타 PC로 전파되어 DDoS 공격, Worm, Virus 확산 등 네트워크 자원을 악의적인 목적으로 사용할 수 있음
참고	※ **유해 트래픽:** 정상적인 네트워크 운영 및 서비스에 지장을 주는 악의적인 공격성 패킷과 바이러스 패킷으로, 망 운영에 치명적인 장애를 유발하며 동시 다발적이고 급속한 확인이 특징
점검대상 및 판단기준	
대상	■ 방화벽, IPS 등
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
점검 및 조치 사례	

■ 점검방법

Step 1) 침입차단시스템의 유해 트래픽 차단 기능 확인

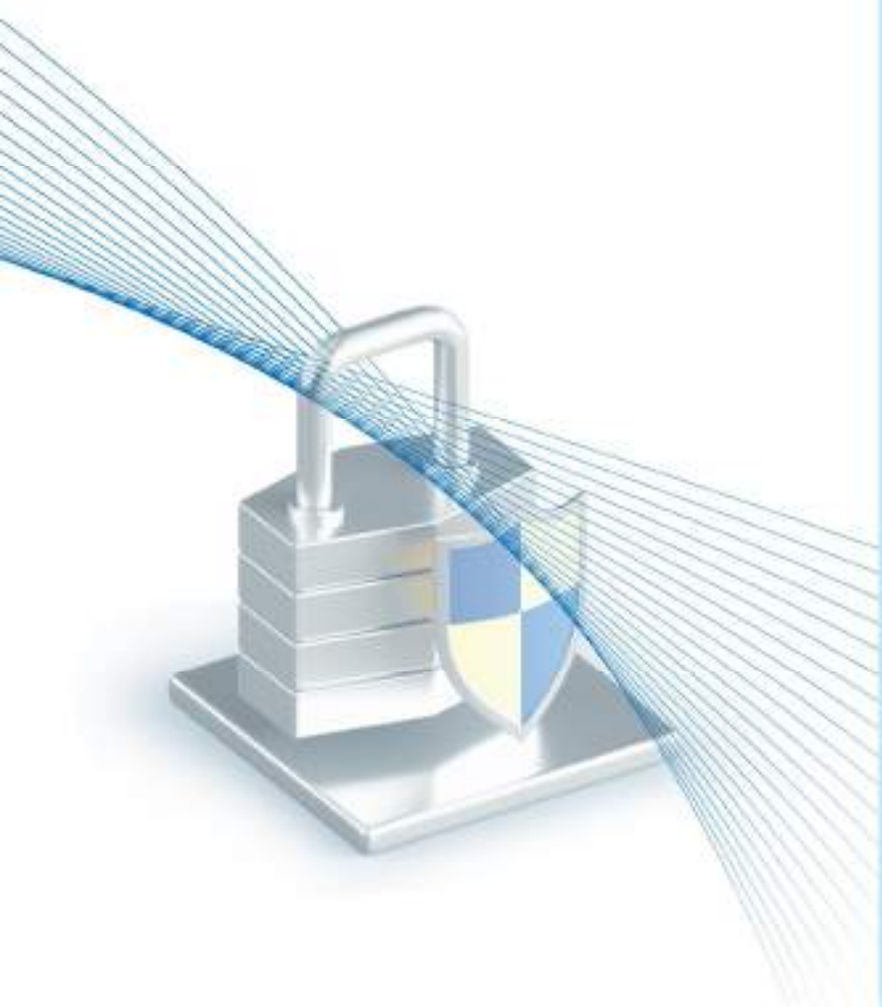
■ 조치방법

Step 1) 침입차단시스템의 유해트래픽 차단 기능 설정

조치 시 영향	오탐으로 인한 정상 트래픽 차단 가능성 있음

Ⅱ

네트워크 장비



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

네트워크장비

N-01 (상)	1. 계정 관리 > 1.1 패스워드 설정
취약점 개요	
점검내용	■ 관리 터미널(콘솔, SSH, https 등)을 통해 네트워크 장비 접근 시 기본 패스워드(기본 관리자 계정도 함께 변경하도록 권고)를 사용하는지 점검
점검목적	■ 기본 패스워드를 변경 후 사용하는지 점검하여 기본 패스워드를 변경하지 않고 사용함으로써 발생할 수 있는 비인가자의 네트워크 장비 접근에 대한 통제가 이루어지는지 확인하기 위함
보안위협	■ 장비 출고 시 설정된 기본 패스워드를 변경하지 않고 그대로 사용할 경우 비인가자가 인터넷을 통해 벤더사 별 네트워크 장비 기본 패스워드를 쉽게 획득할 수 있음 ■ 획득한 패스워드를 사용하여 기본 패스워드를 변경하지 않고 관리 운용 중인 네트워크 장비에 접근하여 장비의 내부 설정(ACL)을 변경함으로써 해당 네트워크 장비를 통해 전송되는 데이터들이 비인가자에게 유출되거나 네트워크 장비를 통해 통신하는 정보시스템(서버, 보안장비, 네트워크장비) 간의 통신에 영향(데이터 전송 불가)을 미칠 수 있음
참고	※ **기본(Default) 패스워드**: 장비 제조업체에서 출고 시 설정되어 나오는 기본 관리자 계정의 패스워드 정보 ※ **기본(Default) 관리자 계정**: 장비 제조업체에서 출고 시 설정되어 나오는 네트워크 장비의 관리용 계정(예 admin, manager 등)
점검대상 및 판단기준	
대상	■ CISCO, Alteon, Passport, Juniper, Piolink 등
판단기준	**양호 :** 기본 패스워드를 변경하여 사용하는 경우
	취약 : 기본 패스워드를 변경(패스워드 미설정 사용 포함)하지 않고 사용하는 경우
조치방법	장비 출고 시 설정되어 있는 기본 패스워드를 기관의 패스워드 설정 규칙에 맞게 변경하여 사용
점검 및 조치 사례	

■ **장비별 점검방법 예시**

- **CISCO**

```
Router# show running-config
```

Enable 패스워드 설정 확인

Line Access에서 각 라인별(VTY, CON, AUX) 패스워드 설정 확인

※ Router(configXline)# login local

: local 계정 패스워드 유무 확인 필요

※ Router(configXline)# no login

: enable 패스워드 유무 확인 필요

네트워크장비

N-01 (상)	1. 계정 관리 > 1.1 패스워드 설정

- **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

■ **장비별 조치방법 예시**

- **CISCO**

  Step 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#
  ```

  Step 2) Virtual Terminal Password 설정
  ```
  Router# config terminal
  Router(config)# line vty ?
  <0X4> First Line number
  Router(config)# line vty 0 4
  Router(configXline)# login
  Router(configXline)# password <패스워드>
  ```

  Step 3) 콘솔 패스워드 설정
  ```
  Router# config terminal
  Router(config)# line console ?
  <0X0> First Line number
  Router(config)# line console 0
  Router(configXline)# login
  Router(configXline)# password <패스워드>
  ```

  Step 4) 보조포트(AUX) 패스워드 설정
  ```
  Router# config terminal
  Router(config)# line aux ?
  ```

N-01 (상)	1. 계정 관리 > 1.1 패스워드 설정

```
<0X0> First Line number
Router(config)# line aux 0
Router(configXline)# login
Router(configXline)# password <패스워드>
```

- **Alteon**

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

- **Passport**

[CLI]

Step 1) switch로 접속

Step 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>
# 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 rootXauthentication plainXtextXpasswd
New password : 패스워드 <- 새로운 패스워드 입력
retype new password: : 패스워드 <- 입력했던 패스워드 확인
```

- **Piolink**

Step 1) Switch로 접속

Step 2) root 계정으로 로그인

Step 3) (configuration)# 에서 password 명령어 사용

Step 4) new password: 입력

Step 5) retype password: 입력

조치 시 영향	일반적인 경우 영향 없음

네트워크장비

N-02 (상)	1. 계정 관리 > 1.2 패스워드 복잡성 설정
취약점 개요	
점검내용	■ 네트워크 장비에 기관 정책에 맞는 계정 패스워드 복잡성 정책이 적용되어 있는지 점검 ■ 패스워드 복잡성 정책 설정 기능이 장비에 존재하지 않을 경우 기관 정책에 맞게 계정 패스워드를 설정하여 사용하는지 점검
점검목적	■ 패스워드 복잡성 정책이 장비 정책에 적용되어 있는지 점검하여 비인가자의 네트워크 장비 터미널(콘솔, SSH, https 등) 접근 시도 공격(무작위 대입 공격, 사전 대입 공격 등)에 대한 대비 여부를 확인하기 위함
보안위협	■ 패스워드 복잡성 정책이 적용되어 있지 않을 경우 계정 생성 후 초기 패스워드 설정 및 기존 패스워드 변경 시 패스워드 복잡성 제약 규칙을 적용받지 않아 취약한 패스워드(예 qwerty, 12345, pass1234 등)를 설정할 수 있도록 허용함 ■ 해당 취약점으로 인해 비인가자의 공격(무작위 대입 공격, 사전 대입 공격 등)에 계정 패스워드가 유출되는 원인을 제공하여 유출된 패스워드를 사용하여 비인가자가 네트워크 장비 터미널에 접근할 수 있는 위험이 존재함
참고	※ **패스워드 복잡성:** 계정 패스워드 설정 시 영문(대문자, 소문자), 숫자, 특수문자가 혼합된 패스워드로 설정하는 것 ※ **무작위 대입 공격(Brute Force Attack):** 컴퓨터로 암호를 해독하기 위해 가능한 모든 키를 하나하나 추론해 보는 시도를 말함. ※ **사전 대입 공격(Dictionary Attack):** 사전에 있는 단어를 입력하여 패스워드를 알아내거나 암호를 해독하는 데 사용되는 컴퓨터 공격 방법 ※ 관련 점검 항목 : A-28(상), A-66(중)
점검대상 및 판단기준	
대상	■ 공통
판단기준	**양호 :** 기관 정책에 맞는 패스워드 복잡성 정책이 네트워크 장비에 적용되어 있거나, 패스워드 복잡성 기능이 장비에 존재하지 않을 경우 기관 정책에 맞게 패스워드를 설정하여 사용하는 경우
	취약 : 기관 정책에 맞지 않는 패스워드를 설정하여 사용하는 경우
조치방법	해당 기관의 보안 정책에 맞게 패스워드 복잡성 설정

네트워크장비

N-02 (상)	1. 계정 관리 > 1.2 패스워드 복잡성 설정

점검 및 조치 사례

■ **장비별 점검방법 예시**

- **공통**

  Step 1) 장비에 패스워드 복잡성 설정이 적용되어 있는지 점검

  Step 2) 패스워드 복잡성 설정이 존재하지 않을 경우 기관 내 정책에 따라 패스워드를 설정하여 사용하는지 확인

■ **장비별 조치방법 예시**

- **공통**

  Step 1) 패스워드 설정 시 아래와 같은 패스워드 정책을 적용해야 함

  1. 암호는 최소 8 자 이상이어야 함 (Passport 9 자 이상)
  2. 사용자 계정 이름이나 이름의 문자를 3 개 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

1. 최소 10자리 이상: 영대문자, 영소문자, 숫자 및 특수문자 중 2종류 이상으로 구성한 경우
2. 최소 8자리 이상: 영대문자, 영소문자, 숫자 및 특수문자 중 3종류 이상으로 구성한 경우

조치 시 영향	일반적인 경우 영향 없음

네트워크장비

N-03 (상)	1. 계정 관리 > 1.3 암호화 된 패스워드 사용
취약점 개요	
점검내용	■ 계정 패스워드 암호화 설정이 적용되어 있는지 점검
점검목적	■ 계정 패스워드 암호화 설정 유무를 점검하여 비인가자의 네트워크 장비 터미널 접근으로 인해 발생할 수 있는 장비 내 계정 패스워드 유출에 대비가 되어 있는지 확인하기 위함
보안위협	■ 계정 패스워드 암호화 기능이 설정되어 있지 않을 경우, 비인가자가 네트워크 터미널에 접근하여 장비 내에 존재하는 모든 계정의 패스워드를 획득할 수 있는 위험이 존재함
참고	-
점검대상 및 판단기준	
대상	■ CISCO, Passport, Juniper 등
판단기준	**양호 :** 패스워드 암호화 설정이 적용된 경우
	취약 : 패스워드 암호화 설정이 적용되어 있지 않은 경우
조치방법	패스워드 암호화 설정 적용
점검 및 조치 사례	

■ **장비별 점검방법 예시**

- **CISCO**

```
Router# show running-config
```

1. Enable Secret 사용 확인
2. Password-Encryption 서비스 동작 확인

- **Passport**

Configuration file에서 Enable Secret 패스워드를 제외한 모든 패스워드 암호화 설정 확인

- **Juniper**

```
user@juniper>configure
[edit]
user@juniper#show
```

root authentication 설정을 이용하여 [edit system] 레벨에서 패스워드 암호화 설정

N-03 (상)	1. 계정 관리 > 1.3 암호화 된 패스워드 사용

■ 장비별 조치방법 예시

- **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
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
```

조치 시 영향	일반적인 경우 영향 없음

네트워크장비

N-04 (상)	2. 접근 관리 > 2.1 VTY 접근(ACL) 설정
취약점 개요	
점검내용	■ 원격 터미널(VTY) 통해 네트워크 장비 접근 시 지정된 IP에서만 접근이 가능 하도록 설정되어 있는지 점검
점검목적	■ 지정된 IP 만 네트워크 장비에 접근하도록 설정되어 있는지 점검하여 비인가자의 터미널 접근을 원천적으로 차단하는지 확인하기 위함
보안위협	■ 지정된 IP 만 네트워크 장비에 접근하도록 설정되어 있지 않을 경우, 비인가자가 터미널 접근 시도 공격(무작위 대입 공격, 사전 대입 공격 등)을 시도 하여 관리자 계정 패스워드 획득 후 네트워크 장비에 접근하여 장비 설정(기능, ACL정책) 변경 및 삭제 등의 행위를 통해 네트워크 장비를 경유하는 데이터의 유출 및 가용성 저하 등을 발생 시킬 수 있는 위험이 존재함
참고	※ **VTY(Virtual Type Terminal):** 가상 유형 터미널의 약어. 가상 터미널 라인(virtual terminal line)이라는 용어가 더 흔하게 사용되며 네트워크 장비를 원격 프로토콜(ssh)에서 관리하기 위한 터미널 서비스 ※ 기반시설 시스템은 VTY을 통한 접근을 원칙적으로 금지하나, 부득이 VTY을 사용하여 접근을 해야 하는 경우 허용한 시스템만 접근할 수 있게 하여 사용해야 함
점검대상 및 판단기준	
대상	■ CISCO, Alteon, Passport, Juniper 등
판단기준	**양호 :** 원격 터미널(VTY) 접근 시 지정된 IP 만 접근 하도록 설정이 되어있는 경우
	취약 : 원격 터미널(VTY) 접근 시 지정된 IP 만 접근하도록 설정이 되어있지 않는 경우
조치방법	VTY(SSH) 사용 시 지정된 IP만 접근 하도록 설정
점검 및 조치 사례	

■ **장비별 점검방법 예시**

- **CISCO**

```
Router# show running-config
```

1. Access-List 설정 확인
2. 각 Line Vty에 access-class 설정 확인

- **Alteon, Passport**

장비로 접속하여 Telnet 또는 SSH 사용자의 접속 IP 설정 확인(Access Policies)

- **Juniper**

```
user@juniper# configure
[edit]
```

N-04 (상)	2. 접근 관리 > 2.1 VTY 접근(ACL) 설정

```
user@juniper# show
```
root authentication 설정을 이용하여 [edit system] 레벨에서 ACL 설정 확인

■ **장비별 조치방법 예시**

- **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 mode로 접속
(config)# access-list <access_list_num> permit <source_ip mask>
(config)#ssh access-group <num>
(config)#write memory
```
또는,
Global configuration mode로 접속
```
(config)# ip ssh client <IP_address>
```
또는,
Global configuration mode로 접속
```
(config)# ip ssh client <IP_address><mac_address>
```

- **Alteon**

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

네트워크장비

N-04 (상)	2. 접근 관리 > 2.1 VTY 접근(ACL) 설정

- **Passport**

  Step 1) switch로 접속

  Step 2) `# config sys access-policy`

  Step 3) `config/sys/access-policy# enable true`

  Step 4) `config/sys/access-policy# policy <pid> create`

  Step 5) `config/sys/access-policy# policy <pid>`

  Step 6) `config/sys/access-policy/policy/<pid># enable true`

  Step 7) `config/sys/access-policy/policy/<pid># accesslevel rwa`

  Step 8) `config/sys/access-policy/policy/<pid># host <ip-addr>`

  Step 9) `config/sys/access-policy/policy/<pid># service snmp enable`

  Step 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

N-05 (상)	2. 접근 관리 > 2.2 Session Timeout 설정
취약점 개요	
점검내용	■ 기관 정책에 맞게 Session Timeout 설정이 적용되어 있는지 점검
점검목적	■ Session Timeout 설정 유무를 점검하여 터미널 접속 후 일정 시간(Session Timeout 지정 시간)이 지난 뒤 터미널 세션이 자동으로 종료되어 관리자의 부재(터미널 작업 중 자리 비움, 작업 완료 후 터미널 접속을 종료하지 않음) 시 발생 가능한 비인가자의 터미널 접근 통제가 되는지 확인하기 위함
보안위협	■ Session Timeout 정책이 적용되지 않았을 경우, 관리자 부재 시 비인가자가 네트워크 장비 터미널에 접속된 컴퓨터를 통해 네트워크 장비의 정책 변경 및 삭제 등의 행위를 할 수 있는 위험이 존재함
참고	※ **Session Timeout:** 터미널 접속 후 유휴 상태 일 때 자동으로 터미널 접속을 종료하는 시간 설정
점검대상 및 판단기준	
대상	■ CISCO, Alteon, Juniper, Piolink 등
판단기준	**양호 :** Session Timeout 시간을 기관 정책에 맞게 설정한 경우
	취약 : Session Timeout 시간을 기관 정책에 맞게 설정하지 않은 경우
조치방법	Session Timeout 설정 (5분 이하 권고)
점검 및 조치 사례	

■ **장비별 점검방법 예시**

- **CISCO**

```
Router# show running-config
```

각 Line Access의 exec-timeout 설정 확인

- **Alteon**

idle timeout in minutes 설정 확인

- **Juniper**

```
user@juniper>configure
[edit]
user@juniper#show
```

root authentication설정을 이용하여 [edit system] 레벨에서 Session Timeout 설정확인

- **Piolink**

terminal timeout 설정 확인

네트워크장비

N-05 (상)	2. 접근 관리 > 2.2 Session Timeout 설정

■ 장비별 조치방법 예시

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

- **Alteon**

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

- **Juniper**

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

- **Piolink**

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

조치 시 영향	일반적인 경우 영향 없음

N-06 (상)	3. 패치 관리 > 3.1 최신 보안 패치 및 벤더 권고사항 적용
취약점 개요	
점검내용	■ 패치 적용 정책에 따라 주기적인 패치를 하고 있는지 점검
점검목적	■ 네트워크 장비의 보안 수준을 높이고 성능 및 기능 향상을 위해서 버전 업그레이드 및 보안 패치 작업을 수행해야 함
보안위협	■ 알려진 네트워크 장비의 버그나 취약점을 통하여 관리자 권한 획득이나 서비스 거부 공격 등을 발생시킬 수 있음
참고	▪ CISCO 버전별 정보 및 취약점 정보 http://www.cisco.com/web/about/security/intelligence/ios-ref.html (버전별 정보) http://tools.cisco.com/security/center/navigation.x?i=118 (취약점 정보) ▪ Juniper 버전별 정보 http://www.juniper.net/us/en/products-services/routing/ ▪ Alteon은 Radware로 벤더가 변경됨
점검대상 및 판단기준	
대상	■ 공통
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
점검 및 조치 사례	

■ **장비별 점검방법 예시**

- **CISCO**

```
Router# show version
```

버전정보 확인

- **Juniper**

```
user@juniper> configure
[edit]
user@juniper# show version
```

root authentication 설정을 이용하여 [edit system] 레벨에서 패치 정보 확인

네트워크장비

N-06 (상)	3. 패치 관리 > 3.1 최신 보안 패치 및 벤더 권고사항 적용
■ **장비별 조치방법 예시** • **공통** 1. 네트워크 장비는 지속해서 취약점이 발견되고 있으며, 이에 대한 패치도 계속 제공되고 있음 2. 테스트와 수정을 통하여 검증 받은 패치를 사용하여야 하며, 이외 버전은 꼭 필요한 기능이 있는 경우만 사용함 3. 최신 패치를 적용 하지 않을 경우 IP Option, TCP, IPv6, Header 패킷을 발송할 경우 서비스 거부 등의 피해가 발생할 수 있음	
조치 시 영향	서비스 영향을 고려하여 벤더사와 협의 후 적용

N-07 (상)	5. 기능 관리 > 5.1 SNMP 서비스 확인
취약점 개요	
점검내용	■ 네트워크 장비에 사용하지 않는 SNMP 서비스가 구동되고 있거나 SNMP 서비스 사용 시 암호화가 지원되는 버전을 사용하고 있는지 점검
점검목적	■ 불필요한 SNMP 서비스 차단 및 보안에 취약한 SNMP 버전의 사용을 방지함으로써 SNMP 서비스의 취약점(조작된 MIB 정보를 통한 네트워크 설정 변경, 전송 데이터 평문전송 등)을 이용한 공격을 차단하기 위함
보안위협	■ SNMP v3 아래 버전을 사용할 경우, 요청 및 응답 패킷이 평문으로 전송되어 공격자가 스니핑을 할 경우 Community String을 획득할 수 있으며 획득한 Community String을 이용하여 환경 설정 파일 열람 및 수정이나 정보 수집 및 관리자 권한 획득, DoS 등 다양한 형태의 공격이 가능해 짐
참고	※ **SNMP(Simple Network Management Protocol):** TCP/IP 기반 네트워크상의 각 호스트에서 정기적으로 여러 정보를 자동으로 수집하여 네트워크 관리를 하기 위한 프로토콜을 의미하며 v1, v2, v3 세 가지 버전이 존재하는데 v2까지도 요청, 응답 패킷이 평문으로 전송되기 때문에 스니핑이 가능하지만 v3 이상부터는 HMAC-MD5 또는 HMAC-SHA 알고리즘 기반의 인증을 제공함 1 ※ **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):** 시스템을 악의적으로 공격해 해당 시스템의 자원을 부족하게 하여 원래 의도된 용도로 사용하지 못하게 하는 공격을 말하며 특정 서버에게 수많은 접속 시도를 만들어 다른 이용자가 정상적으로 서비스 이용을 하지 못하게 하거나, 서버의 TCP 연결을 바닥내는 등의 공격이 이 범위에 포함됨
점검대상 및 판단기준	
대상	■ CISCO, Alteon, Passport, Juniper 등
판단기준	**양호 :** SNMP v3이상 버전을 사용하거나 서비스를 사용하지 않는 경우
	취약 : SNMP v2이하 버전을 사용하거나 불필요하게 서비스를 활성화한 경우
조치방법	SNMP 서비스가 불필요할 경우 중지

네트워크장비

N-07 (상)	5. 기능 관리 > 5.1 SNMP 서비스 확인

점검 및 조치 사례

■ **장비별 점검방법 예시**

- **CISCO**

```
Router# show running-config
Router# show snmp
```

1. SNMP 설정 확인
2. SNMP 서비스 동작 확인

※ SNMP 서비스 비활성화 시 아래 문구 출력

```
!
%SNMP agent not enabled
!
```

- **Juniper**

```
user@juniper> configure
[edit]
user@juniper# show snmp
```

root authentication 설정을 이용하여 [edit system] 레벨에서 snmp 서비스 설정 확인

■ **장비별 조치방법 예시**

- **CISCO**

```
Router# config terminal
Router(config)# no snmp-server
Router(config)# ^Z
```

- **Alteon / Passport**

SNMP 서비스가 불필요하다면 서비스 중지

- **Juniper**

```
user@juniper> configure
user@juniper# no set snmp community public
```

조치 시 영향	SNMP 서비스에 영향을 줄 수 있음

네트워크장비

N-08 (상)	5. 기능 관리 > 5.2 SNMP community string 복잡성 설정
취약점 개요	
점검내용	■ SNMP 서비스 사용 시 Community String을 기본 설정(public, private)으로 사용하고 있는지 점검
점검목적	■ SNMP Community String을 공격자가 쉽게 유추하지 못하도록 설정하여 Community String 탈취에 대한 위험을 줄이기 위함
보안위협	■ SNMP Community String을 기본 설정(public, private) 또는 유추하기 쉽게 설정하여 사용하는 경우, 공격자가 자동화된 방법을 통하여 community string을 탈취하여 서비스거부공격(DoS), 비인가 접속, MIB 값 수정 등 다양한 공격을 할 수 있음
참고	※ Community String은 영숫자, 문자, 하이픈, 밑줄 및 마침표를 사용할 수 있지만, 기타 모든 특수 문자를 사용할 수 없음
점검대상 및 판단기준	
대상	■ CISCO, Alteon, Passport, Juniper 등
판단기준	**양호 :** SNMP 서비스를 사용하지 않거나, 유추하기 어려운(영문자, 숫자 포함 10자) Community String을 설정한 경우
	취약 : 디폴트 Community String을 변경하지 않거나, 유추하기 쉬운 Community String으로 설정한 경우
조치방법	Public, Private 외 유추하기 어려운 Community String을 설정
점검 및 조치 사례	

■ **장비별 점검방법 예시**

- **CISCO**

```
Router# show running-config
```

SNMP 설정 확인

- **Alteon / Passport**

#snmp 설정에서 Community String 설정 확인

- **Juniper**

```
user@juniper> configure
[edit]
user@juniper# show
```

root authentication 설정을 이용하여 [edit system] 레벨에서 community string 확인

네트워크장비

N-08 (상)	5. 기능 관리 > 5.2 SNMP community string 복잡성 설정

■ **장비별 조치방법 예시**

- **CISCO**

  Step 1) Community String 문자열 변경

  ```
  Router# config terminal
  Router(config)# snmp-server Community <커뮤니티명>
  ```

- **Alteon**

  네트워크 장비는 SNMP 취약성이 존재하므로 누구나 추측하기 어렵고 의미가 없는 문자열, 영문자 혼합으로 변경 권고함.

  Step 1) switch로 접속

  Step 2) `# cfg/sys/ssnmp`

  Step 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)

  Step 4) `# apply`

  Step 5) `# save`

- **Passport**

  Step 1) switch로 접속

  Step 2) `# config snmp-v3 community commname <Comm Idx> new-commname <value>`

조치 시 영향	일반적인 경우 영향 없음

N-09 (상)	5. 기능 관리 > 5.3 SNMP ACL 설정
취약점 개요	
점검내용	■ SNMP 서비스 사용 시 네트워크 장비 ACL(Access list)을 설정하여 SNMP 접속 대상 호스트를 지정하여 접근이 가능한 IP를 제한하였는지 점검
점검목적	■ SNMP ACL 설정을 함으로써 임의의 호스트에서 SNMP 접근을 차단하여 네트워크 정보의 노출을 제한하기 위함
보안위협	■ 비인가자의 SNMP 접근을 차단하지 않을 경우, 공격자가 Community String 추측 공격 후 MIB 정보를 수정하여 라우팅 정보를 변경하거나 터널링 설정을 하여 내부망에 침투할 수 있는 위험이 존재함
참고	-
점검대상 및 판단기준	
대상	■ CISCO, Alteon, Passport, Juniper 등
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 ACL(Access list) 설정
점검 및 조치 사례	

■ **장비별 점검방법 예시**

- **CISCO**

```
Router# show running-config
```

1. SNMP 설정 확인
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

■ **장비별 조치방법 예시**

- **CISCO**

Step 1) access-list를 이용하여 특정 호스트만 열어 주기(port:161,162)

Step 2) `Router# config terminal`

네트워크장비

N-09 (상)	5. 기능 관리 > 5.3 SNMP ACL 설정

Step 3) `Router(config)# access-list 100 permit ip host 100.100.100.100 any`
Step 4) `Router(config)# access-list 100 deny udp any any eq snmp`
Step 5) `Router(config)# access-list 100 deny udp any any eq snmptrap`
Step 6) `Router(config)# access-list 100 permit ip any any`
Step 7) `Router(config)# interface serial 0` (해당 인터페이스에 설정)
Step 8) `Router(config-if)# ip access-group 100 in`
Step 9) 시스코 스위치 장비인 경우 vlan 에 설정

```
Router(config)# interface vlan1
Router(config-if)# ip access-group 100 in
```

- **Passport**

Step 1) switch로 접속
Step 2) `# config snmp-v3 community create <Comm Idx> <name> <security> [tag <value>]`
Step 3) `# config snmp-v3 group-member create <user name> <model> [<group name>]`
Step 4) `# config snmp-v3 group-access create <group name> <prefix> <model> <level>`
Step 5) `# config snmp-v3 group-access view <group name> <prefix> <model> <leve> [read <value>][write <value>] [notify <value>]`

- **Juniper**

Step 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 ];
}
```

Step 2) `203.235.xxx.xxx`에서만 해당 네트워크 장비로 접속가능

```
[edit snmp community]
clients {
default restrict;
203.235.xxx.xxx <restrict>;
```

- **Piolink**

Step 1) 관리자 모드로 접속
Step 2) `configuration`
Step 3) `snmp <agent-address> <ip-addr> <port>`

조치 시 영향	일반적인 경우 영향 없음

N-10 (상)	5. 기능 관리 > 5.4 SNMP 커뮤니티 권한 설정
취약점 개요	
점검내용	■ SNMP 서비스 사용 시 Community String 권한이 불필요하게 RW로 설정 되어 있는지를 점검
점검목적	■ 불필요한 SNMP Community String의 RW 권한을 제거함으로써 공격자의 SNMP를 통한 라우터 정보 수정을 막기 위함
보안위협	■ SNMP Community String 권한이 불필요하게 RW로 설정되어 있으면, 공격자가 Community String 추측 공격을 통해 Community String을 탈취했을 시 SNMP를 이용하여 네트워크 설정 정보를 변경하여 내부망 침투가 가능해 짐
참고	※ SNMP Community String 권한에는 RO(Read Only)와 RW(Read Write) 모드가 있으며 RO 모드의 경우 네트워크 설정 값에 대한 열람만 가능하고 RW 모드는 열람 및 수정을 할 수 있음
점검대상 및 판단기준	
대상	■ CISCO, Alteon, Passport, Juniper 등
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)
점검 및 조치 사례	

■ **장비별 점검방법 예시**

- **CISCO**

  Router# `show running-config`

  SNMP 설정 확인

- **Passport**

  config snmp 에서 SNMP community 권한 확인

- **Juniper**

  ```
  user@juniper> configure
  [edit]
  user@juniper# show
  ```

  root authentication 설정을 이용하여 [edit system] 레벨에서 SNMP community 권한 확인

네트워크장비

N-10 (상)	5. 기능 관리 > 5.4 SNMP 커뮤니티 권한 설정

■ **장비별 조치방법 예시**

- **CISCO**

Step 1) 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**

Step 1) SNMP Community String 권한 설정 방법 (RW 권한 삭제 권고)

1. switch로 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

N-11 (상)	5. 기능 관리 > 5.5 TFTP 서비스 차단
취약점 개요	
점검내용	■ 네트워크 장비 서비스 중 불필요한 TFTP 서비스가 구동되어 있거나 TFTP 서비스 사용 시 ACL을 적용하여 허용된 시스템에서만 TFTP 서비스를 사용하도록 설정되어 있는지 점검
점검목적	■ 인증 기능이 없는 TFTP 단점을 보완하기 위해 사용이 허용된 시스템만 TFTP 서비스를 사용하게 하여 TFTP를 이용한 비인가자의 내부 정보 유출을 막고 중요정보(예: 장비 설정파일) 등의 정보 유출을 막기 위함.
보안위협	■ TFTP 서비스는 인증절차 없이 누구나 사용이 가능한 서비스로 공격자가 TFTP를 통해 악성 코드가 삽입된 파일을 올려 사용자에게 배포할 수 있고, 네트워크 설정 파일이나 중요한 내부 정보를 유출할 수 있음
참고	※ **TFTP(Trivial File Transfer Protocol):** 임의의 시스템이 원격 시스템으로부터 부팅(Booting)코드를 다운로드하는데 사용하는 프로토콜로 UDP 기반으로 포트는 69번을 사용함. FTP와 같은 기능을 하지만 FTP보다 구현하기 쉽고 사용하기 편하지만, 인증절차 없이 사용할 수 있어 보안에 취약하고 데이터 전송 과정에서 데이터가 손실될 수 있는 등 불안정한 단점이 있음
점검대상 및 판단기준	
대상	■ CISCO, Alteon, Juniper 등
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
점검 및 조치 사례	

■ **장비별 점검방법 예시**

- **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

네트워크장비

N-11 (상)	5. 기능 관리 > 5.5 TFTP 서비스 차단

■ **장비별 조치방법 예시**

- **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

N-12 (상)	5. 기능 관리 > 5.6 Spoofing 방지 필터링 적용
취약점 개요	
점검내용	■ 네트워크 장비에 ACL 적용 시 일반적으로 사용하지 않는 broadcast, multicast, loopback 주소로 오는 패킷에 대한 필터 정책을 적용하였는지 점검
점검목적	■ 일반적으로 사용될 필요가 없는 Source IP로 설정된 패킷에 대한 ACL을 적용시켜 패킷을 필터 함으로써 사용되지 않는 주소로 속여 공격하는 변조된 불법 패킷을 차단하기 위함
보안위협	■ 일반적으로 사용되지 않는 Source IP에 대한 ACL 적용을 하지 않은 경우, 공격자가 악의적인 목적으로 패킷을 조작하여 DoS 공격을 시도 할 수 있음
참고	※ IP Spoofing은 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
점검대상 및 판단기준	
대상	■ CISCO, Alteon, Juniper 등
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
점검 및 조치 사례	

■ **장비별 점검방법 예시**

- **CISCO**

```
Router# show running
```

IP spoofing 방지 설정 확인

- **Alteon**

/slb/filt에서 IP spoofing 방지를 위한 ACL 설정 확인

N-12 (상)	5. 기능 관리 > 5.6 Spoofing 방지 필터링 적용

- **Juniper**

  Configure Firewall Filters와 Apply Firewall Filters 설정 확인

■ **장비별 조치방법 예시**

- **CISCO**

  Step 1) Global configuration mode 로 접속

  Step 2) `access-list number deny ip 127.0.0.0 0.255.255.255 any`

  Step 3) `access-list number deny ip 224.0.0.0 31.255.255.255 any`

  Step 4) `access-list number deny ip host 0.0.0.0 any`

  Step 5) `access-list number permit ip any any`

- **Alteon**

  Step 1) switch로 접속함.

  Step 2) `# cfg`

  Step 3) `# /slb/filt <filter number>`

  Step 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;
                }
            }
        }
    }
```

N-12 (상)	5. 기능 관리 > 5.6 Spoofing 방지 필터링 적용

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;
                               }
                         }
           }
   }
```

조치 시 영향	필터링 적용 시 사용하는 ACL은 라우터 성능에 많은 영향을 미침

네트워크장비

N-13 (상)	5. 기능 관리 > 5.7 DDoS 공격 방어 설정
취약점 개요	
점검내용	■ DDoS 공격에 사용되는 IP 대역을 ACL 적용하여 차단하였는지 점검
점검목적	■ 외부에서 사용할 수 없거나 특수한 목적으로만 사용하는 IP 대역을 차단하여 DDoS 공격의 피해를 감소시키기 위함
보안위협	■ 외부망에서 사용하지 않는 IP 또는 특수한 목적으로만 사용하는 IP 대역을 차단하지 않을 경우, 공격자가 해당 IP들을 이용하여 DDoS 공격을 시도하면 공격 발생지를 파악할 수 없어 DDoS 방어가 어려워지고 피해 시간이 길어짐
참고	※ **DDoS(Distributed Denial of Service)**: 해커에 의해 감염된 다수의 좀비 PC로부터 다량의 트래픽이 특정 서버로 유입되어 시스템, 네트워크에 가용성을 저해시켜 서비스를 방해하는 공격
점검대상 및 판단기준	
대상	■ CISCO, Juniper 등
판단기준	**양호 :** DDoS 공격 방어 설정이 되어있는 경우
	취약 : DDoS 공격 방어 설정이 되어있지 않은 경우
조치방법	DDoS 공격 방어 설정 점검
점검 및 조치 사례	

■ **장비별 점검방법 예시**

- **CISCO**

```
Router> enable
Router# show running (하단 부분에서 확인 가능)
```

- **Juniper**

```
user@juniper> configure
[edit]
user@juniper# show configuration
```

root authentication 설정을 이용하여 [edit system] 레벨에서 DDoS 방어 설정 요소 확인

■ **장비별 조치방법 예시**

- **CISCO, Juniper**

<DDoS 공격 방어 설정 요소>

1. Fragment 공격 차단 설정
2. 적절한 ACL을 통한 사전방어 설정 필요
3. 보안담당자와 네트워크담당자가 연계하여 차단 설정

네트워크장비

N-13 (상)	5. 기능 관리 > 5.7 DDoS 공격 방어 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 : DHCP를 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

N-14 (상)	5. 기능 관리 > 5.8 사용하지 않는 인터페이스의 Shutdown 설정
취약점 개요	
점검내용	■ 사용하지 않는 불필요한 인터페이스가 Shutdown 되지 않고 활성화되고 있는지를 점검
점검목적	■ 필요한 인터페이스만 활성화하여 비인가자가 사용하지 않는 인터페이스를 통하여 네트워크에 접근하는 것을 차단하기 위함
보안위협	■ 사용하지 않는 포트에 연결된 인터페이스를 Shutdown 하지 않을 경우, 물리적인 내부 접근을 통해 비인가자의 불법적인 네트워크 접근이 가능하게 되며 이로 인하여 네트워크 정보 유출 및 네트워크 손상이 발생할 수 있음
참고	-
점검대상 및 판단기준	
대상	■ CISCO, Alteon, Juniper 등
판단기준	**양호 :** 사용하지 않는 인터페이스가 차단된 경우
	취약 : 사용하지 않는 인터페이스가 차단되지 않은 경우
조치방법	사용하지 않는 인터페이스 차단
점검 및 조치 사례	

■ 장비별 점검방법 예시

- **CISCO**

```
Router# show running-config
Router# show interface status
Router# show ip interface brief
```

1. 각 Interface 설정 확인
2. Interface 상태 확인
   (해당포트가 down/up 이 되어 있는지 확인할 수 있음)

- **Juniper**

```
user@juniper> configure
user@juniper# show ip
```

불필요한 포트 차단 확인

■ 장비별 조치방법 예시

- **CISCO**

```
Router# config terminal
Router(config)# interface fastethernet 0/1
Router(config-line)# shutdown
```

사용할 포트는 no shutdown 으로 포트 상태를 up 시켜줌

N-14 (상)	5. 기능 관리 > 5.8 사용하지 않는 인터페이스의 Shutdown 설정

- **Alteon**

  사용하지 않은 인터페이스 차단

```
# config terminal
# interface fastethernet 0/1
# shutdown
```

  사용할 포트는 no shutdown으로 포트 상태를 up 시켜줌

- **Juniper**

  기본적인 인터페이스 비활성

  [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

N-15 (중)	1. 계정 관리 > 1.4 사용자·명령어별 권한 수준 설정
취약점 개요	
점검내용	■ 네트워크 장비 사용자의 업무에 따라 계정 별로 장비 관리 권한을 차등(관리자 권한은 최소한의 계정만 허용) 부여하고 있는지 점검
점검목적	■ 업무에 따라 계정 별 권한이 차등 부여되어 있는지 점검하여 계정 별 권한에 따라 장비의 사용 및 설정 가능한 기능을 제한하는지 확인하기 위함
보안위협	■ 계정 별 권한이 차등 부여되어 있지 않은 경우, 일반 계정으로 장비의 모든 기능을 제어할 수 있어 일반 계정이 비인가자에 노출되었을 때 비인가자가 획득한 계정 정보를 통해 네트워크 장비에 접근하여 장비의 설정(ACL) 변경, 삭제 등의 행위를 하여 장비의 가용성(해당 장비를 통해 통신하는 정보시스템 간 데이터 전송 불가)저하 문제가 발생할 위험이 존재함
참고	※ **관리자 계정**: 장비의 모든 기능(계정 생성 및 권한 부여, 장비 정책 설정, 모든 명령어 사용 가능 등)을 제한 없이 사용하거나 설정할 수 있는 계정 ※ **일반 계정**: 장비의 일부 기능(모니터링, 룰셋적용, 일부 명령어만 사용 등) 만 사용하거나 설정할 수 있는 계정
점검대상 및 판단기준	
대상	■ CISCO, Alteon, Juniper, Piolink 등
판단기준	**양호 :** 업무에 맞게 계정의 권한이 차등 부여 되어있을 경우
	취약 : 업무에 맞게 계정의 권한이 차등 부여 되어있지 않을 경우
조치방법	업무에 맞게 계정 별 권한 차등(관리자 권한 최소화) 부여 ※ 한명의 관리자가 네트워크 장비를 관리할 경우는 해당하지 않음
점검 및 조치 사례	

■ **장비별 점검방법 예시**

- **CISCO**

```
Router# show privilege
```

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

N-15 (중)	1. 계정 관리 > 1.4 사용자·명령어별 권한 수준 설정

- **Piolink**

  슈퍼유저(root)와 일반유저로 권한을 부여하여 관리하는지 확인

■ **장비별 조치방법 예시**

- **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

  Step 1) 사용자별 권한 수준 지정

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

  Step 2) 명령어별 권한 수준 지정

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

  ※ 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 그러나 스위치의 어떤 설정도 바꿀 수 없음
SLB Operator / slboper	SLB Operator는 Web 서버들과 다른 인터넷 서비스의 로드를 관리함 부가적으로 모든 스위치 정보와 통계를 볼 수 있으며, Server Load Balancing 운영 메뉴를 사용하는 서버의 사용 가능/사용 불가능을 설정할 수 있음

네트워크장비

N-15 (중)	1. 계정 관리 > 1.4 사용자·명령어별 권한 수준 설정

Layer4 Operator / l4oper	Layer4 Operator는 공유된 인터넷 서비스들에 따른 라인의 트래픽을 관리함 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 부가적으로 SLB Operator 기능과 포트나 전반적인 스위치를 재설정 할 수 있음
SLB Administrator / slbadmin	SLB Administrator는 웹서버들과 다른 인터넷 서비스들과 그것에 대한 로드를 설정 및 관리 할 수 있음 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 관리 함 부가적으로 SLB Administrator 기능들, 설정 필터들이나 대역폭 관리 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 스위치의 모든 메뉴, 정보 그리고 설정 명령어들에 사용할 수 있음

Step 1) switch로 접속
Step 2) `# cfg`
Step 3) `# sys`
Step 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
Step 5) 암호 및 설정 변경
Step 6) `# apply`
Step 7) `# save`

N-15 (중)	1. 계정 관리 > 1.4 사용자·명령어별 권한 수준 설정

- **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

Step 1) `[edit system login] hierarchy level:`

Step 2)
```
[edit system]
        login {10
        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

N-16 (중)	2. 접근 관리 > 2.3 VTY 접속 시 안전한 프로토콜 사용
취약점 개요	
점검내용	■ 네트워크 장비 정책에 암호화 프로토콜(ssh)을 이용한 터미널 접근만 허용하도록 설정되어 있는지 점검
점검목적	■ 암호화 프로토콜을 이용한 터미널 접근만 허용하도록 설정되어 있는지 점검하여 네트워크 터미널 접근 시 전송되는 데이터의 스니핑 공격에 대한 대비가 되어 있는지 확인하기 위함
보안위협	■ 암호화 프로토콜이 아닌 평문 프로토콜(telnet)을 이용하여 네트워크 장비에 접근할 경우, 네트워크 스니핑 공격에 의해 관리자 계정 정보(계정, 패스워드)가 비인가자에게 유출될 위험이 존재함
참고	※ **스니핑(Sniffing) 공격**: 스니퍼(Sniffer)는 "컴퓨터 네트워크상에 흘러 다니는 트래픽을 엿듣는 도청장치"라고 말할 수 있으며 "스니핑"이란 이러한 스니퍼를 이용하여 네트워크상의 데이터를 도청하는 행위를 말함
점검대상 및 판단기준	
대상	■ CISCO, Alteon, Juniper 등
판단기준	**양호 :** 장비 정책에 VTY 접근 시 암호화 프로토콜(ssh) 이용한 접근만 허용하고 있는 경우
	취약 : 장비 정책에 VTY 접근 시 평문 프로토콜(telnet) 이용한 접근을 허용하고 있는 경우
조치방법	암호화 프로토콜만 VTY에 접근 할 수 있도록 설정
점검 및 조치 사례	

■ **장비별 점검방법 예시**

- **CISCO**

```
Router# show ip ssh
SSH Enabled – version 1.5
Authentication timeout: 120 secs; Authentication retries: 3 (활성화)
%SSH has not been enabled (비 활성화)
SSH 활성화 확인
```

- **Alteon**

  /sys/sshd에서 SSH 활성화 확인

- **Juniper**

```
user@juniper# set ssh
SSH 버전 확인
```

N-16 (중)	2. 접근 관리 > 2.3 VTY 접속 시 안전한 프로토콜 사용

■ 장비별 조치방법 예시

- **CISCO**

Step 1) 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
Router(config-line)# transport input ssh
```

Step 2) SSH 접속

1. ssh 접속 프로그램 사용
2. # ssh -c rsa -l <ID><라우터IP>

- **Alteon**

Step 1) SSH 설정 방법

1. switch로 접속
2. # cfg
3. # /sys/sshd ena
4. # /sys/sshd on
5. # apply
6. # save

- **Juniper**

Step 1) SSH 버전 확인

```
user@juniper# set ssh
```

Step 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

N-17 (중)	2. 접근 관리 > 2.4 불필요한 보조 입·출력 포트 사용 금지
취약점 개요	
점검내용	■ 장비 관리나 운용에 쓰이지 않는 포트 및 인터페이스가 비활성화 되어 있는지 점검
점검목적	■ 불필요한 포트 및 인터페이스의 비활성화 여부를 점검하여 불필요한 포트 및 인터페이스를 통한 비인가자의 접근을 원천적으로 차단하는지 확인하기 위함
보안위협	■ 불필요한 포트 및 인터페이스가 활성화되어 있을 경우, 비인가자가 활성화된 포트 및 인터페이스를 통해 네트워크 장비에 접근할 수 있는 위험이 존재함
참고	-
점검대상 및 판단기준	
대상	■ CISCO, Juniper 등
판단기준	**양호 :** 불필요한 포트 및 인터페이스 사용을 제한한 경우
	취약 : 불필요한 포트 및 인터페이스 사용을 제한하지 않은 경우
조치방법	불필요한 포트 및 인터페이스 사용 제한 또는 비활성화
점검 및 조치 사례	

■ **장비별 점검방법 예시**

- **CISCO**

```
Router# show running
```

불필요한 보조 입출력 포트의 오른쪽 끝부분에 Up (활성화)
불필요한 보조 입출력 포트의 오른쪽 끝부분에 Down (비활성화)

- **Juniper**

```
user@juniper>configure
[edit]
user@juniper#show
```

root authentication 설정을 이용하여 [edit system] 레벨에서 interface 차단 설정 확인

■ **장비별 조치방법 예시**

- **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)
```

N-17 (중)	2. 접근 관리 > 2.4 불필요한 보조 입·출력 포트 사용 금지

2. 해당 인터페이스 차단

```
Router# config terminal
Router(config)# int f0/1 (해당 포트 선택)
Router(config-line)# shutdown
```

- **Juniper**

```
user@juniper> configure
[edit]
user@juniper# editinterfacesso-1/0/3
[edit interfaces so-1/0/3]
user@juniper# setunit0familyinetaddress10.0.20.1/24
user@juniper# commit
```

조치 시 영향	차단된 포트나 인터페이스를 사용해야 할 경우 별도의 활성화 설정 필요

네트워크장비

N-18 (중)	2. 계정 관리 > 2.5 로그온 시 경고 메시지 설정
취약점 개요	
점검내용	■ 터미널 접속 화면에 비인가자의 불법 접근에 대한 경고 메시지를 표시하도록 설정되어 있는지 점검
점검목적	■ 경고 메시지 표시 설정 적용 유무를 점검하여 비인가자에게 불법 적으로 터미널 접근 시 법적인 처벌에 대해 경각심을 가질 수 있게 하는지 확인하기 위함
보안위협	■ 터미널 접근 시 경고 메시지가 표시 되도록 설정되지 않을 경우, 비인가자가 법 위반에 대한 경각심을 느끼지 않게 되어 더 많은 공격을 시도할 수 있는 원인이 됨
참고	-
점검대상 및 판단기준	
대상	■ CISCO, Alteon, Juniper 등
판단기준	**양호 :** 로그온 시 접근에 대한 경고 메시지를 설정한 경우
	취약 : 로그온 시 접근에 대한 경고 메시지를 설정하지 않거나 시스템 관련 정보가 노출되는 경우
조치방법	네트워크 장비 접속 시 경고 메시지 설정
점검 및 조치 사례	

■ **장비별 점검방법 예시**

- **CISCO**

```
Router# show running-config
```

Banner 설정 내용 확인

- **Alteon**

banner <string> 설정 내용 확인

- **Juniper**

edit system login 설정 내용 확인

■ **장비별 조치방법 예시**

- **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 '#'.
```

N-18 (중)	2. 계정 관리 > 2.5 로그온 시 경고 메시지 설정

<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 or20
related organization.
Use of this system constitutes consent to monitoring for these purposes.

- **Alteon**

Step 1) switch로 접속
Step 2) `# cfg`
Step 3) `# sys`
Step 4) `# banner <string>`
Step 5) `# apply`
Step 6) `# save`

- **Juniper**

Step 1) `[edit system login]`
`message text`

조치 시 영향	일반적인 경우 영향 없음

네트워크장비

N-19 (하)	4. 로그 관리 > 4.1 원격 로그서버 사용
취약점 개요	
점검내용	■ 네트워크 장비의 로그를 별도의 원격 로그 서버에 보관하도록 설정하였는지를 점검
점검목적	■ 네트워크 장비의 로그를 별도의 원격 로그 서버에 보관하도록 설정하여 네트워크 장비에 이상이 발생하거나 로그 저장 공간 부족, 공격자의 로그 삭제나 변조 위험에 대비하기 위함
보안위협	■ 별도의 로그 서버를 통해 로그를 관리하지 않을 경우, 네트워크 장비에 이상이 발생하거나 공격자의 로그 삭제 및 변조가 일어났을 시 사고 원인 분석에 어려움이 발생함
참고	※ **원격 로그 서버**: 정보시스템(서버, 네트워크, 보안장비 등)의 로그를 통합적으로 보관하는 서버 ※ **관련 점검 항목**: A-29(상)
점검대상 및 판단기준	
대상	■ CISCO, Alteon, Juniper, Piolink 등
판단기준	**양호 :** 별도의 로그 서버를 통해 로그를 관리하는 경우
	취약 : 별도의 로그 서버가 없는 경우
조치방법	Syslog 등을 이용하여 로그 저장 설정
점검 및 조치 사례	

■ **장비별 점검방법 예시**

- **CISCO**

```
Router# show running-config
Router# show logging
```

1. Logging 설정 확인
2. Log 정보 확인

- **Alteon**

/syslog/host에서 syslog host 설정 확인

- **Juniper**

```
user@juniper> configure
[edit]
user@juniper# show version
```

root authentication 설정을 이용하여 [edit system] 레벨에서 syslog 설정 확인

N-19 (하)	4. 로그 관리 > 4.1 원격 로그서버 사용

- **Piolink**

  configure에서 logging 서버 설정 확인

■ **장비별 조치방법 예시**

- **CISCO**

  Step 1) 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)
Router(config)# logging source-interface serial 0 (syslog interface)
```

- **Alteon**

  Step 1) switch로 접속

  Step 2) # cfg

  Step 3) # sys

  Step 4) 다음과 같이 설정할 수 있음

```
# /syslog/host: first syslog host의 IP 주소 설정
# /syslog/host2: second syslog host의 IP 주소 설정
```

  Step 5) # apply

  Step 6) # save

- **Juniper**

```
user@juniper> configure
edit
user@juniper# edit system syslog
[edit system syslog]
user@juniper# set system syslog file message any error
user@juniper# set system syslog host 192.168.0.245 any any
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**

  Step 1) #logging server enable

  Step 2) #logging server <ip address><event><level>

조치 시 영향	상세한 로깅 설정은 라우터 성능에 영향을 미칠 수 있음

네트워크장비

N-20 (중)	4. 로그관리 > 4.2 로깅 버퍼 크기 설정
취약점 개요	
점검내용	■ 버퍼 메모리의 크기를 어느 정도로 설정하고 있는지 점검
점검목적	■ 장비 성능을 고려하여 최대 용량에 가깝도록 버퍼 크기를 설정하도록 함
보안위협	■ 버퍼 메모리의 용량을 초과하는 로그가 저장될 경우 로그 정보를 잃게 되어 침해사고 발생 시 침입 흔적을 알 수 없는 상황이 발생함
참고	※ **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 ※ 기본적으로 로그는 파일이 아닌 버퍼 메모리에 저장됨 ※ 최대 버퍼 크기는 65,500byte이며 버퍼 용량을 높게 설정하면 패킷 전달이 안 되는 경우가 발생함. 일반적으로 16Kbyte에서 32Kbyte의 크기가 적당하며, 최대 용량이 16Kbyte에 못 미치는 장비의 경우 장비 성능을 고려하여 최대 용량에 가깝게 설정하는 것을 권고함
점검대상 및 판단기준	
대상	■ CISCO, Piolink 등
판단기준	**양호 :** 저장되는 로그 데이터보다 버퍼 용량이 큰 경우
	취약 : 저장되는 로그 데이터보다 버퍼 용량이 작은 경우
조치방법	로그에 대한 정보를 확인하여 장비 성능을 고려한 최대 버퍼 크기를 설정
점검 및 조치 사례	

■ **장비별 점검방법 예시**

- **CISCO**

```
Router> enable
Router# show logging
```
로그에 대한 정보를 확인

메모리(RAM)에 저장된 로그는 'show logging'으로 확인할 수 있고, 'clear logging'을 실행하거나 RAM에 저장된 로그는 재부팅하면 사라지게 됨

- **Piolink**

```
(config)# show logging
```
로그에 대한 정보를 확인

N-20 (중)	4. 로그관리 > 4.2 로깅 버퍼 크기 설정

■ 장비별 조치방법 예시

- **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
```

- **Piolink**

```
(config)#logging buffer <size> (버퍼 크기 설정 범위 1~1000KB [기본설정 100KB])
(config)#logging priority <event><level>
```

조치 시 영향	버퍼 크기가 장비 성능에 비해 큰 경우 라우터 성능에 영향을 줌

네트워크장비

N-21 (중)	4. 로그관리 > 4.3 정책에 따른 로깅 설정
취약점 개요	
점검내용	■ 정책에 따른 로깅 설정이 이루어지고 있는지 점검
점검목적	■ 로그 정보를 통해 장비 상태, 서비스 정상 여부 파악 및 보안사고 발생 시 원인 파악 및 각종 침해 사실에 대한 확인을 하기 위함
보안위협	■ 로깅 설정이 되어 있지 않을 경우 원인 규명이 어려우며, 법적 대응을 위한 충분한 증거로 사용할 수 없음
참고	-
점검대상 및 판단기준	
대상	■ CISCO, Juniper 등
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
점검 및 조치 사례	

■ **장비별 점검방법 예시**

- **CISCO**

```
Router> enable
Router# show logging
```

로그에 대한 정보 확인

- **Juniper**

```
user@juniper> configure
[edit]
user@juniper# show log messages
```

로그에 대한 정보 확인

■ **장비별 조치방법 예시**

- **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

N-21 (중)	4. 로그관리 > 4.3 정책에 따른 로깅 설정

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 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

조치 시 영향	일반적인 경우 영향 없음

네트워크장비

N-22 (중)	4. 로그 관리 > 4.4 NTP 서버 연동
취약점 개요	
점검내용	■ 네트워크 장비의 NTP 서버 연동 설정 적용 여부 점검
점검목적	■ 시스템 운영 또는 보안사고 발생으로 인한 로그 분석 과정에서 이벤트 간의 인과 관계 파악에 도움을 주고 로그 자체의 신뢰성을 갖도록 함
보안위협	■ 시스템 간 시간 동기화 미흡으로 보안사고 및 장애 발생 시 로그에 대한 신뢰도 확보 미흡
참고	※ IOS 12.2 이전 버전을 사용하는 장비에는 접근 통제(ACL) 설정이 되어 있어야 양호
점검대상 및 판단기준	
대상	■ CISCO, Alteon, Juniper 등
판단기준	**양호 :** NTP 서버를 통한 시스템 간 실시간 시간 동기화가 설정된 경우
	취약 : NTP 서버와 연동되어 있지 않아 시스템 간 실시간 시간 동기화 설정이 되어 있지 않은 경우
조치방법	NTP 사용 시 신뢰할 수 있는 서버로 설정
점검 및 조치 사례	

■ **장비별 점검방법 예시**

- **CISCO**

```
Router# show running-config
```

NTP 서버 설정 확인

- **Alteon**

/sys/ntp에서 NTP 서버 설정 확인

- **Juniper**

```
user@juniper> configure
[edit]
user@juniper# show
```

root authentication 설정을 이용하여 [edit system] 레벨에서 NTP 서비스 설정 확인

■ **장비별 조치방법 예시**

- **CISCO**

Step 1) NTP 서버 연동 설정

```
Router# config terminal
Router(config)# ntp server 129.237.32.2 (NTP 서버 IP)
Router(config)# ^Z
```

N-22 (중)	4. 로그 관리 > 4.4 NTP 서버 연동

- **Alteon**

Step 1) switch로 접속함.
Step 2) # cfg
Step 3) # /sys/ntp
Step 4) # on
Step 5) # prisrvr [NTP 서버 IP]
Step 6) # intrval [동기화 주기]
tzone +9:00
Step 7) # apply
Step 8) # save

- **Juniper**

Step 1) 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 ative 모드
  user@juniper# set peer (NTP 서버주소) prefer
  user@juniper# set peer (NTP 서버주소)

조치 시 영향	일반적인 경우 영향 없음

네트워크장비

N-23 (하)	4. 로그 관리 > 4.5 timestamp 로그 설정
취약점 개요	
점검내용	■ 네트워크 장비 설정 중 timestamp를 설정하여 로그 시간을 기록할 수 있게 하였는지 점검
점검목적	■ 네트워크 장비 로그에 시간을 기록하게 설정하여 공격자의 악의적인 행위를 파악하기 위한 로그의 신뢰성을 확보하기 위함
보안위협	■ 네트워크 장비에 timestamp를 설정하지 않을 경우, 로그에 시간이 기록 되지 않아 공격 및 침입시도에 관한 정보를 정확히 분석할 수 없고 로그 기록에 대한 신뢰성을 잃게 됨
참고	※ **timestamp**: 네트워크 장비 로그 메시지에 관리자가 지정한 형식으로 시간 정보를 남기도록 하는 설정
점검대상 및 판단기준	
대상	■ CISCO, Juniper 등
판단기준	**양호 :** timestamp 로그 설정이 되어있는 경우
	취약 : timestamp 로그 설정이 되어있지 않은 경우
조치방법	로그에 시간 정보가 기록될 수 있도록 timestamp 로그 설정
점검 및 조치 사례	

■ **장비별 점검방법 예시**

- **CISCO**

```
Router> enable
Router# show logging    로그의 기록 정보 설정 확인
```

- **Juniper**

```
user@juniper> configure
[edit]
user@juniper# show log messages  로그의 기록 정보 설정 확인
```

■ **장비별 조치방법 예시**

- **CISCO**

```
Router# config terminal
Router(config)#service timestamp log date time msec local show-timezone
(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

N-24 (중)	5. 기능 관리 > 5.9 TCP Keepalive 서비스 설정
취약점 개요	
점검내용	■ 네트워크 장비 서비스 중 keepalive 서비스의 활성화 여부를 점검
점검목적	■ TCP/IP 기반으로 연결된 상태에서 클라이언트의 의도하지 않은 리부팅이나 스위치 Off가 일어날 경우 해당 세션을 서버에서 자동으로 종료하지 못하므로 Keepalive 기능을 활성화하여 비정상적으로 종료된 세션을 정상적으로 종료 될 수 있도록 하기 위함
보안위협	■ 네트워크 장비에 TCP Keepalive 기능이 활성화되지 않으면 대량의 세션을 맺어 서비스를 마비시키는 TCP SYN Flooding 등의 DoS 공격이 가능해 짐
참고	※ **keepalive:** 유휴 연결인지 확인하기 위해 데이터가 없는 prove 패킷을 보내어 비정상적으로 종료된 세션을 감지하여 정상적으로 종료시켜 주는 기능
점검대상 및 판단기준	
대상	■ CISCO 등
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
점검 및 조치 사례	
■ **장비별 점검방법 예시** • **CISCO** `Router# show running-config` TCP Keepalive 서비스 설정 확인 ■ **장비별 조치방법 예시** • **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

N-25 (중)	5. 기능 관리 > 5.10 Finger 서비스 차단
취약점 개요	
점검내용	■ 네트워크 장비 서비스 중 Finger 서비스가 활성화되고 있는지를 점검
점검목적	■ Finger(사용자 정보 확인 서비스)를 통해 네트워크 외부에서 해당 시스템에 등록된 사용자 정보를 확인할 수 있어 비인가자에게 사용자 정보가 조회되는 것을 차단하고자 함
보안위협	■ Finger 서비스가 활성화되어 있으면, 장비의 접속 상태가 노출될 수 있고 VTY(Virtual Type terminal)의 사용 현황을 원격에서 파악하는 것이 가능함
참고	※ **Finger(사용자 정보 확인 서비스):** finger 서비스는 접속된 시스템에 등록된 사용자뿐만 아니라 네트워크를 통하여 연결된 다른 시스템에 등록된 사용자들에 대한 자세한 정보를 보여줌
점검대상 및 판단기준	
대상	■ CISCO, Juniper 등
판단기준	**양호 :** Finger 서비스를 차단하고 있는 경우
	취약 : Finger 서비스를 차단하고 있지 않는 경우
조치방법	각 장비별 Finger 서비스 제한 설정
점검 및 조치 사례	

■ **장비별 점검방법 예시**

- **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

N-25 (중)	5. 기능 관리 > 5.10 Finger 서비스 차단

■ 장비별 조치방법 예시

- **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

N-26 (중)	5. 기능 관리 > 5.11 웹 서비스 차단
취약점 개요	
점검내용	■ 웹서비스를 이용하여 네트워크 장비를 관리할 경우 허용된 IP에서만 접속할 수 있게 ACL을 적용하였는지 점검 ■ 웹서비스가 불필요(장비 관리에 사용하지 않은 경우 포함)하게 활성화 되어 있는지 점검
점검목적	■ 허용된 IP만 웹 관리자 페이지에 접속할 수 있도록 설정하는지 점검하여 비인가자가 웹 관리자 페이지를 공격하여 네트워크 장비를 장악하지 못하도록 하기 위함
보안위협	■ 허용된 IP에서만 웹 관리자 페이지 접속을 가능하게 ACL 적용하지 않을 경우, 공격자는 알려진 웹 취약점(SQL 인젝션, 커맨드 인젝션 등)이나 자동화된 패스워드 대입 공격을 통하여 네트워크 장비의 관리자 권한을 획득할 수 있음
참고	※ IOS 상의 HTTP 서버를 사용해야만 한다면, HTTP WEB_EXEC 서비스를 비활성화 함으로써 위험을 감소시킬 수 있음
점검대상 및 판단기준	
대상	■ CISCO 등
판단기준	**양호 :** 불필요한 웹 서비스를 차단하거나 허용된 IP에서만 웹서비스 관리 페이지에 접속이 가능한 경우
	취약 : 불필요한 웹 서비스를 차단하지 않은 경우
조치방법	HTTP 서비스 차단 또는 HTTP 서버를 관리하는 관리자 접속 IP 설정
점검 및 조치 사례	

■ **장비별 점검방법 예시**

- **CISCO**

```
Router# show running-config   웹 서비스 설정 확인
```

■ **장비별 조치방법 예시**

- **CISCO**

```
Router# config terminal
Router(config)# no ip http server
Router(config)# ^Z

Router# config terminal
Router(config)# ip http active-session-modules exclude_webexec
Router(config)# ip http secure-active-session-modules exclude_webexec
Router(config)# ^Z
```

조치 시 영향	일반적인 경우 영향 없음

N-27 (중)	5. 기능관리 > 5.12 TCP/UDP Small 서비스 차단
취약점 개요	
점검내용	■ TCP/UDP Small 서비스가 제한되어 있는지 점검
점검목적	■ TCP/UDP Small 서비스를 차단하여 보안성을 높이고자 함
보안위협	■ TCP/UDP Small 서비스를 차단하지 않을 경우, DoS 공격의 대상이 될 수 있음
참고	※ **Dos 공격 대상:** CISCO 제품의 경우 DoS 공격 대상이 될 수 있는 서비스인 echo, discard, daytime, chargen 을 기본적으로 제공하며 일반적으로 거의 사용하지 않음 ※ TCP/UDP Small 서비스는 IOS 11.3 이상에서는 기본적으로 서비스가 제거된 상태이므로 Small 서버들이 Default로 Disable되어 있지만 낮은 버전의 경우는 직접 설정해 주어야 함
점검대상 및 판단기준	
대상	■ CISCO 등
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
점검 및 조치 사례	

■ **장비별 점검방법 예시**

- **CISCO**

```
Router# show running-config
```

1. tcp-small-servers 설정 확인
2. udp-small-servers 설정 확인

■ **장비별 조치방법 예시**

- **CISCO**

1. 서비스 거부 공격을 완전히 차단하지는 못하지만, 알려진 서비스 거부 공격 포트 설정 권고
2. TCP/UDP 관련 Small 서버들의 기능은 Disable 설정함

```
Router# config terminal
Router(config)# no service tcp-small-servers
Router(config)# no service udp-small-servers
Router(config)# ^Z
```

조치 시 영향	일반적인 경우 영향 없음

네트워크장비

N-28 (중)	5. 기능관리 > 5.13 Bootp 서비스 차단
취약점 개요	
점검내용	■ Bootp 서비스의 차단 여부 점검
점검목적	■ 서비스 제거를 통해 비인가자에게 OS 정보가 노출되는 것을 차단함
보안위협	■ Bootp 서비스를 차단하지 않을 경우, 다른 라우터 상의 OS 사본에 접속하여 OS 소프트웨어 복사본을 다운로드 할 수 있음
참고	※ **Bootp 서비스:** 네트워크를 이용하여 사용자가 OS를 로드할 수 있게 하고 자동으로 IP주소를 받게 하는 프로토콜임
점검대상 및 판단기준	
대상	■ CISCO, Alteon, Juniper 등
판단기준	**양호 :** Bootp 서비스가 제한되어 있는 경우
	취약 : Bootp 서비스가 제한되어 있지 않는 경우
조치방법	각 장비별 Bootp 서비스 제한 설정
점검 및 조치 사례	

■

■ **장비별 점검방법 예시**

- **CISCO**

  `Router# show running-config`

  ip bootp server 설정 확인

- **ALteon**

  `#bootp disable` 설정 확인

- **Juniper**

  `user@switch>show configuration & show interfaces detail`

  bootp 서비스 설정 확인

■ **장비별 조치방법 예시**

- **CISCO**

  라우터를 자동리부팅 하는 취약점이 존재하므로 서비스를 차단하여 방어하기를 권고함

  Bootp 차단 설정

  ```
  Router# config terminal
  Router(config)# no ip bootp server
  ```

N-28 (중)	5. 기능관리 > 5.13 Bootp 서비스 차단

- **Alteon**

  Step 1) 스위치로 접속

  Step 2) `#cfg`

  Step 3) `#sys`

  Step 4) `#bootp disable|enable`

  Step 5) `#apply`

  Step 6) `#save`

- **Juniper**

  DHCP 서버 IP 주소와 서버가 연결되어 있는 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

N-29 (중)	5. 기능관리 > 5.14 CDP 서비스 차단
취약점 개요	
점검내용	■ CDP 서비스의 차단 여부 점검
점검목적	■ 동일 네트워크에 있는 다른 CISCO 장비들의 정보 유출 방지 및 DoS 공격을 차단하기 위함
보안위협	■ 보안이 검증 되지 않은 서비스로, 비인가자가 다른 cisco 장비의 정보를 획득할 수 있으며, Routing Protocol Attack 을 통해 네트워크 장비의 서비스 거부 공격을 할 수 있음
참고	※ **CDP(Cisco Discovery Protocol):** Cisco 제품의 관리를 목적으로 만든 프로토콜로 같은 네트워크에 있는 장비들과 정보를 공유하고, 같은 세그먼트에 있는 다른 라우터에 IOS version, Model, device 등의 정보를 제공함
점검대상 및 판단기준	
대상	■ CISCO 등
판단기준	**양호 :** CDP 서비스가 제한되어 있는 경우
	취약 : CDP 서비스가 제한되어 있지 않는 경우
조치방법	각 장비별 CDP 서비스 제한 설정
점검 및 조치 사례	

■ **장비별 점검방법 예시**

- **CISCO**

```
Router# show running-config
Router# show cdp
```

1. cdp run 설정 확인
2. global CDP 정보 확인

※ CDP를 라우터 전체에서 사용하지 못하도록 하기 위해서는 no cdp run 명령어가 사용되며, 특정 인터페이스에서 사용하지 못하도록 하려면 no cdp enable 명령어를 사용함

■ **장비별 조치방법 예시**

- **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

N-30 (중)	5. 기능관리 > 5.15 Directed-broadcast 차단
취약점 개요	
점검내용	■ Directed-broadcast 서비스의 차단 여부 점검
점검목적	■ Directed-broadcast 서비스 차단을 통해 DoS 공격을 방지하기 위함
보안위협	■ IP Directed-Broadcast는 유니캐스트 IP 패킷이 특정 서브넷에 도착 했을 때 링크-레이어 브로드캐스트로 전환되는 것을 허용함. 이것은 보통 악의적으로 이용되며, 특히 smurf 공격에 이용됨
참고	※ **Smurf 공격:** 인터넷 프로토콜(IP) 브로드캐스트나 기타 인터넷 운용 측면을 이용하여 인터넷망을 공격하는 행위로 브로드캐스트에 대한 응답받을 IP 주소를 변조하여 해당 IP 주소 호스트에 DoS 공격을 감행하는 공격 기법
점검대상 및 판단기준	
대상	■ CISCO, Alteon, Passport, Juniper 등
판단기준	**양호 :** Directed Broadcasts가 제한된 경우
	취약 : Directed Broadcasts가 제한되지 않은 경우
조치방법	각 장치별로 Directed Broadcasts 제한 설정
점검 및 조치 사례	

■ **장비별 점검방법 예시**

- **CISCO**

```
Router# show running-config
```

Directed-Broadcast 설정 확인

- **Alteon**

dirbr에서 disable 설정 확인

- **Passport**

config에서 ip directed-broadcast 설정 확인

- **Juniper**

```
user@juniper> configure
[edit]
user@juniper# show
```

root authentication 설정을 이용하여 [edit system] 레벨에서 Directed-Broadcast 설정 확인

네트워크장비

N-30 (중)	5. 기능관리 > 5.15 Directed-broadcast 차단

■ **장비별 조치방법 예시**

- **CISCO**

1. Smurf Attack 공격 예방

다량의 ICMP 패킷(Echo Request Packet)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)# access-list 108 deny icmp any host 1.1.1.255
(1.1.1.0/24 의 broadcast address인 1.1.1.255 ICMP 차단)
Router(config)# access-list 108 deny icmp any host 1.1.1.0
(1.1.1.0/24 의 network address인 1.1.1.0 ICMP 차단)
```

2. Directed Broadcast 차단

Cisco IOS는 내부 사용자가 외부 네트워크의 Broadcast 주소로 요청할 수 없도록 이와 관련된 설정이 이미 Default로 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**

Step 1) switch로 접속
Step 2) `# cfg/l3/frwd`
Step 3) `# dirbr disable`
Step 4) `# apply`
Step 5) `# save`

- **Passport**

Step 1) Switch로 접속
Step 2) `# config vlan <vid> ip directed-broadcast`
Step 3) `# disable`

- **Juniper**

```
user@juniper> configure
[edit]
user@juniper# no ip directed-broadcast
```

조치 시 영향	일반적인 경우 영향 없음

N-31 (중)	5. 기능관리 > 5.16 Source 라우팅 차단
취약점 개요	
점검내용	■ source routing 서비스의 차단 여부 점검
점검목적	■ 인터페이스마다 no ip source-route를 적용하여 ip spoofing을 차단함
보안위협	■ 공격자가 source routing된 패킷을 네트워크 내부에 발송할 수 있을 경우, 수신된 패킷에 반응하는 메시지를 가로채어 사용자 호스트를 마치 신뢰 관계에 있는 호스트와 통신하는 것처럼 만들 수 있음
참고	※ **source routing:** 송신 측에서 routing 경로 정보를 송신 데이터에 포함해 routing시키는 방법으로 패킷이 전송되는 경로를 각각의 시스템이나 네트워크에 설정되어 있는 라우팅 경로를 통하지 않고 패킷 발송자가 설정 할 수 있는 기능임
점검대상 및 판단기준	
대상	■ CISCO, Juniper 등
판단기준	**양호 :** ip source route가 제한된 경우
	취약 : ip source route가 제한되지 않은 경우
조치방법	각 인터페이스별로 ip source route 제한 설정
점검 및 조치 사례	

■ **장비별 점검방법 예시**

- **CISCO**

```
Router# show running-config
```

ip source route 설정 확인

- **Juniper**

```
user@juniper# show route
```

ip source route 설정 확인

■ **장비별 조치방법 예시**

- **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

N-32 (중)	5. 기능관리 > 5.17 Proxy ARP 차단
취약점 개요	
점검내용	■ ARP 프록시(Proxy) 서비스 제한 여부를 점검함
점검목적	■ Proxy ARP 차단으로 IP와 MAC이 관련된 호스트에 대해 정상적인 통신을 유지함
보안위협	■ Proxy ARP를 차단하지 않을 경우, 악의적인 사용자가 보낸 거짓 IP와 MAC 정보를 보관하게 되며 이로 인해 호스트와 호스트 사이에서 정상적인 통신이 이루어지지 않을 수 있음
참고	※ **ARP 프록시(Proxy):** 게이트웨이를 가지고 있지 않은 네트워크의 호스트들에게 arp 서비스를 제공하는 역할을 함. IP와 MAC주소의 캐시 기능을 제공
점검대상 및 판단기준	
대상	■ CISCO, Alteon, Juniper 등
판단기준	**양호 :** ARP Proxy 서비스가 제한되어 있는 경우
	취약 : ARP Proxy 서비스가 제한되어 있지 않는 경우
조치방법	각 장비별 ARP Proxy 서비스 제한 설정
점검 및 조치 사례	

■ **장비별 점검방법 예시**

- **CISCO**

```
Router# show running-config
```

각 인터페이스 정보에서 Proxy ARP 설정 확인

- **ALteon**

proxy disable 설정 확인

- **Juniper**

```
user@juniper# show
proxy {
          inet-address inet-address;
      }
```

proxy로 검색하여 특정 MAC과 IP로 제한하거나 off되어 있는지 확인

■ **장비별 조치방법 예시**

- **CISCO**

Proxy ARP를 차단하기 위해서는 no ip proxy-arp 명령 사용

<이더넷 인터페이스에 대한 적용 예>

N-32 (중)	5. 기능관리 > 5.17 Proxy ARP 차단

```
Router# config terminal
Router(config)# interface fastethernet 0/1
Router(config-line)# no ip proxy-arp
Router(config)# ^Z
```

- **Alteon**

  Step 1) switch 접속
  Step 2) `# cfg`
  Step 3) `# /slb/real`
  Step 4) `# proxy disable`
  Step 5) `# apply`
  Step 6) `# save`

- **Juniper**

```
user@juniper> configure
[edit]
user@juniper# delete interfaces (interface-name) unit logical - unit
-member proxy-arp
```

조치 시 영향	일반적인 경우 영향 없음

네트워크장비

N-33 (중)	5. 기능관리 > 5.18 ICMP unreachable, Redirect 차단
취약점 개요	
점검내용	■ ICMP unreachable, redirect 서비스 차단 여부 점검
점검목적	■ ICMP unreachable 차단으로 DoS 공격을 차단하고 공격자가 네트워크 스캔 시 소요되는 시간을 길어지게 하여 스캔 공격을 지연 및 차단함 ■ ICMP redirect 차단으로 라우팅 테이블이 변경되는 것을 차단하기 위함
보안위협	■ ICMP unreachable을 차단하지 않을 경우, 공격자의 스캔 공격을 통해 시스템의 현재 운영되고 있는 상태 정보가 노출될 수 있음 ■ ICMP redirect을 차단하지 않을 경우, 호스트 패킷 경로를 다시 지정하는 과정에서 특정 목적지로 가기 위해 고의적으로 패킷 경로를 변경하여 가로챌 수 있음 ■ 연속적으로 ICMP의 port-unreachable frame을 보내서 시스템의 성능을 저하시키거나 마비시킬 수 있음..
참고	※ **ICMP unreachable:** ICMP unreachable 메시지에는 특정 호스트 및 게이트웨이에 패킷을 보냈을 때 어떠한 이유로 전달될 수 없는지 나타내는 코드들을 포함하고 있음 ※ **ICMP redirect:** ICMP redirect는 라우터가 송신 측 호스트에 적합하지 않은 경로로 설정되어 있으면 해당 호스트에 대한 최적 경로를 다시 지정해주는 용도로 사용됨
점검대상 및 판단기준	
대상	■ CISCO, Juniper 등
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
점검 및 조치 사례	

■ **장비별 점검방법 예시**

- **CISCO**

```
Router> enable
Router# show running
```

각 인터페이스별 정보에 적용된 것을 확인

- **Juniper**

```
user@juniper# show
```

ICMP Unreachables , ICMP redirects 적용 확인

N-33 (중)	5. 기능관리 > 5.18 ICMP unreachable, Redirect 차단

■ 장비별 조치방법 예시

- **CISCO**

인터페이스에 no ip unreachables를 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
[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 많은 시간이 경과 될 수 있음

네트워크장비

N-34 (중)	5. 기능관리 > 5.19 identd 서비스 차단
취약점 개요	
점검내용	■ identd 서비스 차단 여부 점검
점검목적	■ 보안과 속도 등의 문제 해결을 위해 identd 서비스를 차단함
보안위협	■ identd 서비스를 차단하지 않을 경우, 인증 데몬에 대한 응답을 받을 때 유효성을 체크하지 않고 전적으로 클라이언트에서 처리하므로 인증이 위조될 수 있음
참고	※ **identd 서비스:** 네트워크 장비에 접속을 요청한 사용자에 대한 신원 확인을 위해 사용함
점검대상 및 판단기준	
대상	■ CISCO 등
판단기준	**양호 :** identd 서비스가 차단되어 있는 경우
	취약 : identd 서비스가 차단되어 있지 않은 경우
조치방법	idnetd 서비스 차단 설정
점검 및 조치 사례	

■ **장비별 점검방법 예시**

- **CISCO**

```
Router> enable
Router# show running
```

identd 설정 확인

■ **장비별 조치방법 예시**

- **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

N-35 (중)	5. 기능관리 > 5.20 Domain lookup 차단
취약점 개요	
점검내용	■ Domain lookup 서비스 차단 여부 점검
점검목적	■ CLI 에서 오타 및 특정 명령어를 잘못 입력했을 경우, 장비가 도메인을 찾는 과정을 없애도록 함
보안위협	■ 주위 서버나 라우터와의 정보 공유로 인해 네트워크 속도가 저하되거나 불필요한 시간을 낭비하게 됨
참고	※ **Domain lookup:** 라우터 상에서 명령어 수행 시 오타가 발생하는 경우 그 명령어를 주위의 인접한 서버나 라우터에 묻는 역할을 함
점검대상 및 판단기준	
대상	■ CISCO, Juniper 등
판단기준	**양호 :** Domain lookup이 차단되어 있는 경우
	취약 : Domain lookup이 차단되어 있지 않은 경우
조치방법	Domain Lookup 차단 설정
점검 및 조치 사례	
■ **장비별 점검방법 예시** • **CISCO** `Router> enable` Router# show running 모드로 접속하여 확인 • **Juniper** `user@juniper# show ip domain-lookup [ filter ]` no ip domain-lookup 설정 확인 ■ **장비별 조치방법 예시** • **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

N-36 (중)	5. 기능관리 > 5.21 pad 차단
취약점 개요	
점검내용	■ pad 서비스 차단 여부 점검
점검목적	■ X.25 프로토콜을 사용하지 않을 경우 pad 서비스를 중지함
보안위협	■ pad 서비스는 불필요한 서비스로 차단하지 않을 경우, 보안 허점이나 감염된 장치를 찾는 해커들에게 침입할 수 있는 기회를 제공하게 됨
참고	※ **pad 서비스:** 라우터 서비스 중 하나로 Packet assembler/disassembler 라는 뜻의 서비스로서 기계적인 패킷을 서비스 할 때(주로 X.25 프로토콜 사용 시) 사용함
점검대상 및 판단기준	
대상	■ CISCO, Juniper 등
판단기준	**양호 :** pad 서비스가 차단되어 있는 경우
	취약 : pad 서비스가 차단되어 있지 않은 경우
조치방법	pad 서비스 차단 설정
점검 및 조치 사례	

■ **장비별 점검방법 예시**

- **CISCO**

```
Router> enable
```

Router# show running 모드로 접속하여 확인

- **Juniper**

```
user@juniper> configure
[edit]
user@juniper# show
```

pad 설정 확인

■ **장비별 조치방법 예시**

- **CISCO**

pad 차단 설정

```
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

N-37 (중)	5. 기능관리 > 5.22 mask-reply 차단
취약점 개요	
점검내용	■ mask-reply 서비스 차단 여부 점검
점검목적	■ mask-reply 서비스를 차단하여 신뢰할 수 없는 네트워크에 netmask 정보를 제공하지 않음
보안위협	■ mask-reply 서비스를 차단하지 않을 경우, 비인가자에게 네트워크 구성 정보가 노출될 수 있음
참고	※ **mask-reply 서비스:** 인터페이스를 통해 netmask를 요청하는 ICMP 패킷 발송 시 응답해주는 역할을 함
점검대상 및 판단기준	
대상	■ CISCO, Juniper 등
판단기준	**양호 :** mask-reply가 차단되어 있는 경우
	취약 : mask-reply가 차단되어 있지 않은 경우
조치방법	mask-reply 차단 설정
점검 및 조치 사례	

■ **장비별 점검방법 예시**

- **CISCO**

만약 serial interface 1/0 에 no ip mask-reply 설정을 하였다면

```
Router# config terminal
Router(config)# show ip interface serial1/0
```

(아래의 config를 볼 수 있지만 브로드 캐스트 포워딩이 다르다.)

```
!
Directed broadcast forwarding is * disabled * <- 변경후
ICMP redirects are never sent
ICMP unreachables are never sent
ICMP mask replies are never sent
!
Directed broadcast forwarding is * enable * <- 변경전
ICMP redirects are never sent
ICMP unreachables are never sent
ICMP mask replies are never sent
!
```

N-37 (중)	5. 기능관리 > 5.22 mask-reply 차단

- **Juniper**

```
user@juniper> configure
[edit]
user@juniper# show interface terse
```

■ **장비별 조치방법 예시**

- **CISCO**

reply 설정 차단

```
Router# config terminal
Router(config)# interface serial 1/0
Router(config)# no ip mask-reply
```

- **Juniper**

```
user@juniper> configure
[edit]
user@juniper# no ip mask-reply
```

조치 시 영향	일반적인 경우 영향 없음

네트워크장비

N-38 (하)	5. 기능관리 > 5.23 스위치, 허브 보안 강화
취약점 개요	
점검내용	■ 스위치나 허브에서 포트 보안, SPAN 설정이 적용되고 있는지 점검
점검목적	■ 보안설정을 통해 네트워크 트래픽이 비인가자에게 노출 또는 변조되지 않도록 함
보안위협	■ 포트 보안을 설정하지 않을 경우, 동일 네트워크 내에서 mac flooding, arp spoofing 공격으로 비인가자에게 패킷 정보가 제공될 수 있음
참고	※ **SPAN:** Switch Port Analyzer 로 스위치의 특정 포트에 분석장비를 접속하고 다른 포트의 트래픽을 분석장비로 자동 복사해주는 기술을 말함
점검대상 및 판단기준	
대상	■ 스위치, 허브
판단기준	**양호 :** 스위치나 허브에 포트 보안, SPAN 설정이 적용되어 있는 경우
	취약 : 스위치나 허브에 포트 보안, SPAN 설정이 적용되어 있지 않는 경우
조치방법	장비별 보안 위협에 관한 대책 설정 적용(포트 보안, SPAN 설정)
점검 및 조치 사례	

■ **장비별 점검방법 예시**

- **스위치 / 허브**

1. 포트 보안 설정 확인

`Switch> enable`

`Switch# show port-security address` 명령을 통해 확인

2. SPAN 설정 확인

`Switch> enable`

`Switch# show monitor` 명령을 통해 확인

※ 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/ community의 포트 속성을 정의하여 트래픽 이동에 대한 제한이 가능함

네트워크장비

N-38 (하)	5. 기능관리 > 5.23 스위치, 허브 보안 강화

■ **장비별 조치방법 예시**

- **스위치 / 허브 포트 보안 설정**

1. 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
```

2. 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	보안 침해 발생 시 해당 장비에 접속을 차단. 허용된(보안용 맥주소로 등록된) 호스트는 허용
restrict Security violation restrict mode	protect mode 기능과 더불어 보안 침해 호스트에 대한 로깅 메시지 발생, 보안 침해 카운터 증가
shutdown Security violation shutdown mode	보안 침해 발생 시 해당 포트 shutdown

3. 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)

- **스위치 / 허브 SPAN 보안 설정**

```
(config)# monitor session 1 source interface Fastethernet 1/1
```

: 소스포트를 지정, 소스포트 - 트래픽을 캡쳐하려고 하는 포트

```
(config)# monitor session 1 destination interface Fastethernet 1/10
```

: Fa1/1 포트를 통해 입/출력되는 모든 프레임이 Fa1/10 포트(목적지포트)로 복사

`# show monitor` 명령어로 설정 확인

`# show interface |`해당포트`|`

: 상태가 모니터링(Monitoring)으로 표시됨

```
(config)# monitor session 1 source interface Fastethernet 1/2 both
(config)# monitor session 1 destination interface Fastethernet 1/1,
Fastethernet 1/5 - 7 rx
```

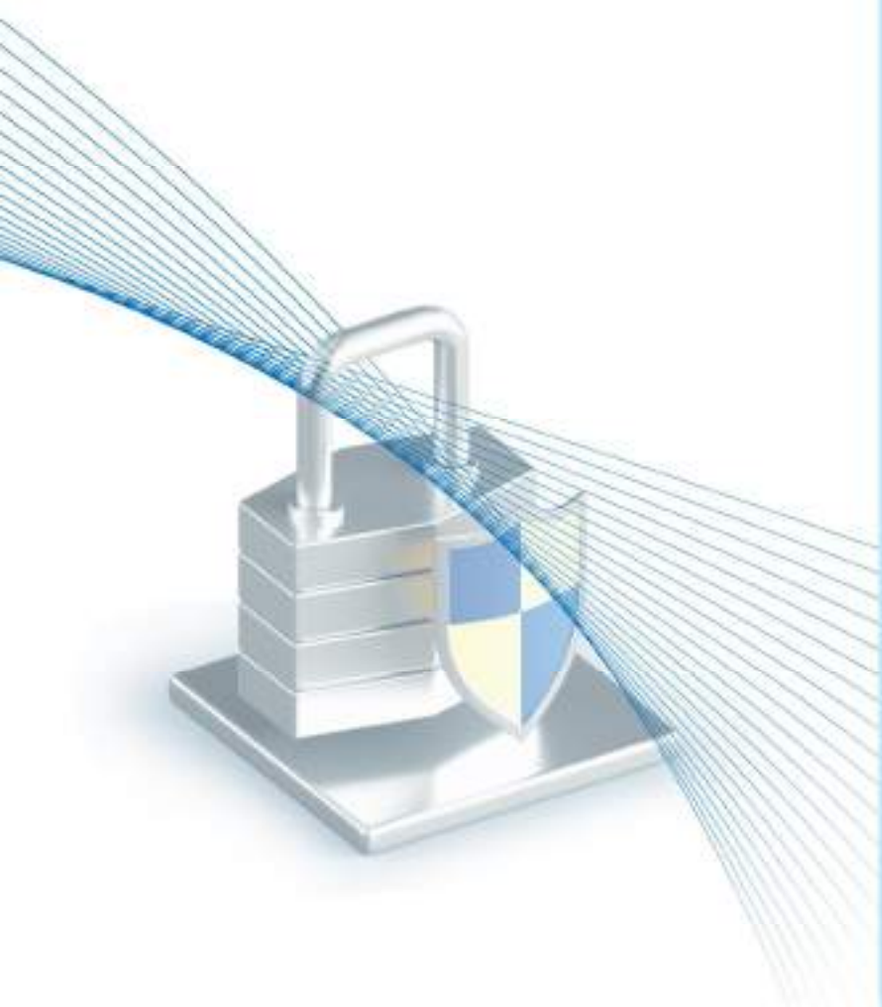
: 포트 1/2은 양방향 트래픽을 미러링, 나머지는 수신 트래픽만 미러링

조치 시 영향	일반적인 경우 영향 없음

Ⅱ

제어시스템

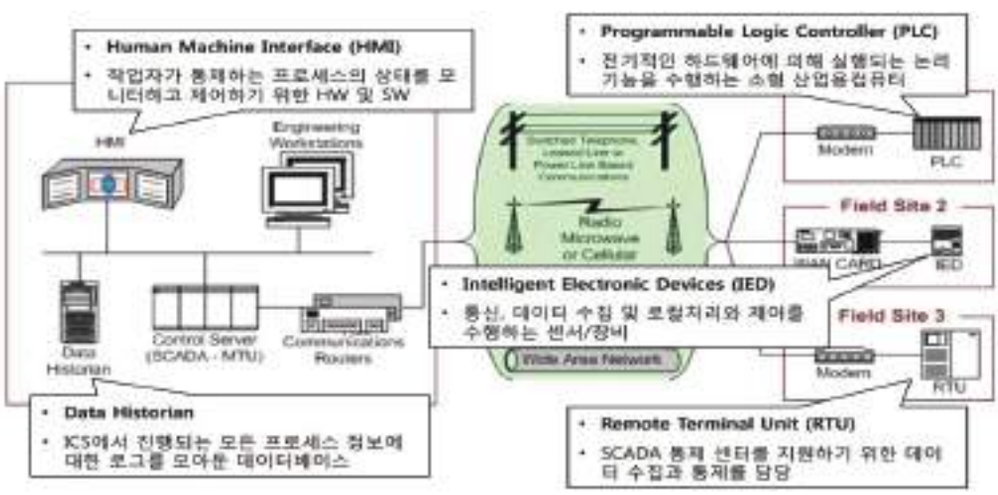
기본/선택



제어시스템 취약점 분석·평가 항목

분류	점검항목	중요도	항목코드
1. 계정관리	제어시스템 운영, 관리를 위한 계정이 타 사용자와 공유되지 않음	상	C-01
	ID/PW, 접속경로, 인증서 등이 하드코딩되지 않음	상	C-02
	제어시스템 운영, 관리를 위한 계정의 로그인, 사용 기록 저장	상	C-03
2. 패치관리	제어시스템에 대한 최신 업데이트, 보안패치를 안전하게 적용하기 위한 테스트 등의 절차 수립	상	C-04
3. 접근통제	제어시스템 운영자의 운영 권한은 제한된 범위 및 명령으로 제한	상	C-05
	제어시스템은 업무망, 인터넷 망과 물리적으로 분리	상	C-06
	제어 네트워크 외부와 자료연계 시 물리적 일방향 환경을 구축하여 제어 네트워크로의 침입을 근본적으로 차단	상	C-07
	제어 네트워크에 무선인터넷, 테더링, 외부망등 연결 등의 외부망 연결을 제한하고 점검	상	C-08
	제어 네트워크에 비인가된 시스템에 대한 연결 및 접속 차단	상	C-09
4. 보안관리	제어시스템 구성도, 운용 매뉴얼, 비상조치 절차서 등을 작성하고 최신으로 관리	상	C-10
	제어시스템에서의 USB 사용을 금지하고, 사용시 USB 등의 이동형 저장매체 사용 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 에러메시지가 출력되도록 하여 시스템 중요정보가 노출되지 않도록 설정	상	C-16
	정보시스템에 대한 정책과 별도로 제어시스템에 대한 정보보안 정책, 지침이 수립되어 있는가?	중	CS-17
	비인가자 또는 인증과정이 없는 제어시스템, 제어기기에 대한 환경 설정이 가능하지 않도록 되어있는가?	중	CS-18
	제어시스템 및 운영시스템은 제어를 위한 목적으로만 사용되도록 다른 기능 및 서비스를 제거하였는가?	중	CS-19
	운영에 있어 사용가능한 제어명령 및 안전한 제어를 위한 파라미터의 범위를 제한하고 있는가?	중	CS-20
	제어시스템 개선, 신규 시스템 도입, 패치 및 수정 시, 안전성을 테스트하기 위한 테스트베드 또는 시험환경을 구축하였는가?	중	CS-21
	제어 네트워크는 각각의 세부망으로 세분화하고 제어시스템 운영에 필요한 네트워크, 시스템 간으로 통신을 제한하고 있는가?	중	CS-22

제어시스템

C-01 (상)	1. 계정관리 > 1.1 제어시스템 운영, 관리를 위한 계정이 타 사용자와 공유되지 않음
취약점 개요	
점검내용	■ 제어시스템의 운영, 관리를 위한 사용자 및 관리자 계정을 1인 1계정으로 사용하는지 점검
점검목적	■ 제어시스템의 사용자 및 관리자 계정은 1인 1계정을 사용하도록 하여 계정 사용에 대한 책임추적성(Accountability)을 높일 수 있도록 함
보안위협	■ 운영상 편의를 위하여 다수의 인원이 HMI 공용계정을 사용하고 패스워드를 공유하는 경우 패스워드 노출, 권한 남용, 사용자 책임 추적 어려움 등의 우려가 있음
참고	※ **책임추적성(Accountability):** 정보시스템의 접속자, 접속시간, 접속위치, 업무내역 등을 식별하여 장애 원인, 침해사고 경위 등을 조사하는 과정에서 책임을 규명할 수 있도록 하는 것을 의미 ※ 제어시스템의 기본 구성도 및 각 구성요소  ※ HMI 및 PLC 예시  [그림] HMI 화면 예시  [그림] PLC 기기 예시

제어시스템

C-01 (상)	1. 계정관리 > 1.1 제어시스템 운영, 관리를 위한 계정이 타 사용자와 공유되지 않음
점검대상 및 판단기준	
대상	■ 분산네트워크 환경에서 HMI, PLC 등의 S/W를 통해 대상 시스템 및 기기에 접속하기 위해 계정(ID) 접근이 요구되는 제어시스템 ■ HMI 및 DB 서버
판단기준	**양호:** 1인 1계정을 사용하는 경우
	취약: 공용 계정을 사용하는 경우
조치방법	운영자, 관리자 등 1인 1계정 발급
점검 및 조치 사례	

Step 1) HMI, PLC 등의 소프트웨어(어플리케이션)를 통해 각 시스템 및 기기에 접근하기 위하여 사용하는 계정(ID) 목록과 각 계정을 사용하는 운영자 및 관리자 명단을 확인
(이 경우 다음 사항을 포함하여 점검)
- 공용 계정을 사용하는지 확인
- 접속기록(Log)을 통해 계정별 지정된 단일 IP에서 접속이 이루어지는지 확인
(2개 이상의 IP주소에서 접속이 있거나, 단일 IP를 사용하더라도 해당 업무PC를 서로 다른 인원이 사용한다면 공용계정으로 판단)

Step 2) HMI, DB 서버 등의 운영체제 계정(ID) 목록과 각 계정을 사용하는 인원의 명단을 확인(이 경우 다음 사항을 포함하여 점검)
- 공용 계정을 사용하는지 확인 (운영체제별 확인 방법은 아래 예시 참조)

■ Windows OS
1) 운영자, 관리자별 계정 발급 확인
- 시작> 제어판> 사용자 계정
2) (개선조치 시) 제어시스템 운영자, 관리자별 계정 추가
- 시작> 제어판> 사용자 계정> 추가

■ Unix, Linux OS
1) 운영자, 관리자별 계정 발급 확인
- #cat /etc/passwd
2) (개선조치 시) 제어시스템 운영자, 관리자별 계정 추가
- #useradd 계정명

- 접속기록(Log)을 통해 계정별 지정된 단일 IP에서 접속이 이루어지는지 확인
(2개 이상의 IP주소에서 접속이 있고 해당 업무PC를 서로 다른 인원이 사용한다면 공용계정으로 판단)

※ 개선조치를 위하여 운영인원별 1인 1계정을 발급하되 업무상 반드시 필요한 인원에게만 계정을 부여한다.

조치 시 영향	일부 제어시스템에 따라 접속 오류

제어시스템

C-02 (상)	1. 계정관리 > 1.2 ID/PW, 접속경로, 인증서 등이 하드코딩 되지 않음
취약점 개요	
점검내용	■ 제어시스템을 감시, 제어하는 HMI, PLC 소프트웨어 등을 이용하는 경우 운영자 및 관리자 접속을 위한 계정정보, 접속위치, 기타 인증정보 등이 하드코딩과 같은 방식으로 노출되지 않도록 암호화된 데이터 형태로 보관, 처리하는지 점검
점검목적	■ 접속정보와 같은 중요 정보가 하드코딩되어 있으면 비인가자 및 악성코드에 의해 제어시스템의 접근권한을 획득할 수 있기 때문에, 안전한 데이터 형태로 중요정보를 보관, 처리하도록 하여 제어시스템의 안전한 접속환경을 유지 ■ 또한 이와 같은 취약점이 HMI, PLC 등의 소프트웨어에 존재하는지 관련 제품도입 또는 개발사업 시에 이를 사전 확인하여 안전한 접속환경을 수립
보안위협	■ 접속정보와 같은 중요 정보를 하드코딩하는 경우 비인가자 및 악성코드 등에 의한 제어시스템의 운영 및 관리 권한이 획득될 수 있음 ■ 또한 기본(Default) 패스워드, 추측 가능한 패스워드를 사용하는 경우 비인가자 및 악성코드에 의한 접근권한 획득이 용이할 수 있음 ※ 위협 사례 : 윈도우 시스템에 설치된 스턱스넷(Stuxnet)은 지멘스사의 WinCC/PCS 7 SCADA 제어 소프트웨어인 Step 7을 감염시켜, WinCC의 핵심 라이브러리인 s7otbxdx.dll의 내용을 변경한다. 이후 스턱스넷은 감염된 라이브러리를 통해 WinCC와 지멘스 PLC 사이의 데이터 통신을 몰래 가로채, PLC를 제어하였다. 특히 이 과정에서 스턱스넷은 하드코딩된 기본 SQL 서버의 패스워드를 이용한다. 스턱스넷은 PLC 시스템의 Profibus 메시지 버스 시스템을 감시하는 D8890 블록에 악성코드를 설치하여 특정 조건이 만족되면, 스턱스넷은 주기적으로 모터의 회전수를 1410Hz, 2Hz, 1064Hz로 변경해 모터에 과부하를 일으킨다. 또한 PLC 시스템에 루트킷을 설치하여 자기 자신을 숨기고, 모터의 회전수가 변경되고 있다는 것을 숨긴다.
참고	※ **하드코딩(Hard Coding):** 프로그램 개발 시 접속자 정보를 미리 평문형태로 소스코드 내에 삽입시켜 사용자 및 관리자 계정정보를 소스코드 또는 평문파일을 수정하는 것으로 등록, 변경, 삭제할 수 있도록 하는 개발 방법 ※ **Strings 명령어:** 바이너리 형태의 파일 내용 중 텍스트 형태인 Ascii코드만을 확인할 때 유용하게 활용되는 프로그램으로 유닉스, 리눅스 계열에는 기본 명령어로 존재하고, 윈도우의 경우는 별도 설치해서 이용 가능
점검대상 및 판단기준	
대상	■ 분산네트워크 환경에서 HMI, PLC 등의 S/W를 통해 대상 시스템 및 기기에 접속하기 위해 계정(ID) 접근이 요구되는 제어시스템 ■ HMI 및 DB 서버
판단기준	**양호:** ID/PW, 접속경로, 인증서 등의 접속정보가 하드코딩되어 있지 않은 경우
	취약: ID/PW, 접속경로, 인증서 등의 접속정보가 하드코딩되어 있는 경우
조치방법	하드코딩된 접속정보를 소스코드에서 삭제하고 별도의 암호화된 데이터 또는 DB내에 저장되도록 하는 방식으로 개발 변경(필요시 개발업체에 요청)

제어시스템

C-02 (상)	1. 계정관리 > 1.2 ID/PW, 접속경로, 인증서 등이 하드코딩 되지 않음
점검 및 조치 사례	
Step 1) HMI, PLC, Data Historian 등의 소프트웨어 매뉴얼에서 ID/PW, 접속경로 등의 중요정보를 변경할 수 없게 설정되어 있는지 확인 Step 2) strings 등의 명령어를 이용하여 제어시스템 내의 실행파일 또는 접속정보 파일 내에 하드코딩된 정보 확인 (단, 다음 명령으로 텍스트(Ascii) 정보의 확인이 어려운 경우에도 중요 접속정보의 변경이 불가능하도록 되어 있다면 하드코딩된 것으로 판단하고 Step 3의 내용을 확인) - # strings 실행파일명(예: scada.exe) Step 3) 하드코딩된 접속정보를 제거하고, 별도의 인증절차, 인증정보 보관이 이루어지도록 개발 변경 (필요시 개발업체에 요청) ※ 제어시스템 가용성에 영향이 없는지 충분한 개발 검토 및 영향도 테스트를 거친 후 조치한다. 개발업체의 협조 여부에 따라서 개발 변경이 어려울 수 있다. 개발 변경 가능 여부를 파악하여 취약점 조치 여부를 결정한다.	
조치 시 영향	▪ 하드코딩된 ID/PW, 접속 경로, 인증서 등의 오류에 따른 제어시스템 접속장애 ▪ 하드코딩된 정보가 외부 시스템 과 연계된 경우 해당 연계시스템과의 접속장애

제어시스템

C-03 (상)	1. 계정관리 > 1.3 제어시스템 운영, 관리를 위한 계정의 로그인, 사용 기록 저장
취약점 개요	
점검내용	■ 운영자, 관리자 등의 계정 접근을 허용하는 제어시스템(운영체제, HMI 등)의 계정 접속 로그인 및 사용 기록(Log)이 저장되는지 점검
점검목적	■ 제어시스템(운영체제, HMI 등)의 계정 접속 로그인 및 사용 기록(Log)이 저장되도록 하여 계정 사용에 대한 책임추적성(Accountability)을 높일 수 있도록 함
보안위협	■ 계정 접속 로그인 및 사용내역 등의 접속기록(Log)이 생성되지 않거나 접속기록의 내용이 미흡(예: 사용내역 누락)하여 책임 추적이 어려울 수 있음
참고	※ **접속기록(Log):** 시스템(운영체제) 또는 어플리케이션의 접속기록은 접속자(예: ID), 접속일시, 접속자의 위치(예: IP주소), 사용내역(예: 운영체제의 명령 실행 또는 제어설비에 밸브 조작명령 실행) 등 4가지 유형의 정보를 모두 포함하는 데이터
점검대상 및 판단기준	
대상	■ 분산네트워크 환경에서 HMI, PLC 등의 S/W를 통해 대상 시스템 및 기기에 접속하기 위해 계정(ID) 접근이 요구되는 제어시스템 ■ HMI 및 DB 서버
판단기준	**양호:** 로그온 및 로그오프에 대한 감사(로그)정책이 설정되어 있는 경우 (HMI 등의 경우) 접속기록이 저장(별도 File 또는 DB)되었고 접속기록의 내용이 4가지 유형 모두를 포함하는 경우
	취약: 로그온 및 로그오프에 대한 감사(로그)정책이 설정되어 있지 않은 경우 (HMI 등의 경우) 접속기록이 저장(별도 File 또는 DB)되지 않았거나, 저장되었더라도 접속기록의 내용 중 일부(예: 사용내역)가 생성되지 않은 경우
조치방법	대상 시스템에 로그가 기록되도록 운영체제 설정 적용 (HMI 등의 경우) 사용내역까지를 포함하는 접속기록이 생성 및 저장(별도 File 또는 DB)되도록 개발
점검 및 조치 사례	
■ **HMI, PLC, Data Historian 등의 소프트웨어** Step 1) 접속기록 생성 및 해당 내역 확인 방법을 해당 소프트웨어 매뉴얼(또는 개발업체 문의)을 통해 확인 Step 2) 생성된 접속기록(별도 File 또는 DB)의 내용에 접속자의 접속 ID, 일시, IP주소, 사용내역 등 4가지 유형을 모두 포함하는지 확인 ■ **Windows OS** Step 1) 로깅설정 및 로그파일의 로깅정보 확인 - 제어판> 관리도구> 로컬보안정책> 보안설정> 로컬 정책> 감사 정책	

제어시스템

C-03 (상)	1. 계정관리 > 1.3 제어시스템 운영, 관리를 위한 계정의 로그인, 사용 기록 저장

- 계정 로그온 이벤트 감사> “성공”, “실패” 설정
- 권한 사용 감사> "성공", "실패" 설정

■ UNIX, Linux OS

Step 1) #cat /etc/syslog.conf 파일에서 로그 설정 확인

- #cat /var/adm/loginlog, authlog, sulog의 파일을 열어 로깅 정보 확인

Step 2) #vi /etc/syslog.conf 파일 설정 변경

* Unix 계열 운영체제의 생성 로그 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 발생한 메시지
syslog : syslog 프로그램 유형이 발생한 메시지
user : 사용자 프로세스
uucp : 시스템이 발생한 메시지
local0 : 여분으로 남겨둔 유형

※ 개발업체의 협조 여부에 따라서 개발 변경이 어려울 수 있다. 개발 변경 가능 여부를 파악하여 취약점 조치 여부를 결정한다.

조치 시 영향	일반적인 경우 영향 없음

제어시스템

C-04 (상)	2. 패치관리 > 2.1 제어시스템에 대한 최신 업데이트, 보안패치를 안전하게 적용하기 위한 테스트 등의 절차 수립
취약점 개요	
점검내용	■ 제어시스템을 구성하는 소프트웨어, 시스템(OS), 장비 등에 대한 최신 업데이트, 보안패치를 적용하여 알려진 취약점이 존재하지 않도록 하는지 점검
점검목적	■ 최신 보안취약점의 주기적인 확인, 조치 전 영향성 검토, 취약점 조치 등의 체계적인 업무절차를 수립하고 이를 이행함으로써 알려진 취약점으로 인한 제어시스템의 보안위협을 줄이고자 함
보안위협	■ 알려진 취약점이 조치되지 못한 제어시스템을 대상으로 해당 취약점을 악용한 비인가자의 침해 시도 또는 자동화된 악성코드의 감염 우려가 있음 ※ 위협 사례 : 스턱스넷(Stuxnet)의 경우 다음과 같은 취약점을 이용하고 있으므로 위협 대상 취약점은 이미 조치되어 있어야 한다.  CVE-2008-4250 (MS08-067) – 윈도우 서버 서비스 NetPathCanonicalize() 취약점: http://www.microsoft.com/korea/technet/security/bulletin/ms08-067.mspx CVE-2010-2568 (MS10-046) – 윈도우 쉘 LNK 취약점: http://www.microsoft.com/korea/technet/security/bulletin/ms10-046.mspx CVE-2010-2729 (MS10-061) – 윈도우 프린트 스풀러 서비스 취약점: http://www.microsoft.com/korea/technet/security/bulletin/ms10-061.mspx CVE-2010-2743 (MS10-073) – 윈도우 Win32K 키보드 레이아웃 취약점: http://www.microsoft.com/korea/technet/security/bulletin/ms10-073.mspx CVE-2010-2772 – 지멘스 SIMATIC WinCC 기본 데스워드 취약점 http://support.automation.siemens.com/WW/view/en/43876783 현재까지 아직 패치되지 않은 윈도우 작업 스케줄러 취약점
참고	※ **ICS CERT:** 美 국토안보부(DHS)의 산업제어시스템(Industrial Control System) 사이버비상대응기관(Cyber Emergency Response Team)으로 전 세계 각종 ICS 보안동향, 최신 취약점 정보, 사건사례, 정기 리포트 등을 공개하고 발생하는 사건을 조사, 대응하는 기관 (홈페이지 https://ics-cert.us-cert.gov/)
점검대상 및 판단기준	
대상	■ HMI(Human Machine Interface), PLC(Programmable Logic Controller), Data Historian 등의 소프트웨어 및 해당 소프트웨어가 구동하는 시스템(운영체제) ■ 전체 제어시스템을 구성하는데 이용되는 각종 장비(예: 라우터, 모뎀 등)
판단기준	**양호:** 제어시스템 업데이트 및 보안패치 적용 절차가 수립되어 있고 알려진 취약점이 조치된 경우
	취약: 제어시스템 업데이트 및 보안패치 적용 절차가 수립되어 있지 않거나, 알려진 취약점이 조치되지 않은 경우
조치방법	제어시스템에 대한 안전한 업데이트 및 보안패치 절차 수립 (알려진 취약점이 있는 경우)취약점의 조치 테스트 후 영향성 검토 및 승인절차를 통한 해당 취약점 조치(업그레이드 또는 보안패치)

제어시스템

C-04 (상)	2. 패치관리 > 2.1 제어시스템에 대한 최신 업데이트, 보안패치를 안전하게 적용하기 위한 테스트 등의 절차 수립

점검 및 조치 사례

Step 1) 제어시스템의 알려진 취약점을 공개하는 기관(예: https://ics-cert.us-cert.gov/) 또는 제어시스템을 구성하는 소프트웨어, 시스템, 장비 등을 납품하는 업체를 통해 최신 업데이트, 보안패치 정보를 입수하고 있는지 확인

- ICS CERT 홈페이지 > Information Products > Alerts & Advisories

[그림] 2015년에 공개된 제어시스템 취약점 정보

Step 2) 확인된 제어시스템과 취약점이 있는 경우, 해당 소프트웨어, 시스템(OS), 장비 등에 대한 최신 업데이트 및 보안패치가 적용하기 전에 제어시스템의 장애 등을 우려하여 시험 적용, 영향성 평가, 적용 후 문제발생 시 롤백 방안, 최종 적용 승인 등의 절차를 거치도록 하는지 확인

Step 3) 해당 소프트웨어, 시스템(OS), 장비 등에 대한 최신 업데이트 및 보안패치가 적용되는지 확인
(예시) LOYTEC Router 중 특정 제품은 백업파일이 생성될 때 해시된 사용자 패스워드까지 저장되고 있어 백업파일을 획득하는 경우 장비에 대한 사용자 접근 패스워드를 알아낼 수 있는 위험이 존재하나, 펌웨어(Firmware)를 업그레이드하면 해당 취약점은 조치 가능
- 출처: ICS CERT 홈페이지에 공개된 취약점(ICSA-15-342-02)

※ HMI, PLC 등의 소프트웨어는 특정 운영체제 버전에서만 동작하는 경우도 있기 때문에 운영체제 자체의 업그레이드, 보안패치가 불가능할 수 있다. 이 경우는 제어시스템을 구성하는 소프트웨어, 장비 등에 대한 전문기관 및 공급업체를 통해 알려진 취약점만을 고려하여 업그레이드 및 보안패치를 적용할 수 있도록 한다.
※ 제어시스템 전체 또는 구성 요소간의 동작 장애가 우려되는 경우는 업그레이드 및 보안패치에 대한 영향을 시험하는 과정을 통해 그 적용여부를 결정하되, 이 경우도 시험, 보완통제 방안, 보고 등의 절차는 거치도록 한다.

조치 시 영향	제어시스템 전체 또는 구성 요소간의 동작 장애

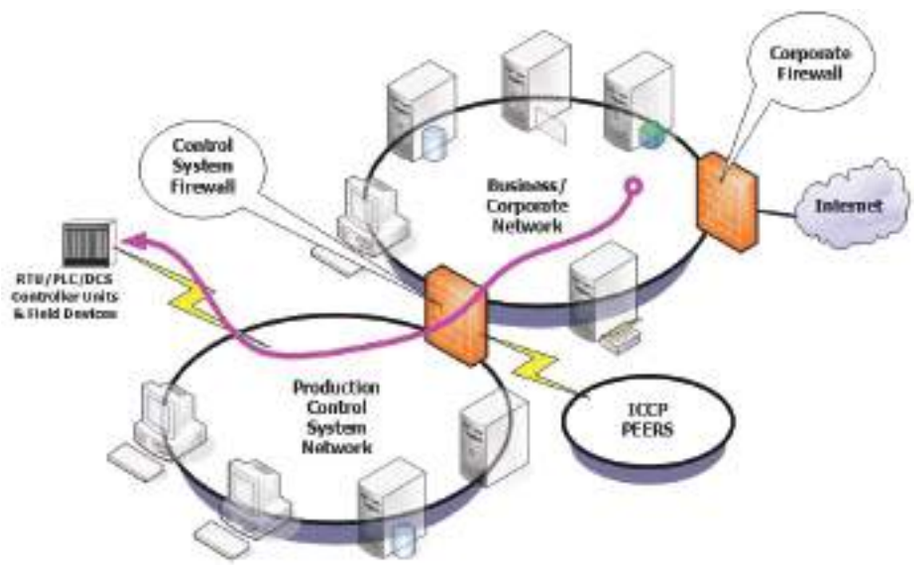
제어시스템

C-05 (상)	3. 접근통제 > 3.1 제어시스템 운영자의 운영 권한은 제한된 범위 및 명령으로 제한
취약점 개요	
점검내용	■ 제어시스템을 감시, 제어하고 주요 기능을 수행하는 HMI, PLC, Data Historian 등의 운영자에게 최소 권한(제어범위, 제어명령 등) 이외 불필요한 권한(예: 모니터링 인원이 특정 설비를 가동, 정지 가능)이 부여되어 있지 않은지 점검
점검목적	■ HMI 등의 감시, 제어 권한을 업무상 필요한 최소 권한만을 갖도록 하여 권한의 오·남용을 예방하고자 함
보안위협	■ HMI 등의 감시, 제어 권한을 운영 업무에 따라 차등부여하지 않아 과도한 권한 부여가 이루어지는 경우 내부 권한자(직원 또는 협력사 직원)에 의한 오작동(Human Error) 또는 오·남용을 일으킬 수 있음 ※ 위협 시나리오 : HMI 등의 소프트웨어 취약점 또는 운영자 부주의에 의해 악성코드가 감염되는 경우 해당 시스템의 운영자 권한을 악용할 수 있다. 이 경우 운영자가 모든 설비를 대상으로 가동 정지를 시킬 수 있는 권한이 있다면 해당 권한을 악성코드가 이용할 수 있게 되는 것이다.
참고	※ 제어시스템의 운영권한 차등화 부여 요령 제어시스템의 운영권한은 HMI 등의 소프트웨어에 따라 다를 수 있으나 일반적으로 제어범위와 제어명령 수준으로 차등 부여되도록 하는 것이 좋다. 예를 들어, 운영자 계정을 보유한 모든 인원이 전체 설비를 대상으로 운전 및 정지를 할 수 있는 권한이 있다면 이는 모든 운영인력에게 제어시스템 전체에 대한 모든 권한을 부여한 것과 같다. 이를 위하여는 운영 직무를 수행하는 부서, 인원별 필요한 직무를 파악하고 각 인원별로 부여된 제어시스템 운영계정별 제어범위, 제어명령이 차등 부여되도록 권한 관리(예: 운영권한 정의표(부서, 인원, 범위, 명령 등을 포함) 작성 및 관리)가 선행되어야 한다.
점검대상 및 판단기준	
대상	■ 분산네트워크 환경에서 HMI, PLC 등의 S/W를 통해 대상 시스템 및 기기에 접속하기 위해 계정(ID) 접근이 요구되는 제어시스템
판단기준	**양호:** HMI 등의 운영 계정별 제어범위 및 제어명령 실행권한이 차등 부여되어 있는 등 필요한 최소 권한으로 제한하는 경우
	취약: HMI 등의 운영 계정별 제어범위 및 제어명령 실행권한이 업무상 필요한 권한을 초과하는 경우
조치방법	HMI 등의 운영계정별 업무상 필요한 제어범위 및 제어명령의 차등 부여

제어시스템

C-05 (상)	3. 접근통제 > 3.1 제어시스템 운영자의 운영 권한은 제한된 범위 및 명령으로 제한
점검 및 조치 사례	
Step 1) HMI 등을 통해 운영업무를 수행하는 부서 및 인원별 가능한 제어범위와 제어명령이 사전 정의(예: 지침, 절차 등)되어 있는지 확인 (만약, 정의되어 있지 않다면 명문화 하여 승인을 받도록 함) Step 2) HMI 등의 임의 운영계정 중 하나로 로그인하여 담당 인원에게 부여된 직무에 맞게 제어범위 및 제어명령을 수행하는 등 적절한 권한 부여가 이루어지는지 확인 (만약, 직무 범위를 초과한 제어범위(예: 전체 설비), 제어명령(예: 가동정지) 실행이 가능하다면 제어권한을 최소화하도록 함) ※ 점검을 위하여 제어를 수행하거나, 권한 이상의 제어명령을 실제로 수행할 경우 심각한 결과를 초래할 수 있으므로, 그 가능성을 중심으로 점검한다.	
조치 시 영향	제어 권한 범위 등 최소권한 분석이 잘못 이루어지는 경우 제어시스템 운영에 제약이 초래됨

제어시스템

C-06 (상)	3. 접근통제 > 3.2 제어시스템은 업무망, 인터넷 망과 물리적으로 분리
취약점 개요	
점검내용	■ 제어시스템을 감시, 통제하는 네트워크 구성이 제어망(Production Control System Network), 업무망(Business Network), 인터넷망 등으로 물리적 분리가 이루어지고 있는지 점검
점검목적	■ 제어시스템에 인터넷을 통한 각종 침해위협(예: 악성코드 등)으로부터 보호하기 위함
보안위협	■ 업무망과 제어망이 분리된 경우에도 업무망 PC에서 제어망에 위치한 설비를 모니터링할 수 있는 경우 해당 PC의 인터넷을 차단하지 않아 스턱스넷과 같은 악성코드에 감염되고 제어망에 위치한 설비의 운영 정보 수집은 물론, 취약점을 악용한 제어시스템 마비를 초래할 수 있음 ※ 위협 사례 : 쇼단(Shodan) 연구원에 따르면 미국은 5만7천개라는 전 세계에서 가장 많은 수의 산업 통제 시스템을 가지고 있으며 이들은 모두 인터넷에 연결되어 있다고 밝혔다. 또한, 2014년 12월 독일 언론에 따르면, 독일의 한 제철소 용광로의 제어시스템에 대한 해킹공격으로 제어시스템이 파괴되면서 관련 산업 전체에 큰 피해를 주었다. 당시 해커들은 보안 의식이 낮은 용광로 운영 직원의 인터넷 Email을 이용해 로그인 계정을 탈취한 뒤 제어시스템을 장악한 것으로 알려져 있다.
참고	※ 제어시스템의 네트워크 구성 요령 제어시스템을 운영하는 조직은 제어망(Production Control System Network)과 업무망(Business Network)을 물리적으로 분리하고 네트워크 경계에는 방화벽(Control System Firewall)을 위치시켜 접근통제를 하여야 한다. 이 경우 업무망 대역에도 제어설비에 대한 접근이 요구되는 업무PC가 있다면 업무망 대역 내에서도 인터넷이 차단된 업무망과 인터넷 접속을 허용하는 업무망으로 분리 구성해야 한다.  [그림 출처] 美 ICS-CERT (https://ics-cert.us-cert.gov)

제어시스템

C-06 (상)	3. 접근통제 > 3.2 제어시스템은 업무망, 인터넷 망과 물리적으로 분리
점검대상 및 판단기준	
대상	■ 제어시스템을 구성하는 네트워크 전체
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
점검 및 조치 사례	

Step 1) 제어시스템 네트워크 구성도를 검토하여 제어망, 업무망, 인터넷망 등이 모두 분리되어 접근이 차단되도록 구성되었는지 확인

[그림] 원전제어망의 분리, 운영 사례

Step 2) 네트워크 분리는 물리적 분리 방식이며, 각 네트워크 간의 접근통제는 방화벽을 통해 이루어지는지 확인

※ 제어시스템 운영 시에 업무망, 인터넷망과의 연계가 불필요한 경우는 물리적으로 분리하여 구성하되, 국가정보원에서 배포한 "전자제어시스템 보안가이드라인" 3장 2절 "제어 네트워크의 물리적 망분리" 내용을 참조하고, 제어시스템 운영 시에 업무망에서의 인터넷 연결이 불가피한 경우는 해당 가이드라인의 3장 3절 "안전한 제어 네트워크 연동 기법"을 참조한다. 단, 이 경우에도 제어망에서의 인터넷 연결은 원칙적으로 금지해야 하고, 업무망에서의 인터넷 이용에 대한 안전대책을 마련해야 한다.

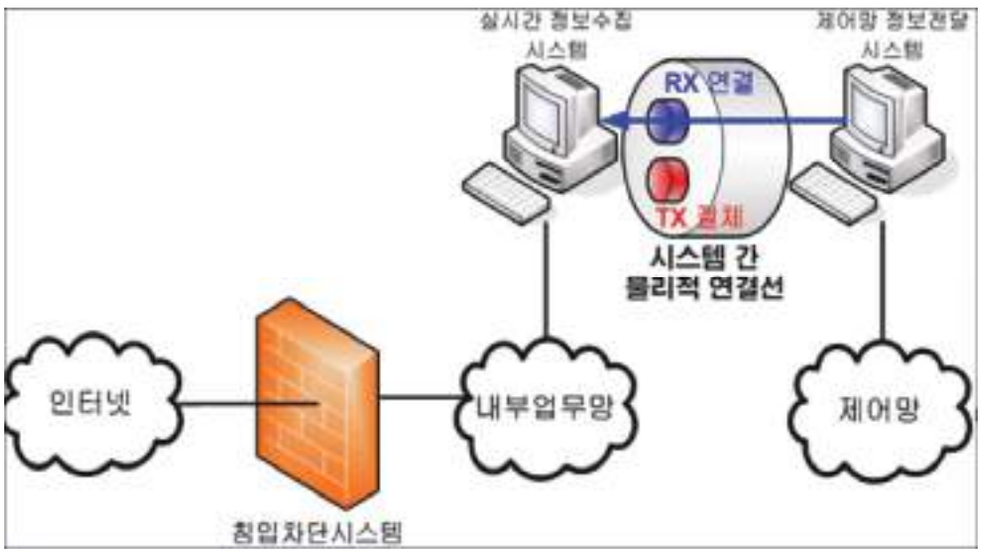
조치 시 영향	외부 시스템 또는 설비와 인터넷을 통한 운영 정보 연계가 이루어지는 경우 해당 시스템 또는 설비와 정보 송수신 불가

제어시스템

C-07 (상)	3. 접근통제 > 3.3 제어 네트워크 외부와 자료연계시 물리적 일방향 환경을 구축하여 제어 네트워크로의 침입을 근본적으로 차단
취약점 개요	
점검내용	■ 제어 네트워크와 외부 자료 연계가 필요한 경우 제어망으로부터 업무망으로의 데이터 전송이 일방향으로 이루어지는지 점검
점검목적	■ 업무망에 대한 침해 위협으로 인해 제어망에 직접적인 피해(예: 운전 조작 등)가 발생하지 않도록 하기 위함
보안위협	■ 제어망과 업무망 간 운전 정보를 양방향 전송하게 되는 경우 업무망의 운영자 PC를 통한 내부자 부주의 또는 오·남용(예: 운전 조작 등) 우려가 있고, 악성코드가 유입되는 경우 제어망에 위치한 시스템까지 감염될 수 있음
참고	※ 본 점검항목은 제어망에 위치한 설비 또는 시스템 등의 정보를 외부(내부 업무망 또는 외부 업무망)로 전송하는 경우 양방향 전송(예: 제어설비의 운전조작)이 불가피한 경우를 제외하고는 일방향 전송을 요구하는 부분이다.
점검대상 및 판단기준	
대상	■ 제어망으로부터 내부 업무망으로 정보 연계가 이루어지는 시스템 ■ 제어망으로부터 외부 업무망으로 제어망의 운전정보 등을 전송하는 설비 및 시스템
판단기준	**양호:** 제어망의 운전정보를 업무망으로 일방향 전송하는 경우 (반드시 필요한 경우는 예외)
	취약: (단순모니터링 업무와 같은 불필요한 업무환경임에도) 제어망의 운전정보를 업무망으로 양방향 전송이 이루어지는 경우
조치방법	내·외부의 통신선로에 대한 물리적 일방향 전송이 이루어지도록 조치하거나, 방화벽 등을 통한 일방향 접근통제 정책(Rule)을 적용
점검 및 조치 사례	
Step 1) 제어시스템 네트워크 구성도를 검토하여 제어망으로부터 내부 업무망 또는 외부 업무망과의 연계지점이 있는지 확인 Step 2) 해당 연계 지점에서의 정보 전송이 다음 각 호의 방법과 같은 일방향으로 이루어지는지 확인 (만약 양방향 전송이 이루어지더라도 반드시 필요한 경우이면 예외) 1. 송·수신 회선 한쪽을 물리적으로 단절 (예: LAN, 시리얼 라인의 업무망에서 제어망으로의 TX-RX 라인을 절체)	

제어시스템

C-07 (상)	3. 접근통제 > 3.3 제어 네트워크 외부와 자료연계시 물리적 일방향 환경을 구축하여 제어 네트워크로의 침입을 근본적으로 차단

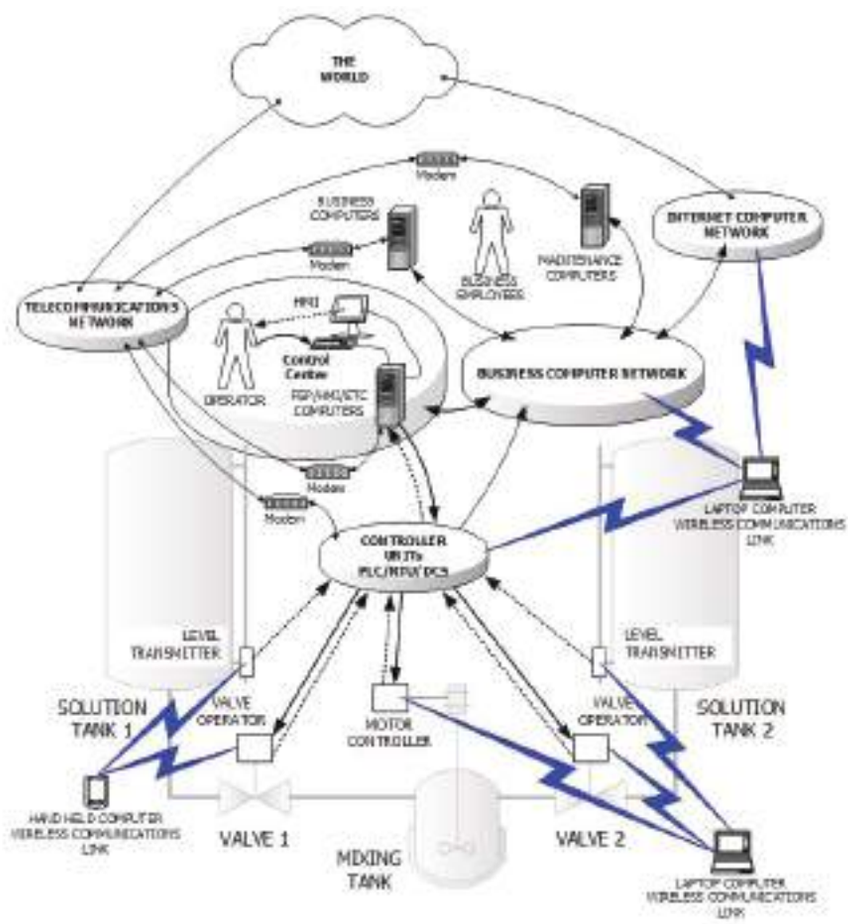


2. 데이터 송신용 장비, 수신용 장비를 한 쌍으로 하여 일방향으로만 정보 전달이 가능하도록 개발된 전용장비 사용
3. 제어망 송신자 주소에서 내·외부 업무망 수신자 주소 및 포트에 대해서만 제한적인 out-bound 정책 허용(in-bound 정책 적용은 금지)

조치 시 영향	긴급한 경우 업무망에서의 운전조작이 어려울 수 있음

제어시스템

C-08 (상)	3. 접근제어 > 3.4 제어 네트워크에 무선인터넷, 테더링, 외부망등 연결 등의 외부망 연결을 제한하고 점검
취약점 개요	
점검내용	■ 제어망, 업무망, 인터넷망 등의 물리적 망분리 이외에도 이를 우회할 수 있는 무선 인터넷, 테더링 등을 이용하지 못하도록 하는 통제가 이루어지는지 점검
점검목적	■ 내부 보안정책을 우회할 수 있는 비인가 무선AP 설치, 스마트폰의 테더링 이용 등과 같은 외부해킹 및 악성코드 감염 경로를 차단하기 위함
보안위협	■ 제어망 또는 업무망 등에 비인가 무선AP 설치, 스마트폰의 테더링 이용 등과 같은 외부로의 인터넷 연결 점검이 생기는 경우는 물리적 망분리를 우회할 수 있고 이를 통해 악성코드가 유입되는 경우 제어망에 위치한 시스템까지 감염될 수 있음
참고	※ 제어시스템의 보안정책 우회 통제 방안 제어시스템을 구성하는 환경에서 내부망 내에 위치한 비인가 무선AP(또는 외부로부터 수신되는 무선AP), 스마트폰의 테더링 등을 이용한 외부 인터넷 연결이 이루어질 수 있다. 이를 차단하기 위해서는 비인가 기기의 반출입 통제, 무선랜카드 사용통제 등의 물리적 통제를 함께 고려하는 것이 좋다.



[그림 출처] 美 ICS-CERT (https://ics-cert.us-cert.gov)

제어시스템

C-08 (상)	3. 접근제어 > 3.4 제어 네트워크에 무선인터넷, 테더링, 외부망등 연결 등의 외부망 연결을 제한하고 점검
점검대상 및 판단기준	
대상	■ 제어시스템을 구성하는 네트워크 전체
판단기준	**양호:** 제어 시설에 비인가 장비에 대한 반입이 불가능하며, 제어망 및 내부 업무망의 유·무선 인터넷 접속차단이 이루어지는 경우
	취약: 제어 시설에 비인가 장비에 대한 반입 통제가 이루어지지 않거나, 제어망 및 내부 업무망에서 유·무선 인터넷 접속이 가능한 경우 (단, 유선 인터넷 접속이 가능한 경우에도 C-06(상), C-07(상)의 점검을 통해 "양호"에 해당하면 본 점검항목도 "양호"로 판단하고 무선 인터넷 접속이 가능한 경우는 취약으로 판단)
조치방법	외부 연계 접점 차단(외부 연계일 경우 물리적 일방향 시스템 적용)

점검 및 조치 사례

Step 1) 제어망 및 업무망에 외부 노트북, 태블릿PC, 스마트폰 등이 반입될 때 이를 통제, 보안 조치하는 절차가 있는지 확인하고, 해당 절차가 없다면 기반시설에 대한 관리·물리 점검 항목 A-18(상), A-19(상), A-21(상), A-22(상)을 참조하여 개선 조치

Step 2) 제어망 및 업무망의 서버, PC에 대해 인터넷 접속 사실이 있는지 다음 각 호의 방법으로 확인하고, 접속이 가능하다면 C-06(상), C-07(상) 등의 조치 방법을 참고하여 개선 조치

1. 윈도우즈 환경인 경우, 웹브라우저에서 인터넷 사이트 연결이력이 있는지 점검
   - 윈도우의 Registry값을 확인하는 방법으로서, CMS창에 다음 명령어를 입력

```
reg query "HKCU₩Software₩Microsoft₩Internet Explorer₩TypedURLs"
```

   - 상기 명령어를 입력 시 웹브라우저 창에 입력한 값이 저장되는 레지스트리 값을 확인 (단, 방문한 웹 사이트 목록 삭제 시는 확인 불가)

```
url1    REG_SZ    http://www.kisa.or.kr/
```

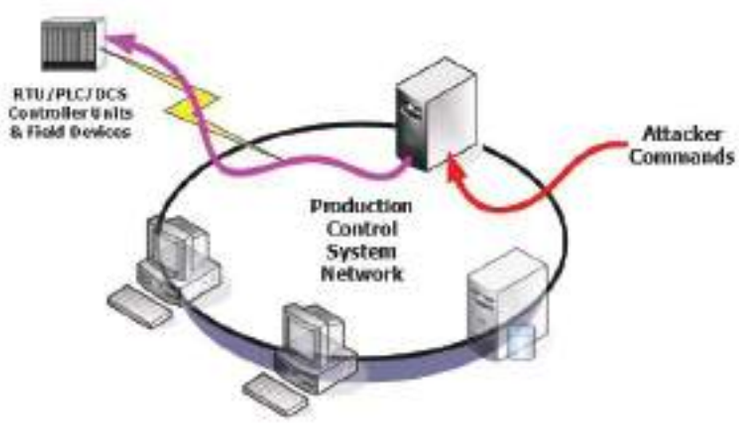
   - Cookie 파일 확인하는 방법으로서, Cookie 파일 안에 내용에 URL을 확인하여 인터넷 사용 여부를 판단 (단, 쿠키 및 웹사이트 데이터 삭제 시는 확인 불가)

```
1) CMD 창에 reg query "HKEY_CURRENT_USER₩Software₩Microsoft₩Windows₩
   CurrentVersion₩Explorer₩Shell Folders" | findstr "Cookies" 입력하여 쿠키 저
   장 위치를 파악
2) 쿠키가 저장 된 폴더에 들어가 쿠키 파일 내용에 포함된 URL 확인
```

2. 망분리가 이루어지지 않고 외부 인터넷 서버로의 패킷 전달이 가능한지 점검
   #ping 외부 IP(예: 공개DNS IP주소, 포털사이트의 IP주소 등)

C-08 (상)	3. 접근제어 > 3.4 제어 네트워크에 무선인터넷, 테더링, 외부망등 연결 등의 외부망 연결을 제한하고 점검
Step 3) 노트북 등을 이용해 제어 시설을 이동하면서 근거리에서 수신되는 내부 무선AP가 있는지 점검하고, 비인가 무선AP가 있으면 제거 1. (만약, 내부가 아닌 외부로부터 수신되는 무선AP가 감지되면 해당 구역의 시스템 무선랜 카드를 제거) 2. (장비가 있는 경우) 무선AP, 무선네트워크 전파 스캐너를 사용하여 점검 Step 4) 노트북 등을 이용해 제어 시설을 이동하면서 근거리에서 수신되는 외부 WiFi 접속 가능성과 스마트폰의 테더링을 통한 접속 가능성이 있는지 점검하고, 가능하다면 다음 각 호의 방법을 적용하여 조치 1. 해당 구역 내 서버 및 업무PC의 무선랜카드를 물리적으로 제거하거나 기능 정지 2. (장비가 있는 경우) 무선 방화벽을 통한 무선망 이용 차단 ※ 불가피하게 무선AP를 사용하여야만 내부망(제어망, 업무망) 내의 특정 설비 또는 시스템간 정보 연계가 이루어지는 경우가 있다면 해당 무선AP의 보안설정을 적용하고 물리적으로 비인가자의 접근을 차단하는 등의 보호대책을 적용해야 한다. 이에 대한 상세한 내용은 기반시설에 대한 관리·물리 점검항목 A-21(상), A-22(상)을 참조한다.	
조치 시 영향	내부망(제어망 및 업무망) 내에서 인가된 무선AP를 통해 정보 연계가 이루어지는 경우 무선 AP 제거 또는 접속 제한조치에 따른 연계 시스템의 기능 장애

제어시스템

C-09 (상)	3. 접근제어 > 3.5 제어 네트워크에 비인가된 시스템에 대한 연결 및 접속 차단
취약점 개요	
점검내용	■ 내부망(제어망 및 업무망)에 비인가 서버 및 노트북 등을 연결하는 경우 내부망에 접속할 수 없도록 사전 승인된 MAC 주소에 대하여만 IP주소가 부여되도록 하는지 점검
점검목적	■ 내부망에 출입자가 비인가 서버 및 노트북 등을 반입하여 임의로 내부망에 연결할 수 없도록 하기 위함
보안위협	■ 악성코드가 감염된 서버 및 노트북 등을 악의적인 목적으로 반입하여 사회공학적인 방법으로 내부 업무망에 연결하고 손쉽게 IP주소를 획득(DHCP 또는 네트워크 대역의 임의 IP주소 연결)할 수 있음 ■ 이를 통해 해당 시스템을 경유하여 업무망 또는 제어망의 취약한 시스템(예: 특정 버전의 OPC 시스템)을 위협하고 제어설비의 권한을 획득할 수 있음 ※ 위협 시나리오 : 美 ICS CERT에서 공개한 취약점 정보에 따르면 “Open Automation Software OPC Systems NET DLL Hijacking Vulnerability”은 특정 버전(OPC Systems.NET Version 8.00.0023과 이전 버전)을 사용하는 HMI 등의 소프트웨어의 사용자 권한을 획득할 수 있는 취약점으로 알려져 있다. 즉 해당 취약점을 공격하는 악성코드를 사회공학적인 방법(예: HMI 운영자에게 내부망의 이메일로 악성코드 전파)으로 감염시킬 수 있는 것이다.  [그림 출처] 美 ICS-CERT (https://ics-cert.us-cert.gov)
참고	※ 제어시스템의 비인가 기기 연결 통제 방안 제어시스템을 구성하는 환경에서 내부망 내에 비인가 서버 및 노트북 등이 반입되고 이를 손쉽게 내부망에 연결하는 것을 차단하기 위해서는 비인가 기기의 반출입 통제, 기기의 네트워크 연결통제 등을 함께 고려하는 것이 좋다.

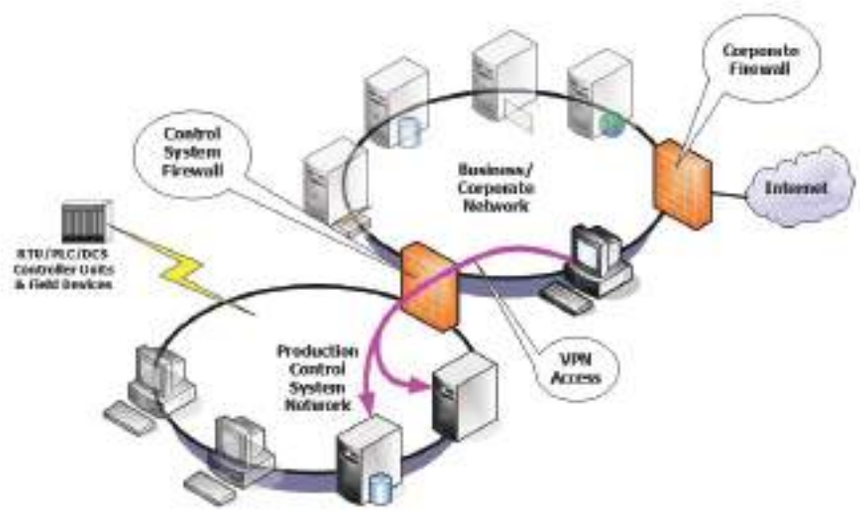
제어시스템

C-09 (상)	3. 접근제어 > 3.5 제어 네트워크에 비인가된 시스템에 대한 연결 및 접속 차단
점검대상 및 판단기준	
대상	■ 제어시스템을 구성하는 네트워크 전체
판단기준	**양호:** 내부망(제어망 및 업무망)에 대한 사전 허가된 시스템 식별과 IP주소 부여 정책이 이루어지는 경우
	취약: 내부망(제어망 및 업무망)에 대한 사전 허가된 시스템 식별과 IP주소 부여 정책이 없이 임의의 기기와 IP주소 부여가 가능한 경우
조치방법	내부망(제어망 및 업무망)에 시스템을 연결하는 경우 MAC 식별 및 IP 부여 등의 절차에 따른 접근통제 조치
점검 및 조치 사례	

Step 1) 제어망 및 업무망 등의 내부망에 비인가 시스템이 임의로 연결되어 IP주소를 부여받을 수 없도록 다음 각 호의 방법과 같은 조치가 적용되는지 확인

1. MAC주소를 식별하고 내부 신청절차에 따라 허가된 IP주소를 부여 (관리적 통제)
2. NAC(Network Access Control) 등의 시스템을 적용하여 사전 정의 및 구성이 허가되지 않은 임의의 시스템 연결을 차단 (기술적 통제)

Step 2) MAC주소가 식별되어 IP주소가 부여된 업무망PC에서 제어망의 시스템 접근이 필요한 경우 (예: IT엔지니어가 제어망의 시스템 유지보수)는 사전 허가된 제어망 시스템에 대하여만 접근할 수 있도록 하는 보안대책(예: 방화벽을 경유한 VPN 접속)을 적용



[그림 출처] 美 ICS-CERT (https://ics-cert.us-cert.gov)

조치 시 영향	업무망PC에서 업무상 접근이 요구되는 제어망 시스템으로의 접근을 원천 차단하는 경우 시스템 유지보수 등의 업무 불가

제어시스템

C-10 (상)	4. 보안관리 > 4.1 제어시스템 구성도, 운용 매뉴얼, 비상조치 절차서 등을 작성하고 최신으로 관리
취약점 개요	
점검내용	■ 제어시스템을 안정적으로 운영, 관리하기 위해 제어시스템 현황(목록), 네트워크 구성도, 운용 매뉴얼, 비상상황 발생 시 업무절차서 등이 수립하고 현재 시스템 구성(HMI, PLC, Data Historian, RTU 등)에 맞도록 개정(현황화)하고 있는지 점검
점검목적	■ 제어시스템의 장애, 사이버 위협 등으로부터 신속한 원인 규명, 복구 등이 이루어질 수 있도록 하여 제어시스템의 안정적인 관리, 운영을 하기 위함
보안위협	■ 제어시스템 현황, 네트워크 구성 등이 현행화되지 않아 장애 및 사이버 위협 발생 시 원인 규명에 어려울 수 있고, 운영 매뉴얼 및 비상 시 업무절차서가 수립되지 않거나 최신화되어 있지 않아 신속한 복구가 어려울 수 있음
참고	※ 본 점검항목은 관련 문서의 수립과 개정(현행화) 여부를 확인하는 항목이며, 각 문서의 개정은 정기적(연 1회)으로 할 수도 있으나 제어시스템의 중요도에 따라 개정이 필요한 시점에서 즉시 개정되도록 하는 것이 바람직하다. 즉 제어시스템의 구성이 변경되었거나 관계법규 및 정책의 변경, 최신 보안위협 등에 따라 개정이 시급하다면 해당 시점에서 개정 작업을 해야 한다.
점검대상 및 판단기준	
대상	■ 제어시스템 전체 및 관련 운영 조직
판단기준	**양호:** 제어시스템 현황, 네트워크 구성도, 운영 매뉴얼, 비상조치 절차서가 수립되었고, 해당 자료가 모두 최신으로 개정된 경우
	취약: 제어시스템 현황, 네트워크 구성도, 운영 매뉴얼, 비상조치 절차서의 전부 또는 일부가 수립되지 않았거나, 수립된 자료의 전부 또는 일부가 현행화(개정)되어 있지 않은 경우
조치방법	제어시스템 현황(목록), 네트워크 구성도, 운영 매뉴얼, 비상조치 절차서를 모두 수립(문서화)하고 정기적 또는 주기적인 개정(현행화) 적용
점검 및 조치 사례	
Step 1) 제어시스템 현황(목록), 네트워크 구성도, (HMI, PLC 등의)운영 매뉴얼, 비상조치 절차서가 수립되어 있는지 확인하고 미수립되어 있다면 해당 자료를 수립하도록 조치 Step 2) Step 1에 따라 수립된 자료가 제어시스템 변경 등에 따라 현행화(개정)되어 있는지 다음 각 호의 사항을 고려한 점검을 수행하고 미흡한 경우 현행화하도록 조치 1. 제어 설비가 위치한 곳을 실사하여 HMI, PLC 등의 제어시스템이 현재 수립된 현황(목록)과 일치하는지 확인 (제어시스템 네트워크 구성도를 함께 확인) 2. HMI, PLC 등을 포함한 제어시스템의 운영매뉴얼 보유 여부(해당 제품의 버전에 따른 운영 매뉴얼 여부 포함) 3. 비상상황 발생 시 업무절차서 보유	
조치 시 영향	일반적인 경우 영향 없음

제어시스템

C-11 (상)	4. 보안관리 > 4.2 제어시스템에서의 USB 사용을 금지하고, 사용시 USB 등의 이동형 저장매체 사용 통제
취약점 개요	
점검내용	■ 내부망(제어망 및 업무망)에 USB 등의 이동형 저장매체의 사용을 통제(예: 사용시 보안대책 적용 또는 원천 차단)하는지 점검
점검목적	■ 제어시스템에 USB 등의 이동형 저장매체를 원천 차단하거나 안전한 저장매체만 연결하도록 하는 등의 통제 정책을 적용하여 악성코드 감염 등의 위협을 차단하기 위함
보안위협	■ 제어시스템에 안전하지 않은 USB 등의 이동형 저장매체 연결 시 악성코드 감염이 이루어지고 이를 통해 제어시스템의 장애 또는 정지 등의 피해가 발생할 수 있음 ※ 위협 사례 : 스턱스넷(Stuxnet)은 이동 저장매체를 통한 전파 시에 autorun.inf 파일을 이용하기도 하지만, 자동실행 기능이 비활성화되어 있는 PC 환경에서도 감염 및 전파를 하기 위해 MS10-046, CVE-2010-2568 등의 취약점(LNK 파일에 대한 윈도우 쉘 아이콘 처리자 취약점)을 이용했다. 이 취약점으로 인해 윈도우 익스플로러는 이동 저장매체 상에 있는 DLL 파일을 실행하게 된다. 즉, 스턱스넷(Stuxnet)에 감염된 USB를 아직 감염되지 않은 PC에 연결하게 되면 USB 내의 파일과 디렉토리를 검색하기 위해 브라우저 창이 열리고, 그때 해당 PC는 감염된다. 아래 그림은 스턱스넷(Stuxnet)에 감염된 이동형 저장매체(USB메모리) 내의 디렉토리 목록이다. 05/20/2010 10:35 AM 4,171 Copy of Copy of Copy of Copy of Shortcut to.lnk 05/20/2010 10:35 AM 4,171 Copy of Copy of Copy of Shortcut to.lnk 05/20/2010 10:35 AM 4,171 Copy of Copy of Shortcut to.lnk 05/20/2010 10:35 AM 4,171 Copy of Shortcut to.lnk 05/20/2010 10:35 AM 517,632 ~WTR4132.tmp 05/20/2010 10:35 AM 25,720 ~WTR4141.tmp
참고	※ 이동형 저장매체 통제 방안 USB 등의 이동형 저장매체는 시스템에 연결이 불가하도록 조치하는 것이 원칙이나 사용이 불가피한 경우는 사전 인가된 저장매체를 준비하고 해당 저장매체의 사용 승인절차와 안전조치(예: 사용 전, 사용 후 악성코드 감염여부 검사)가 적용하도록 하는 통제절차까지 함께 고려한다.
점검대상 및 판단기준	
대상	■ 제어시스템을 구성하는 서버, PC 등, 이동형 저장매체가 연결 가능한 시스템
판단기준	**양호:** 이동형 저장 매체 사용을 원천차단하고, 불가피한 경우 사용통제 절차가 수립되어 해당 절차에 따르는 경우
	취약: 이동형 저장 매체 사용에 대한 원천차단이 이루어지지 않거나, 사용통제 절차 없이 임의 사용이 이루어지는 경우
조치방법	이동형 저장 매체에 대한 물리적 차단 조치를 적용하고 불가피한 경우 사용통제 절차를 수립하여 이행

제어시스템

C-11 (상)	4. 보안관리 > 4.2 제어시스템에서의 USB 사용을 금지하고, 사용시 USB 등의 이동형 저장매체 사용 통제

점검 및 조치 사례

Step 1) HMI, PLC 등의 제어시스템에서 USB 포트를 이용할 수 없도록 하는 다음 각 호의 방법과 같이 적용하는지 확인하고 미적용 시 가능한 조치 적용

1. USB 포트를 물리적으로 봉인 또는 사용 차단 (아래 예시 참조)

2. USB 보안통제 시스템을 구축(예: 보안USB)하여 인가된 보안USB만을 사용하도록 하는 기술적인 통제 적용 (구축 전 보안성검토 및 국정원 인증제품 사용 필수)

Step 2) Step 1의 조치(물리적 또는 기술적)가 적용되나 불가피하게 이동형 저장매체를 사용해야 하는 경우를 위하여 자체적인 사용 통제절차를 수립하고 해당 절차의 안전성을 확인 (아래 그림은 원전제어망에서의 USB 이용통제 절차 예시)

[그림] 원전제어망의 USB 이용 통제 사례

제어시스템

C-11 (상)	4. 보안관리 > 4.2 제어시스템에서의 USB 사용을 금지하고, 사용시 USB 등의 이동형 저장매체 사용 통제

Step 3) Step 2의 통제에도 불구하고 비인가 이동형 저장매체 사용 사례가 있는지 다음과 같이 점검

- 윈도우의 Registry값을 확인하는 방법으로서, CMD 창에서 윈도우 안에 내장되어 있는 Registry유틸리티인 Reg를 사용하여 레지스트리 키 값을 확인

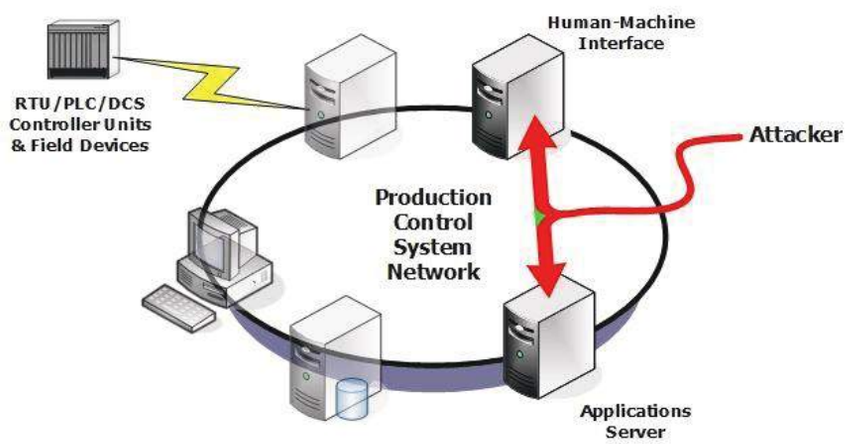
```
reg query HKEY_LOCAL_MACHINE₩SYSTEM₩ControlSet001₩Enum₩USBSTOR | findstr "HKEY_LOCAL_MACHINE"
```

- 상기 명령어를 입력 시 결과값이 나올 경우, USB 장치의 제품명 및 제조사에 대한 정보를 확인하여 인가된 USB인지 여부를 판단

```
HKEY_LOCAL_MACHINE₩SYSTEM₩ControlSet001₩Enum₩USBSTOR₩Disk&Ven_[벤더사]&Prod_[제품명]&Rev_1100
```

조치 시 영향	일반적인 경우 영향 없음

제어시스템

C-12 (상)	4. 보안관리 > 4.3 제어명령에 대한 위변조 방지 대책 적용
취약점 개요	
점검내용	■ HMI, PLC 등을 통해 제어설비에 전송되는 제어명령이 스니핑(Sniffing) 등의 패킷 감청 등으로 노출되지 않고, 중간에 해당 패킷을 가로채 위변조할 수 없도록 하는지 점검
점검목적	■ 제어명령이 비인가자에게 노출되거나 중간에서 가로챌 수 없도록 하여 안정적인 제어시스템을 운영하기 위함
보안위협	■ 제어시스템을 구성하는 HMI, PLC 등의 소프트웨어와 보안이 고려되지 않은 프로토콜을 이용하는 시스템에 따라서는 제어명령을 가로챌 수 있는 취약점이 공개되어 있어 해당 취약점으로 인한 공격이 성공하는 경우 비인가자가 제어설비의 운영권한을 획득할 수 있음 ※ 위협 시나리오 : 美 ICS CERT에서 공개한 취약점 정보에 따르면 "Open Automation Software OPC Systems NET DLL Hijacking Vulnerability"은 Open Automation OPC Systems.NET 8.00.0023 및 초기 버전에 존재하는 취약점으로서 공격자는 악성 DLL을 해당 버전을 사용하는 사용자의 시스템에 설치되도록 유도하고 성공적으로 악성 DLL이 설치되면 해당 시스템의 사용자 권한을 가로채(Hijacking) 동일한 권한을 가질 수 있다. (해당 취약점은 보안패치를 통해 제거 가능)  [그림 출처] 美 ICS-CERT (https://ics-cert.us-cert.gov)
참고	※ **OPC(OLE for Process Control):** OPC XML Data 접근 구조는 플랫폼 독립적인 상호운용성(interoperability)을 높이고 인터넷 기반의 웹서비스에 대한 포괄적인 지원을 위해 OPC 재단(Foundation)에서 연구, 개발한 프로토콜 ※ **무선통신 인터셉트(EM/RF Interception):** 일반적인 제어시스템 통신구간에서는 무선통신을 사용하지 않지만 RTU 하단의 제어기기들과 IED에는 무선통신이 적용되는 경우가 있고 해당 통신 구간의 통신은 비인가 기기를 이용한 가로채기가 상대적으로 용이 ※ **무결성 체크:** 데이터의 무결성을 체크하기 위해 MD5, SHA-1 등의 해쉬함수를 이용하여 데이터가 최초 원본 상태와 다른 변형된 것이지 확인(MD5는 임의의 길이의 메세지를 입력받아 128비트 길이의 출력값을 나타내며, 만약 원본 파일이 1비트라도 다르면 변형된 것으로 판단)

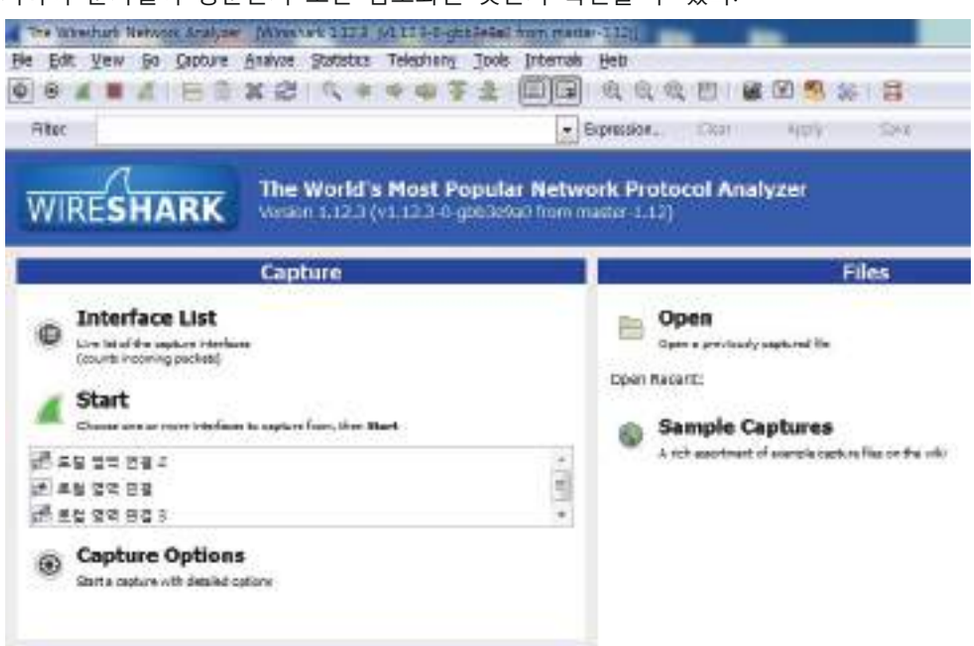
제어시스템

C-12 (상)	4. 보안관리 > 4.3 제어명령에 대한 위변조 방지 대책 적용
점검대상 및 판단기준	
대상	■ 제어시스템을 구성하는 네트워크 전체
판단기준	**양호:** 제어명령을 암호화 전송하거나 송수신 정보의 무결성을 체크(위·변조 여부 확인)하는 경우
	취약: 제어명령이 암호화되지 않고 평문 전송되거나, 송수신 정보의 무결성을 체크하지 않는 경우
조치방법	전송되는 정보를 암호화하거나 정보의 무결성을 점검할 수 있도록 개발 변경
점검 및 조치 사례	

Step 1) 전송되는 제어명령을 스니핑(Sniffing)하여 암호화 송수신이 이루어지는지 확인하고 암호화가 필요함에도 평문 전송이 이루어지고 있다면 암호화 전송되도록 (별도 전송장비를 사용하는 경우)송수신 장비의 설정을 변경하거나 해당 소프트웨어의 개발 변경

- 제어명령을 수신하는 서버 및 PC에서 와이어샤크(WireShark)와 같은 스니핑 도구를 설치, 이용하여 전송되는 데이터가 암호화되는지 점검

※ 와이어샤크(WireShark)가 설치된 시스템의 LAN카드를 지정하면 해당 LAN카드를 통해 송수신되는 데이터 패킷을 캡쳐하여 문자열이 평문인지 또는 암호화된 것인지 확인할 수 있다.



[그림] WirkShark을 설치, 실행한 화면

Step 2) 제어명령을 송수신하는 서버 및 PC 등이 전송된 데이터가 원본과 일치하는지를 확인하는 무결성 체크 과정을 거치는지 점검하고 무결성 체크 없이 송수신 된다면 (별도 전송장비를 사용하는 경우)송수신 장비의 설정을 변경하거나 해당 소프트웨어의 개발 변경

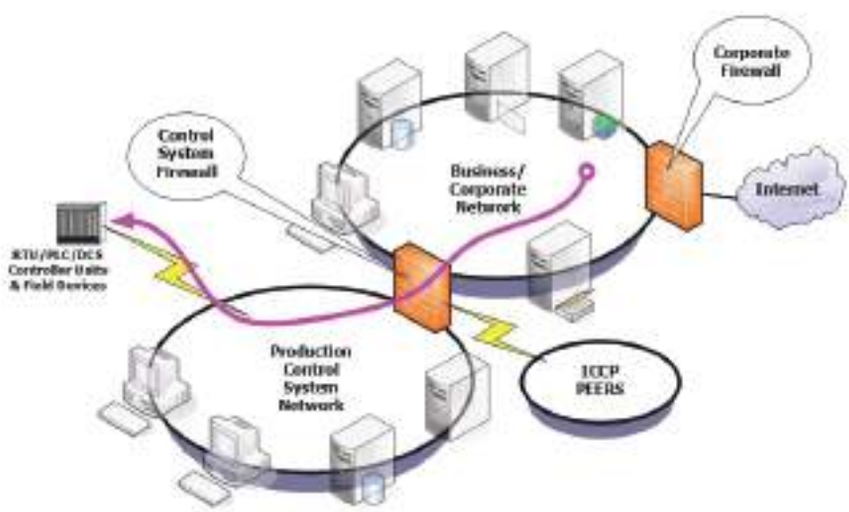
제어시스템

C-12 (상)	4. 보안관리 > 4.3 제어명령에 대한 위변조 방지 대책 적용
- 해당 항목 점검방법은 송수신 되는 데이터를 조작하여 발송한 뒤 무결성 점검 없이 정상 수신되는지를 확인하는 방식으로 이루어져야 하나, 점검 환경의 제약이 따르는 경우는 대상 제어시스템의 개발, 운용 담당자와의 인터뷰를 통하여 확인 ※ 개발업체의 협조 여부에 따라서 개발 변경이 어려울 수 있다. 개발 변경 가능 여부를 파악하여 취약점 조치 여부를 결정한다.	
조치 시 영향	일반적인 경우 영향 없음

제어시스템

C-13 (상)	4. 보안관리 > 4.4 제어명령 replay 공격에 대한 방지 대책 적용
취약점 개요	
점검내용	■ HMI, PLC 등을 통해 제어설비에 전송되는 제어명령을 스니핑(Sniffing) 등의 패킷 감청 등으로 캡쳐하고, 해당 패킷을 임의의 기기에서 재사용하여 제어설비에 전송, 조작할 수 없도록 하는지 점검
점검목적	■ 제어명령이 비인가자에게 노출될 수 있더라도 노출된 정보를 재사용할 수 없도록 하여 안정적인 제어시스템을 운영하기 위함
보안위협	■ HMI, PLC 등 제어시스템의 취약점(보안이 고려되지 않은 프로토콜 사용 등)을 이용하여 제어명령을 스니핑하거나, 조작된 데이터를 전송하여 비인가자가 제어설비의 운영 권한을 획득할 수 있음
참고	※ **Replay 공격:** 네트워크 상의 정보 프레임을 수집한 뒤 해당 메시지를 재전송함으로써 갱신되지 않은 정보의 전달이나, 대상 장비에게 정당한 정보전송으로 인식시켜 오류를 유도하는 공격 기법으로, HMI 서버와 RTU 사이의 통신선로에 인가되지 않은 해킹 기기를 접속시켜 각각 HMI 서버와 RTU에 해당 공격을 수행 가능
점검대상 및 판단기준	
대상	■ 제어시스템을 구성하는 네트워크 전체
판단기준	**양호:** 전송되는 제어명령이 재사용되지 못하도록 인증, 시간확인, 세션확인 등의 검증 과정을 거치도록 하는 경우
	취약: 전송되는 제어명령이 인증, 시간확인, 세션확인 등의 검증 과정을 거치지 않아 임의의 기기에서 재사용 가능한 경우
조치방법	전송되는 정보를 재사용할 수 없도록 인증, 시간확인, 세션확인 등의 방식이 적용되도록 개발 변경
점검 및 조치 사례	
Step 1) 전송되는 제어명령을 스니핑(Sniffing) - 와이어샤크(WireShark)와 같은 스니핑 도구를 이용하여 점검하고 본 단계의 내용은 C-12(상)의 세부점검 요령을 참조 Step 2) 전송되는 제어명령을 스니핑(Sniffing)하여 임의의 기기에 저장하고, 이를 제어설비에 전송하여 제어명령이 수행되는지 점검하되 실제 제어명령 재사용이 가능하다면 다음 각 호의 방법과 같이 (별도 수신장비를 사용하는 경우)장비의 설정을 변경하거나 해당 소프트웨어의 개발 변경 1. 제어명령을 송수신하는 서버 및 PC 등이 상호 맞는지 확인하는 인증 과정(예: IP주소 일치 여부 점검)을 적용 2. 제어명령의 전송시간을 확인하여 일반적인 요청, 응답 시간 이내인지 Time Stamp를 확인하는 과정을 적용 3. 제어명령에 세션키를 적용하여 만료된 세션키인 경우는 재사용된 것으로 판단 ※ 개발업체의 협조 여부에 따라서 개발 변경이 어려울 수 있다. 개발 변경 가능 여부를 파악하여 취약점 조치 여부를 결정한다.	
조치 시 영향	일반적인 경우 영향 없음

제어시스템

C-14 (상)	4. 보안관리 > 4.5 제어시스템 개발자, 운영자, 관리자에 대한 접근권한 분리
취약점 개요	
점검내용	■ 제어시스템(HMI, PLC 등) 접근 권한을 업무상 요구되는 부서(IT, 운영, 관리 등) 및 인원으로 제한하고 있는지 점검
점검목적	■ 제어시스템(HMI, PLC 등) 접근 권한을 업무상 요구되는 부서(IT, 운영, 관리 등) 및 인원으로 제한하여 공격이나 사고에 의한 위협을 감소시킴
보안위협	■ 업무를 수행하는데 불필요한 권한을 할당받은 사용자가 악의적인 목적으로 제어시스템을 공격하거나, 잘못된 운전 조작 사고 등을 일으킬 수 있음(IT 부서는 개발 또는 시스템 유지보수, 운영부서는 제어설비 모니터링, 관리부서는 설비 운전제어를 담당해야 하나 운영부서에 과도한 권한이 할당되어 있다고 가정할 때, 운영자가 제어망 내 임의 설비에 접근하여 운전 조작 등의 피해를 일으킬 수 있음)
참고	※ 네트워크 접근통제 고려사항 업무망에서 제어망 내의 시스템 및 설비를 접근해야 하는 경우, 임의의 PC에서 임의의 시스템과 설비에 접근할 수 없도록 제어망의 방화벽에 접근을 허용하는 출발지 IP주소(또는 대역)와 목적지 IP주소(또는 대역)를 특정하도록 접근통제 정책(Rule)을 적용한다. (단, 제어망 내에서의 접근통제는 네트워크장비(예: 스위치), 서버의 접근통제(예: 서버의 IP Block 기능)를 활용)  [그림 출처] 美 ICS-CERT (https://ics-cert.us-cert.gov)
점검대상 및 판단기준	
대상	■ 분산네트워크 환경에서 HMI, PLC 등의 S/W를 통해 대상 시스템 및 기기에 접속하기 위해 계정(ID) 접근이 요구되는 제어시스템 ■ 제어시스템을 구성하는 네트워크 전체

제어시스템

C-14 (상)	4. 보안관리 > 4.5 제어시스템 개발자, 운영자, 관리자에 대한 접근권한 분리
판단기준	**양호:** 제어망과 업무망 사이 또는 제어망 내에서 방화벽, 네트워크장비(예: 스위치), 시스템(운영체제) 등의 수준으로 접근을 허용하는 대상(IP주소)을 제한하는 경우
	취약: 제어망과 업무망 사이 또는 제어망 내의 시스템이 접근 허용 대상을 특정하지 않아 임의 PC에서 각 시스템에 대한 접근이 가능한 경우
조치방법	각 제어시스템에 대하여 부서(IT, 운영, 관리 등)별 접근 가능한 위치(IP주소)를 지정

점검 및 조치 사례

Step 1) 제어시스템의 네트워크 구성도를 확인하여 제어망, 업무망 간의 업무 목적상 접근을 허용해야 하는 부서 및 인원의 위치(IP주소)와 제어망 내의 주요 시스템 위치(IP주소)를 확인

Step 2) 제어망 내의 주요 시스템에 접근 가능한 IP주소를 지정하여 임의의 PC에서 제어시스템 접근을 할 수 없도록 하는지 확인

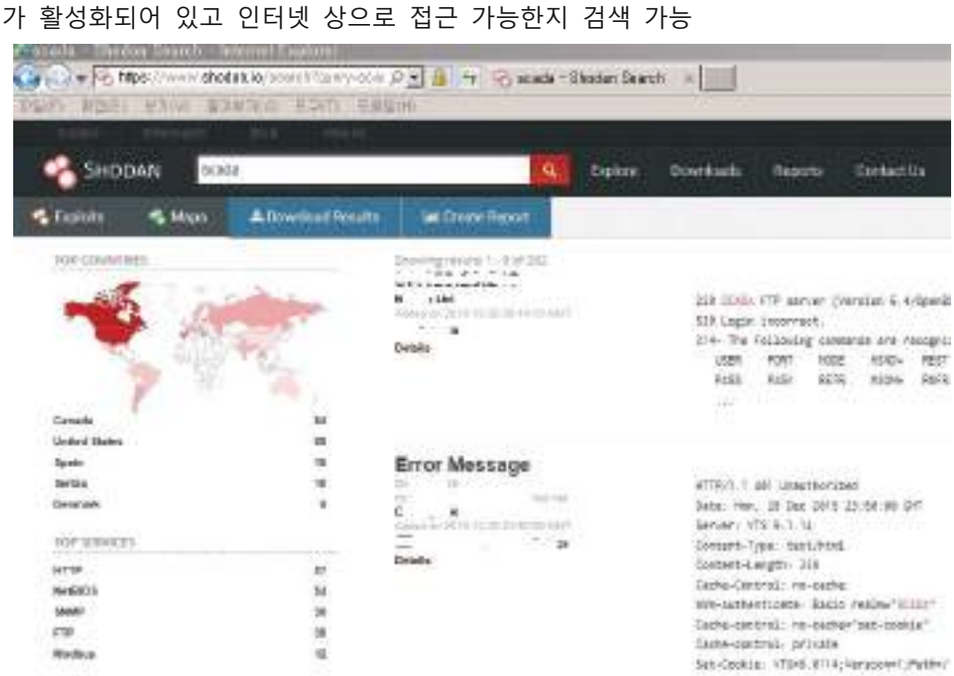
- 제어시스템에 접근이 불필요한 업무망 PC의 윈도우 CMD 창에서 제어시스템까지 접근을 허용(예: ping <제어시스템의 IP주소>)하는지 점검하고 임의 접근이 가능하다면 다음 각 호의 방법 중 하나 이상을 이용하여 개선 조치

1. 제어망과 업무망 사이의 방화벽 접근통제 정책(Rule) 적용
2. 제어망 내의 임의 접근이 가능한 경우, 제어망 내의 네트워크 장비(예: 스위치) ACL 규칙을 적용
3. 대상 제어시스템의 운영체제 방화벽(예: 윈도우즈 방화벽, 유닉스 계열의 IPtables)에 접근규칙을 적용 (이 경우 점검항목 C-15(상)의 조치 방법 참조)

※ 방화벽, 네트워크장비(예: 스위치), 서버 등에 적용 가능한 접근통제 규칙 변경(예: All deny 후 필요한 IP에 대하여만 접근 허용)이 이루어지면 HMI, PLC 등의 제어시스템과 설비 간의 오작동 우려가 있으므로 제어시스템 등의 가용성에 영향이 발생하지 않도록 철저한 사전 준비, 테스트 등을 통해 개선조치가 이루어져야 한다.

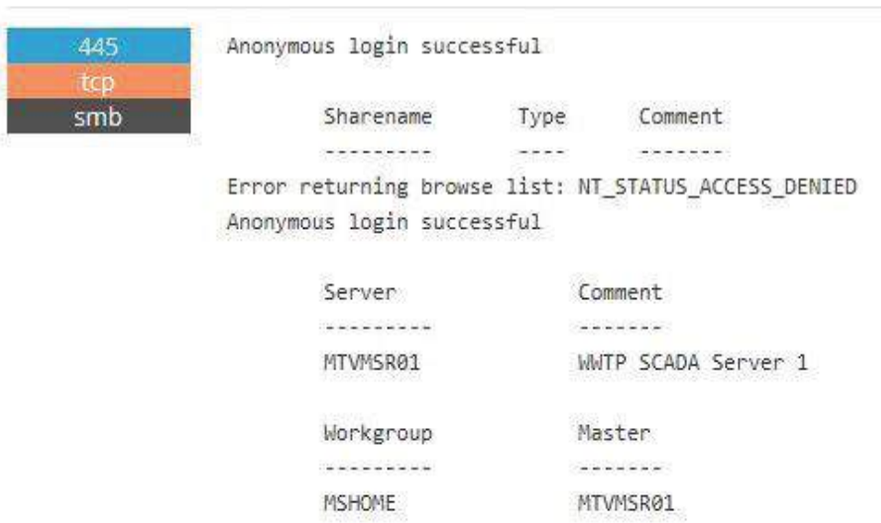
조치 시 영향	제어시스템, 설비 간의 오작동 또는 업무상 필요한 직무자임에도 제어시스템 접근 불가

제어시스템

C-15 (상)	4. 보안관리 > 4.6 제어시스템, 제어기기에 (vendor default) 은닉서비스 및 취약한 서비스가 없도록 설정
취약점 개요	
점검내용	■ HMI, PLC, Data Historian 등의 소프트웨어가 구동되는 제어시스템(서버 또는 PC의 운영체제)에 취약한 서비스를 제거하거나 이용할 수 없도록 비활성화 시켰는지 점검
점검목적	■ 제어시스템(운영체제)에 관련 소프트웨어를 위해 필요한 최소한의 서비스만 활성화하고 취약한 서비스를 제거 또는 비활성화하여 비인가자 및 악성코드에 의한 취약한 서비스 악용이 일어나지 않도록 함
보안위협	■ 불필요하거나 취약한 서비스가 활성화되어 있는 경우 네트워크 스캐닝을 통해 취약한 서비스를 찾아내, 비인가자 접근, 악성코드 유포 등 해당 서비스를 악용한 해킹 우려가 있음 ※ 위협 사례 : SMB 리다이렉트(Redirect To SMB) 공격의 경우, 윈도우 PC간에 파일 공유를 위해 사용하는 SMB(Server Message Block) 프로토콜을 악용하여, 해당 네트워크 트래픽을 해커가 장악한 SMB 서버 또는 악성 웹사이트로 우회시킬 수 있는 취약점을 이용한다. 이를 통해 해커는 윈도우 PC 사용자들의 해당 로그인 정보를 탈취할 수 있다. 이와 같은 공격에 대한 최선의 보안대책은 TCP 139와 445 포트를 차단하여 SMB 프로토콜 자체를 이용하지 못하도록 하는 것이다.
참고	※ **제어시스템 취약점 검색엔진:** 쇼단(Shodan)과 같은 웹사이트는 IoT, ICS 등과 같은 설비 기반의 IT인프라에 대해 국가, 기관, 서비스(Port), IP주소 등의 검색어 입력만으로 어떤 서비스가 활성화되어 있고 인터넷 상으로 접근 가능한지 검색 가능  [그림] 쇼단 홈페이지에서 검색어(예: scada)를 통해 확인된 결과

제어시스템

C-15 (상)	4. 보안관리 > 4.6 제어시스템, 제어기기에 (vendor default) 은닉서비스 및 취약한 서비스가 없도록 설정



[그림] 쇼단을 통해 확인된 제어시스템을 상세 확인한 결과

점검대상 및 판단기준	
대상	■ HMI(Human Machine Interface), PLC(Programmable Logic Controller), Data Historian 등의 소프트웨어가 구동되는 서버 및 PC(운영체제)
판단기준	**양호:** 제어시스템에 불필요하거나 취약한 서비스가 제거 또는 비활성화된 경우
	취약: 제어시스템에 불필요하거나 취약한 서비스가 활성화된 경우
조치방법	제어시스템에 불필요하거나 취약한 서비스를 제거 또는 비활성화 조치 (제어시스템의 운영체제(UNIX, Windows)에 따른 서비스 비활성화는 해당 기술적 취약점 점검영역 중 "서비스 관리" 부분의 조치 방법 참조)

점검 및 조치 사례

Step 1) 제어시스템 현황(목록)과 네트워크 구성도를 확인하여 제어시스템별 감시, 설비제어 등을 위해 필요한 서비스(Port) 종류 확인

Step 2) 제어시스템에 대하여 업무망, 제어망 내에서 네트워크 스캐닝 도구(예: nmap), 운영체제의 방화벽 기능 등을 통해 해당 제어시스템에 활성화된 서비스(Port)가 불필요한 것인지 또는 취약한 것인지 점검하고 불필요하거나 취약하다면 다음 각 호의 방법 등을 이용하여 해당 서비스를 비활성화 조치

1. 제어망, 업무망의 방화벽 접근통제 정책(Rule)을 적용
2. 제어망 내의 네트워크 장비(예: 스위치) 접근규칙(ACL) 적용
3. 제어시스템의 운영체제에 따라서는 다음과 같이 운영체제 방화벽 기능을 이용하여 조치 가능

제어시스템

C-15 (상)	4. 보안관리 > 4.6 제어시스템, 제어기기에 (vendor default) 은닉서비스 및 취약한 서비스가 없도록 설정

■ Windows OS

1) 시작> 설정> 제어판> 관리도구> 서비스에서 불필요한 서비스 중지
(시작옵션에서 시작유형을 "사용안함"으로 설정)
2) 시작> 설정> 제어판> 방화벽설정에서 접근 가능한 IP 제한

■ Unix, Linux OS

1) #vi /etc/inetd.conf 파일에서 불필요한 서비스 주석(#) 처리하여, 해당 서비스 비활성화
2) #/etc/hosts.allow에 접근 가능한 서비스, IP 지정
3) #/etc/hosts.deny에서 차단하고자 하는 서비스, IP 지정

※ 불필요한 서비스 비활성화 예시

SMB(Session Message Block) 프로토콜은 Windows에서 디스크와 프린터를 네트워크 상에서 공유하는데 사용되며, TCP 139번, 445번 포트를 사용한다. SMB를 비활성화하려면 다음과 같은 방법으로 TCP/IP에서 SMB를 언바인드 시킨다.

① 바탕화면 또는 제어판에서 [네트워크 환경]의 [등록정보]를 실행한다.
② 현재 인터넷에 접속된 연결의 [등록정보]를 선택한다.
③ [Microsoft 네트워크용 클라이언트] 항목과 [Microsoft 네트워크용 파일 및 프린터 공유] 항목의 체크를 해제한다.

※ 방화벽, 네트워크장비(예: 스위치), 서버 등에 적용 가능한 접근통제 규칙 변경(예: All deny 후 필요한 Port만 허용)이 이루어지면 HMI, PLC 등의 제어시스템과 설비 간의 오작동 우려가 있으므로 제어시스템 등의 가용성에 영향이 발생하지 않도록 철저한 사전 준비, 테스트 등을 통해 개선조치가 이루어져야 한다.

조치 시 영향	제어시스템 가용성 침해 우려

C-16 (상)	**4. 보안관리 > 4.7 제어프로그램의 입력창에 비정상적인 특정값을 입력할 시 사전에 정의한 에러메시지가 출력되도록 하여 시스템 중요정보가 노출되지 않도록 설정**
취약점 개요	
점검내용	■ HMI 등의 제어시스템 입력창 중 문자열 입력이 가능한 경우 허용된 범위(예: 문자유형, 길이 등)의 값만 입력되도록 하고, 허용된 범위를 초과하는 비정상적인 값이 입력되더라도 오류 화면 등이 나타나지 않도록 하는지 점검
점검목적	■ 제어시스템 감시 및 제어를 위한 HMI 등의 소프트웨어는 운영, 관리 등의 권한에 따라 입력값을 통해 운전정보를 조회하고 제어할 수 있도록 하기 때문에 입력값이 정상적인 범위 내에서 처리되고 오류 화면 등의 불필요한 정보 노출이 이루어지지 않도록 하여 운영자의 부주의(Human Error) 또는 오·남용을 차단하고자 함
보안위협	■ 내부자가 HMI 등의 제어시스템 입력창에 비정상적인 값을 입력하여 그 결과 화면에 노출된 민감한 정보를 수집하여 악의적인 목적으로 사용할 우려가 있음 ■ 해당 취약점이 알려져 있는 경우 이를 악용한 악성코드 감염을 통해 HMI 등의 제어시스템 권한을 이용한 제어설비 오동작 등의 피해 발생 가능
참고	※ 본 취약점은 제어시스템을 개발, 납품하는 업체가 개발단계에서부터 보안취약점이 최소화되도록 해야 하고, 운영단계에서 확인된 취약점이 있다면 제품을 이용하는 회사, 기관 등에 해당 취약점이 조치된 업데이트 및 보안패치를 배포되도록 해야 함  [그림] HMI 화면 예시
점검대상 및 판단기준	
대상	■ HMI(Human Machine Interface), PLC(Programmable Logic Controller), Data Historian 등의 제어시스템 운영 소프트웨어
판단기준	**양호:** 허용된 범위를 초과하는 값을 입력해도 불필요한 민감 정보 등의 노출되지 않는 경우
	취약: 허용된 범위를 초과하는 값을 입력하는 경우 비정상적인 결과 화면이 나타나는 경우
조치방법	허용된 범위의 값만이 입력되도록 하고 비정상적인 값이 입력되더라도 오류 화면 등이 나타나지 않도록 개발 변경

제어시스템

C-16 (상)	4. 보안관리 > 4.7 제어프로그램의 입력창에 비정상적인 특정값을 입력할 시 사전에 정의한 에러메시지가 출력되도록 하여 시스템 중요정보가 노출되지 않도록 설정

점검 및 조치 사례

Step 1) HMI 등의 소프트웨어에 운영자가 입력 가능한 입력창이 있는 경우, 해당 입력창에 다음 각 호와 같은 유형의 비정상적인 값을 입력했을 때 사전 정의된 결과(예: 정상적인 값을 입력하도록 하는 경고 메시지 출력)가 나타나는지 확인

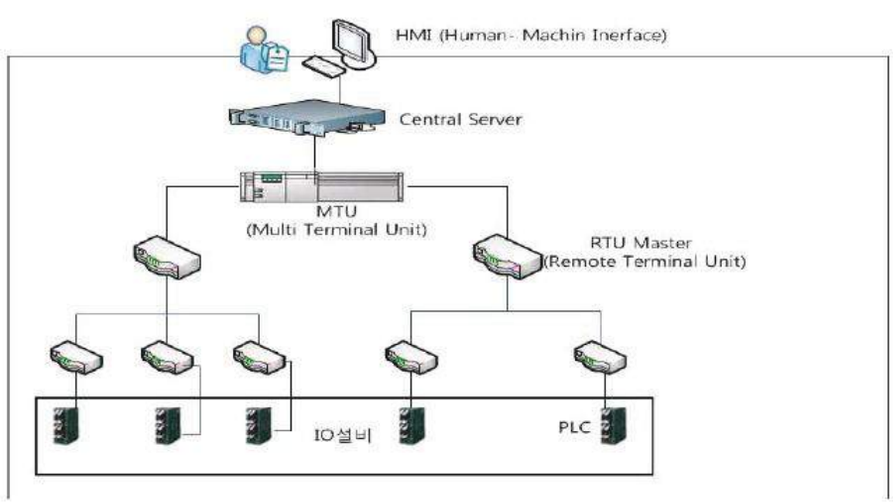
1. 허용되는 문자 유형이 아닌 다른 문자 유형을 입력(예: 숫자만 입력해야 하는 입력창에 문자나 특수문자를 입력)
2. 허용되는 문자 길이를 초과하여 입력(예: 보통 4개 문자만 입력하면 되나 8개 문자를 입력)
3. DB서버와 연동된 경우, DB 쿼리(Query) 수준에 해당하는 문자열을 입력(이 부분은 웹 취약점 점검항목 중 SQL Injection 부분의 점검 및 조치 방법 참조)

Step 2) Step 1의 결과와 달리 비정상적인 에러페이지가 나타나고 특히 해당 에러페이지에 제어시스템에 관련된 주요 시스템 정보가 노출된다면 해당 소프트웨어를 개발한 업체에 개선 조치 요청하여 허용되는 값은 입력되도록 하고 어떠한 경우에도 비정상적인 결과 및 정보가 노출되지 않도록 개발 조치

※ 개발업체의 협조 여부에 따라서 개발 변경이 어려울 수 있다. 개발 변경 가능 여부를 파악하여 취약점 조치 여부를 결정한다.

조치 시 영향	일반적인 경우 영향 없음

제어시스템

CS-17 (중)	4. 보안관리 > 4.8 정보시스템에 대한 정책과 별도로 제어시스템에 대한 정보보안 정책, 지침이 수립되어 있는가?
취약점 개요	
점검내용	■ HMI, PLC, RTU 등의 제어시스템에 특화된 정보보호 지침이 수립되어 있는지 점검
점검목적	■ 제어시스템에 특화된 정보보호 지침을 수립하여 제어시스템 보안관리 주체를 지정하고, 제어시스템에 특화된 관리적·물리적·기술적 보안을 체계적으로 관리하기 위함
보안위협	■ 일반 IT시스템 중심의 보안관리 이외에 제어시스템에 특화된 보안관리 요소, 취약점 조치 등이 누락되어 운영인력의 부주의(Human Error) 발생하거나 운영상의 취약점을 악용한 사이버 침해위협 발생 가능
참고	※ SCADA 시스템의 일반적인 구조 SCADA 시스템은 일반적으로 HMI, PLC, RTU 등의 제어시스템에 특화된 시스템 및 기기로 구성되기 때문에 일반적인 IT시스템 측면의 정보보호와 다른 관리적, 기술적인 정책과 지침이 필요 
점검대상 및 판단기준	
대상	■ 제어시스템 보안관리 조직
판단기준	**양호:** 제어시스템에 특화된 정보보호 지침이 별도로 수립되어 있는 경우
	취약: 제어시스템에 특화된 정보보호 지침이 별도 수립되지 않은 경우 (기존 IT보안 정책 또는 지침에 준하여 관리가 이루어지는 경우)
조치방법	제어시스템에 특화된 정보보호 지침을 별도 제정

제어시스템

CS-17 (중)	4. 보안관리 > 4.8 정보시스템에 대한 정책과 별도로 제어시스템에 대한 정보보안 정책, 지침이 수립되어 있는가?

점검 및 조치 사례

Step 1) 제어시스템에 대한 보안관리 주체와 역할, 제어시스템에 대한 접근통제 및 운영보안 등을 포함하는 제어시스템 보안관리지침(가칭)이 별도 존재하는지 확인하고 존재하지 않다면 다음과 같은 내용(목차 예시) 수준의 제어시스템 보안관리지침을 수립(제정)

제 1 장 총 칙
제1조 (목적)
제2조 (적용범위)
제3조 (정의)
제 2 장 제어보안 관리체계에 대한 활동
제4조 (활동방향)
제5조 (제어보안책임자 및 제어보안담당자)
제6조 (제어보안담당자 임무)
제7조 (취약점 진단 및 보호대책 수립)
제8조 (제어보안 교육)
제9조 (긴급사태 관리)
제10조 (제어망 운영)
제11조 (보안관리 절차 수립)
제12조 (통제구역)
제13조 (백신 프로그램 운영)
제14조 (휴대용 저장매체 사용통제)
제15조 (유지보수 통제 및 기록 관리)
제16조 (원격 유지보수 제한)
제17조 (보안성 검토 및 보안적합성 검증)
제18조 (자료관리)
제19조 (계약사항)
제 3 장 보 칙

※ 제어시스템 보안관리지침의 목차 및 세부 내용은 제어시스템을 보안관리하는 조직에 따라 다를 수 있으나, 제어시스템에 대한 기반시설 취약점 점검항목(총 22개)을 고려하여 그 내용이 포함되도록 한다.

조치 시 영향	일반적인 경우 영향 없음

제어시스템

CS-18 (중)	4. 보안관리 > 4.9 비인가자 또는 인증과정이 없는 제어시스템, 제어기기에 대한 환경 설정이 가능하지 않도록 되어있는가?
취약점 개요	
점검내용	■ HMI, PLC 등의 제어시스템과 제어설비 접근 시에 계정(ID) 로그인 등의 사용자 인증과정을 거치도록 하는지 점검
점검목적	■ 제어시스템을 구성하는 서버, PC, 네트워크장비 및 제어설비 등의 접근 시에 사용자(운영인력, 관리자 등) 인증을 거치도록 하여 비인가자에 의한 임의 접근을 차단함
보안위협	■ 시스템(서버, PC, 네트워크장비, 제어설비 등)에 따라서는 관리자(admin) 페이지가 존재하는 경우가 있고 해당 시스템의 기본 계정(예: admin)과 패스워드(예: admin)가 알려져 있다면 악의적인 운영자가 해당 시스템의 관리자 권한 및 운전제어 권한을 획득할 우려 ■ HMI 등의 소프트웨어인 경우 사용자 인증 없이 운전정보를 모니터링하고 일부 운전제어까지 가능하다면 악의적인 사용자가 로그인할 수 있는 프로그램을 PC에 설치하고 이를 통해 제어시스템 모니터링 및 운전제어 권한을 획득하여 악용할 우려가 있음
참고	※ 각 시스템은 접근을 허용하는 사용자 및 관리자의 위치(IP주소)를 지정하여 접근이 허용된 인원 외에는 임의 접근을 할 수 없도록 하는 네트워크 또는 서버 기반의 접근통제 규칙 적용이 필요 (이에 대한 사항은 점검항목 C-14(상)을 참조)
점검대상 및 판단기준	
대상	■ 제어시스템을 구성하는 서버, PC, 네트워크장비, 제어설비 등의 각종 기기 (특히 HMI, PLC 등)
판단기준	**양호:** 제어시스템을 구성하는 각종 기기에 사용자 인증과정을 거치도록 하는 경우
	취약: 제어시스템을 구성하는 각종 기기에 사용자 인증과정 없이 임의 접근 및 사용이 가능한 경우
조치방법	HMI, PLC 등의 제어시스템에 사용자 인증과정을 거치도록 설정 적용 또는 개발 변경
점검 및 조치 사례	
Step 1) HMI, PLC 등의 제어시스템 접속 시 사용자 인증(예: ID, PW 입력)을 요구하는지 확인하고 사용자 인증 없이 모니터링 및 운전제어 등의 기능을 이용할 수 있다면 사용자 인증을 거치도록 환경설정을 변경하거나 해당 제품의 개발 변경 적용 Step 2) 제어시스템을 구성하는 기기 중 네트워크 상으로 관리자 설정 기능에 접근 가능한 기기가 있다면 해당 기기에 접근하여 사용자 인증(예: ID, PW 입력)을 요구하는지 확인하고 만약 인증절차 없이 관리자 설정 기능에 접근 가능하면 해당 기기의 환경 설정을 통해 인증절차를 거치도록 조치	

제어시스템

CS-18 (중)	4. 보안관리 > 4.9 비인가자 또는 인증과정이 없는 제어시스템, 제어기기에 대한 환경 설정이 가능하지 않도록 되어있는가?
Step 3) Step 1과 Step2를 통해 사용자 인증 절차가 적용되는 경우에도 추측 가능한 계정 및 패스워드(Default ID 및 Password 등)가 존재한다면 해당 패스워드를 안전한 규칙(복잡도, 길이 고려)을 적용하여 변경 ※ 대상 시스템에 따라 개발 변경이 필요한 경우가 존재하며, 개발업체의 협조 여부에 따라서 개발 변경이 어려울 수 있다. 개발 변경 가능 여부를 파악하여 취약점 조치 여부를 결정한다.	
조치 시 영향	인증정보 분실 시 제어시스템 접근 불가(적절한 인수인계 필요) 일부 제어시스템에 따라 접속 오류 또는 부팅 오류

제어시스템

CS-19 (중)	4. 보안관리 > 4.10 제어시스템 및 운영시스템은 제어를 위한 목적으로만 사용되도록 다른 기능 및 서비스를 제거하였는가?
취약점 개요	
점검내용	■ HMI 등의 제어시스템이 운영 목적에 맞게 최소한의 기능(예: 운전정보 모니터링, 운전조작 불가)만을 유지하도록 하는지 점검
점검목적	■ HMI 등이 소프트웨어에 따라서 단순 모니터링부터 제어설비 정지 수준의 기능까지 구현할 수 있으므로, 이를 운영, 관리하는 인원의 업무역할에 맞는 최소한의 기능(예: 단순 모니터링)만이 포함되도록 하여 운영인력의 부주의(Human Error) 및 오·남용을 차단하기 위함
보안위협	■ 제어설비의 운전정보를 단순 모니터링하기 위해 HMI 등의 제어시스템을 구축했지만 해당 제어시스템의 기능에 모니터링 이외에도 제어명령까지 사용할 수 있는 기능이 기본 포함되어 있다면 운영자에게 과도한 제어권한이 부여되어 이를 악용할 수 있음
참고	※ 본 취약점은 제어시스템을 개발, 납품하는 업체가 개발 및 구축단계에서부터 불필요한 기능을 제거하고 제어시스템 운영 목적에 맞는 최소한의 기능만이 적용되도록 해야 하므로, 운영 중인 상황이라면 해당 업체를 통해 불필요한 기능 삭제가 가능한지 여부를 확인하거나 관리자(admin) 기능을 이용해 불필요한 기능을 비활성화(disable)할 수 있는지 확인 필요  [그림] HMI 화면 예시
점검대상 및 판단기준	
대상	■ HMI 등의 제어시스템
판단기준	**양호:** HMI 등의 제어시스템이 업무상 필요한 최소 기능만을 보유한 경우
	취약: HMI 등의 제어시스템이 불필요하거나 민감한 기능(예: 운전정지)을 보유한 경우
조치방법	제어시스템에 불필요하거나 민감한 기능을 삭제(설정 또는 개발 변경)

제어시스템

CS-19 (중)	4. 보안관리 > 4.10 제어시스템 및 운영시스템은 제어를 위한 목적으로만 사용되도록 다른 기능 및 서비스를 제거하였는가?
점검 및 조치 사례	
Step 1) 제어시스템 현황(목록)을 확인하여 특히 HMI 등의 제어시스템으로 가능한 기능과 해당 제어시스템을 운영하는 인력의 업무범위를 상호 비교(예: HMI 운영인력 3명 모두 단순 운전정보 모니터링 업무이고 HMI의 기능에는 운영자 계정 접속 시 운전제어 기능까지 이용 가능) Step 2) HMI 등의 제어시스템 운영인력의 업무범위를 초과하는 불필요한 기능(예: 모니터링 대상이 아닌 설비의 운전정보 열람) 또는 민감한 기능(예: 운전제어 등)이 있는지 확인 ※ 대상 시스템에 따라 개발 변경이 필요한 경우가 존재하며, 개발업체의 협조 여부에 따라서 개발 변경이 어려울 수 있다. 개발 변경 가능 여부를 파악하여 취약점 조치 여부를 결정한다.	
조치 시 영향	업무상 필요한 기능까지 제거하는 경우 정상적인 제어시스템 운영업무 어려움

제어시스템

CS-20 (중)	4. 보안관리 > 4.11 운영에 있어 사용가능한 제어명령 및 안전한 제어를 위한 파라미터의 범위를 제한하고 있는가?
취약점 개요	
점검내용	■ 제어시스템을 통해 설비에 전달되는 제어명령의 문자열이 운영 목적에 맞는 최소 권한으로 전달되도록 불필요한 파라미터 사용을 제한하는지 점검
점검목적	■ 제어시스템 감시 및 제어를 위한 HMI, PLC 등의 소프트웨어는 운영, 관리 등의 권한에 따라 입력값을 통해 운전정보를 조회하고 제어할 수 있도록 하기 때문에 운영자에 따른 제어명령 제한과 파라미터 값의 범위를 제한하여 운영자의 부주의(Human Error), 오·남용 및 악성코드에 의한 악의적인 운전명령 전달 등을 차단하고자 함
보안위협	■ 운영자가 직무 권한을 초과하는 제어명령을 사용할 수 있거나 사용할 수 있는 제어명령의 파라미터 값(예: 설비에 적용할 수치) 범위를 초과한 과도한 값을 부여할 수 있다면 부주의(Human Error), 오·남용이 발생할 수 있고 특히 악성코드에 의한 악의적인 운전명령 및 과도한 파라미터 값 전달을 통해 제어설비의 오작동 등의 피해가 발생할 수 있음 ※ 위협 사례 : 스턱스넷은 PLC 시스템의 Profibus 메시지 버스 시스템을 감시하는 D8890 블록에 악성 코드를 설치하여 특정 조건이 만족되면, 스턱스넷은 주기적으로 모터의 회전수를 1410Hz, 2Hz, 1064Hz로 변경해 모터에 과부하를 일으킨다. 또한 PLC 시스템에 루트킷을 설치하여 자기 자신을 숨기고, 모터의 회전수가 변경되고 있다는 것을 숨긴다.
참고	※ HMI, PLC 등의 소프트웨어를 통해 사용 가능한 제어명령, 파라미터 값의 범위 등을 사전에 제한하여 운영자 권한 또는 악성코드에 의해 불필요한 제어명령과 파라미터 값 전송이 일어나지 않도록 제어시스템의 환경설정 강화 필요
점검대상 및 판단기준	
대상	■ HMI, PLC 등의 제어시스템 운영 소프트웨어
판단기준	**양호:** 운영 업무목적에 필요한 최소한의 제어명령과 파라미터만을 사용하도록 제한하는 경우
	취약: 운영 업무범위를 초과하는 제어명령과 파라미터의 사용 제한이 없는 경우
조치방법	운영 목적에 맞는 필요 최소한의 제어명령과 파라미터만을 사용하도록 HMI, PLC 등의 관리설정을 강화(제어명령 권한 조정)하거나 개발 변경 적용

제어시스템

CS-20 (중)	4. 보안관리 > 4.11 운영에 있어 사용가능한 제어명령 및 안전한 제어를 위한 파라미터의 범위를 제한하고 있는가?

점검 및 조치 사례

Step 1) HMI, PLC 등을 통해 사용 가능한 제어명령어와 제어명령별 파라미터 등을 확인하고 각 운영자별 제어명령 사용권한을 함께 확인
- 운영자별 최소 권한 부분은 점검항목 C-05(상)의 점검 및 조치사항을 함께 고려

Step 2) Step 1을 통해 확인한 결과, 모든 운영자가 동일한 수준의 제어명령 및 파라미터 사용이 가능하다면 HMI, PLC 등의 관리권한을 이용한 설정 또는 개발 변경을 통해 업무목적에 필요한 제어명령과 파라미터만을 사용할 수 있도록 제한 조치

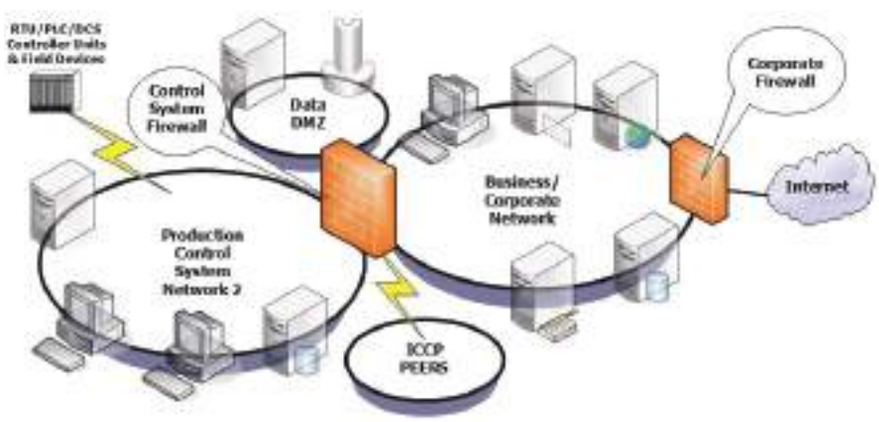
※ 일반적으로 HMI, PLC 설정 변경으로 취약점을 조치할 수 있으나, 대상 시스템에 따라 개발 변경이 필요한 경우가 존재하며, 개발업체의 협조 여부에 따라서 개발 변경이 어려울 수 있다. 개발 변경 가능 여부를 파악하여 취약점 조치 여부를 결정한다.

조치 시 영향	업무상 필요한 기능까지 제거하는 경우 정상적인 제어시스템 운영업무 어려움

제어시스템

CS-21 (중)	4. 보안관리 > 4.12 제어시스템 개선, 신규 시스템 도입, 패치 및 수정 시, 안정성을 테스트하기 위한 테스트베드 또는 시험환경을 구축하였는가?
취약점 개요	
점검내용	■ 제어시스템의 신규 구축 및 변경(개발수정, 업그레이드, 패치 포함) 전 안정성 테스트 등의 시험환경을 구축하는지 점검
점검목적	■ 제어시스템은 각 제어설비를 감시, 통제하기 위한 다양한 구성요소(HMI, PLC, RTU 등)를 포함하고 있고 해당 구성요소의 신규 구축, 변경 등에 따라서는 제어시스템의 일부 또는 전체의 오작동이 발생할 수 있기 때문에 시험환경을 구축하여 안정성을 검증한 뒤 신규 구축 및 변경 등을 적용하기 위함
보안위협	■ 안정성 검증 없이 신규 구축 및 변경 등을 적용하는 경우 제어시스템의 일부 또는 전체의 오작동 등의 피해 발생 가능
참고	※ 시험환경의 구축 고려사항 제어시스템은 IT와 기계적 요소가 결합된 구조를 이루고 있기 때문에 IT환경과 같이 이중화, 유지보수 시간 서비스 정지, 테스트서버 구축 등의 방법 적용이 어려울 수 있으므로 기계적 요소의 오작동 가능성을 시험할 수 있는 산업특성을 고려한 자체적인 방안을 수립하는 것이 필요
점검대상 및 판단기준	
대상	■ HMI(Human Machine Interface), PLC(Programmable Logic Controller), Data Historian 등의 제어시스템 운영 소프트웨어 ■ 제어시스템을 구성하는 RTU, 네트워크장비 등의 기기
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
점검 및 조치 사례	
Step 1) 제어시스템에 대한 신규 구축 또는 다음과 같은 변경 사례가 있는지 확인 - HMI, Data Historian 등의 소프트웨어 업그레이드 또는 패치 이력 - PLC, RTU, 네트워크장비 등의 기기 펌웨어(Firmware) 업그레이드 또는 패치 이력 - 신규 도입 시스템(서버, 네트워크장비, 보안장비 등) 및 기기 이력 Step 2) Step 1에 따른 시험환경 구축과 시험이 이루어지고 그 결과에 따른 신규 구축 또는 변경이 이루어졌는지 확인하되, 상시 운용 가능한 시험환경이 있다면 해당 환경을 실사하고 과거 이력만 있다면 당시 시험수행 결과보고(문건) 자료를 확인	
조치 시 영향	시험 수행 중 실 운영 중인 제어설비의 장애 발생

제어시스템

CS-22 (중)	4. 보안관리 > 4.13 제어 네트워크는 각각의 세부망으로 세분화하고 제어시스템 운영에 필요한 네트워크, 시스템 간으로 통신을 제한하고 있는가?
취약점 개요	
점검내용	■ 제어시스템을 구성하는 네트워크를 물리적 망분리, 서브넷(Subnet) 등의 방법으로 세분화(예: 제어망을 종류별로 구분하고 운영업무망과 행정업무망을 구분)하고 이에 따른 접근통제를 하는지 점검
점검목적	■ 제어시스템 및 운영조직의 규모에 따라서는 제어망, 업무망의 물리적 분리 이외에도 해당 네트워크 내부를 세분화하여 제어망 및 업무망 내에서의 접근통제를 강화하기 위함
보안위협	■ 단일 네트워크 내에 있는 모든 시스템, 기기에 대해 운영자의 임의 접근이 가능하거나 악성코드 감염에 따른 피해 확산 가능
참고	※ 제어망과 업무망의 중간지점(DMZ)을 고려한 네트워크 구성 예시 제어망과 업무망에서 함께 이용하는 Data Historian과 같은 시스템은 별도의 접근통제 정책을 적용하기 위해서 제어망 방화벽의 DMZ 구성 내에 위치하여 관리  [그림 출처] 美 ICS-CERT (https://ics-cert.us-cert.gov)
점검대상 및 판단기준	
대상	■ 제어시스템을 구성하는 네트워크 전체
판단기준	**양호:** 제어망 및 업무망 각각의 내부 네트워크를 세분화하여 구성하고 접근통제 규칙이 적용된 경우
	취약: 제어망 및 업무망 각각의 내부 네트워크를 단일 구성한 경우 (즉, 제어망과 업무망의 물리적 분리만 구성된 상태)
조치방법	제어망 및 업무망 각각의 내부 네트워크를 세분화하여 구성하고 세분화된 네트워크 간에 접근통제 규칙을 방화벽, 스위치 등을 통해 적용

CS-22 (중)	4. 보안관리 > 4.13 제어 네트워크는 각각의 세부망으로 세분화하고 제어시스템 운영에 필요한 네트워크, 시스템 간으로 통신을 제한하고 있는가?

점검 및 조치 사례

Step 1) 제어시스템 네트워크 전체 구성도와 제어망 및 업무망 내의 상세 네트워크 구성도(IP대역 포함)를 확인하되 다음 사항을 함께 점검
- 업무망이 단일 네트워크로 이루어지지 않고 업무 민감 정도에 따라 운영업무망, 행정업무망, 인터넷망 등으로 분리 구성
- 제어망이 단일 네트워크로 이루어지지 않고 제어설비의 구조에 따라 서브넷(Subnet) 구성
- IP대역을 분리, 구성한 장비(예: 방화벽, 스위치 등)에 설정된 접근통제 규칙

Step 2) Step 1에 따라 점검한 결과, 제어망 및 업무망을 세분화하여 네트워크 구성이 이루어졌고 분리 구성된 네트워크 간에 접근통제 규칙이 네트워크 장비 및 방화벽에 적절하게 적용되었는지 점검
- 이 부분의 실사방법 및 조치는 점검항목 C-14(상)의 점검 및 조치사항을 참조

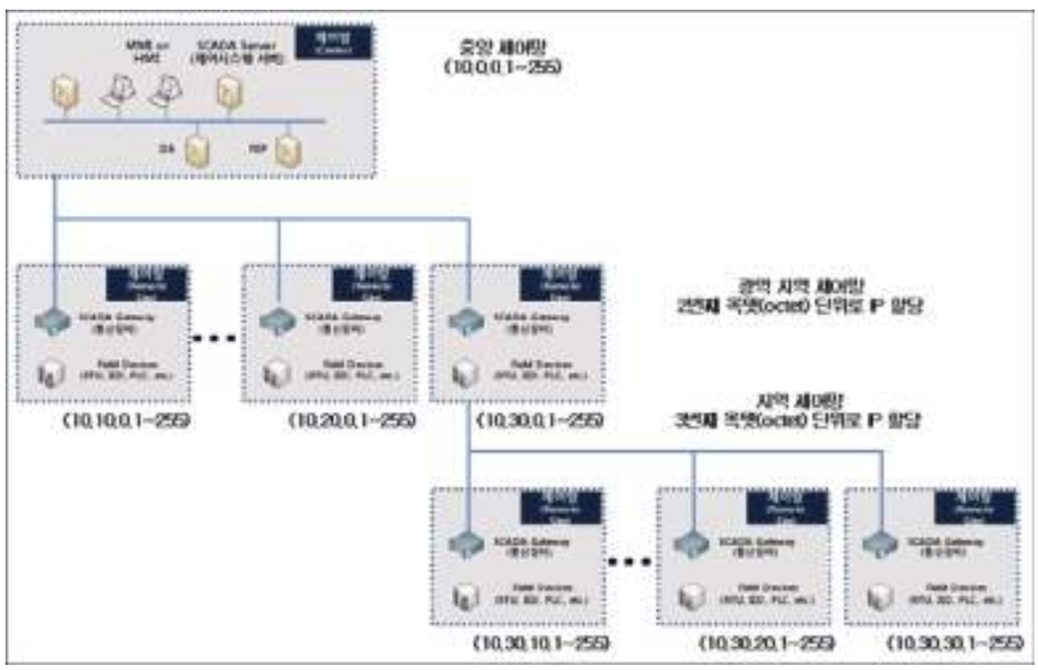
※ 네트워크 구성을 변경하는 것은 제어시스템 일부 또는 전체에 큰 영향을 준다. 즉 서브넷 구성 실수(예: IP주소 충돌 등)와 스위치 및 방화벽의 접근규칙 오류(예: 서브넷간의 IP차단)만으로 HMI 등의 모니터링 장애, 특정 제어설비에 제어명령 수신 오류 등의 발생 가능성이 높다. 따라서 점검항목 C-21(중)에 따른 시험환경 구축은 물론 긴급상황 발생시 복구 대책 등을 함께 고려한 뒤에 개선조치를 수행하는 것이 바람직하다.

※ 계층적으로 구성된 IP 체계 예시

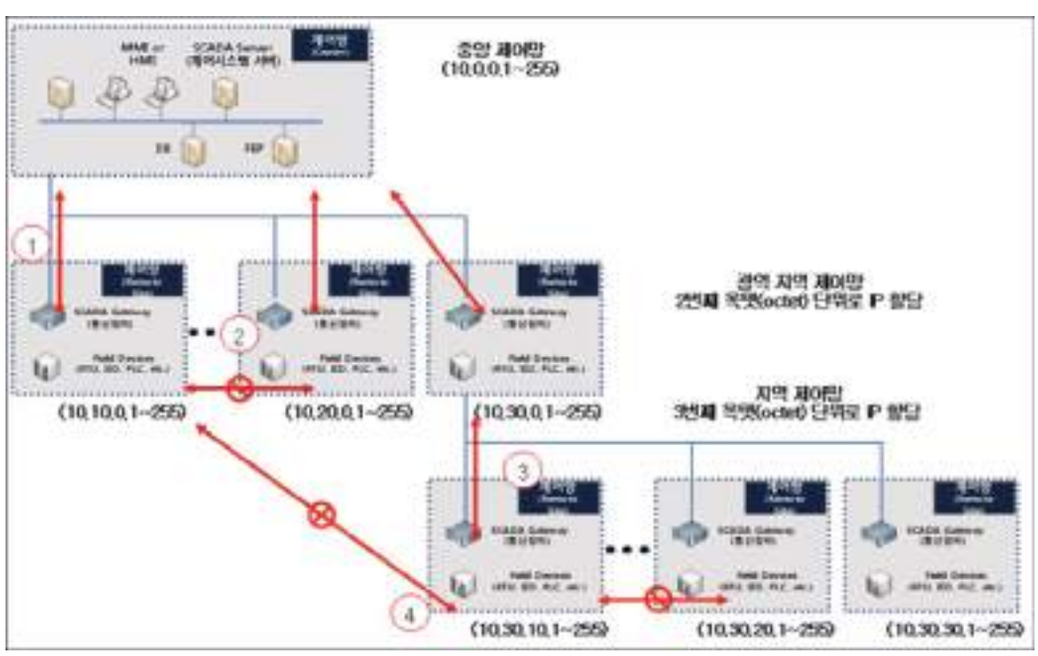
네트워크 단위		IP
중앙 제어 네트워크		10.0.0.1 ~ 255
광역 지역 제어 네트워크	광역 지역 제어 네트워크 1	10.10.0.1 ~ 255
	광역 지역 제어 네트워크 2	10.20.0.1 ~ 255
	광역 지역 제어 네트워크 3	10.30.0.1 ~ 255
지역 제어 네트워크	지역 제어 네트워크 1	10.30.10.1 ~ 255
	지역 제어 네트워크 2	10.30.20.1 ~ 255
	지역 제어 네트워크 3	10.30.30.1 ~ 255

제어시스템

CS-22 (중)	4. 보안관리 > 4.13 제어 네트워크는 각각의 세부망으로 세분화하고 제어시스템 운영에 필요한 네트워크, 시스템 간으로 통신을 제한하고 있는가?



※ 제어시스템 내부 네트워크 구성 및 접근통제 예시

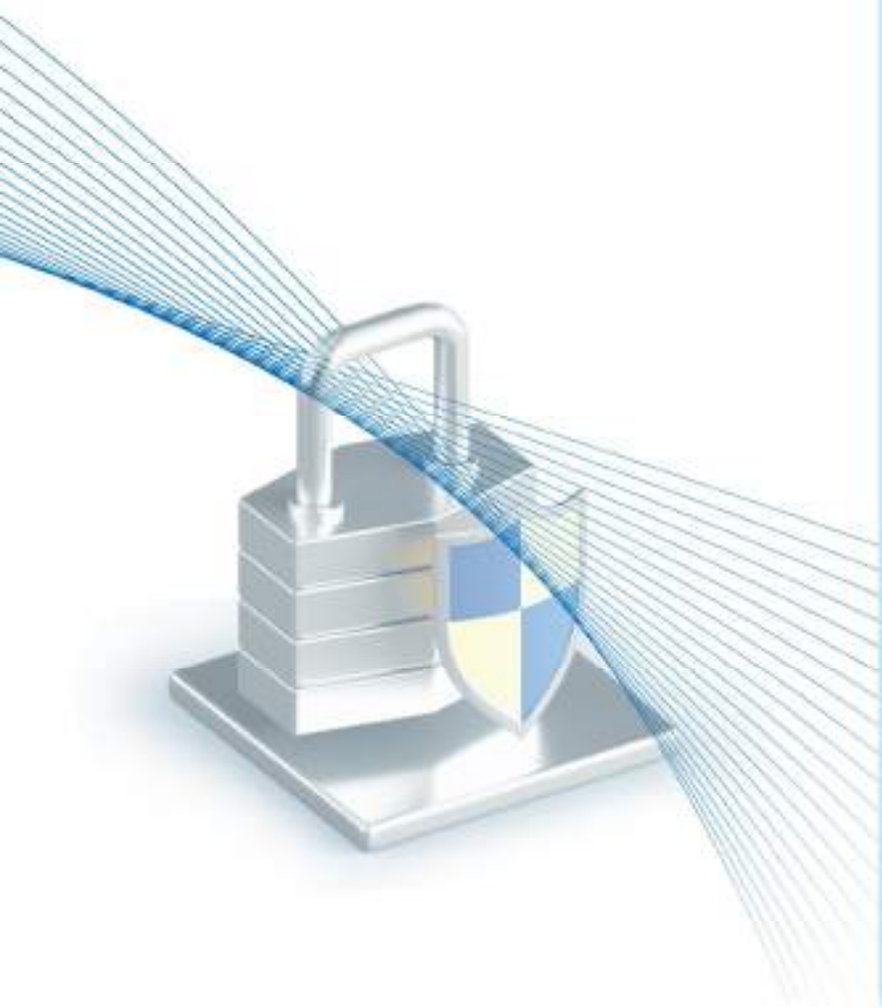


※ 내부 네트워크의 구성을 표준적으로 요구할 수는 없기 때문에 산업특성, 규모 등을 고려해 적절한 세분화가 이루어지는 확인하되, 국가정보원 "전자제어시스템 보안가이드" 3장 4절의 안전한 내부 네트워크 구성 내용을 고려하여 내부 네트워크를 세분화한다.

조치 시 영향	제어시스템, 설비 간의 오작동 또는 업무상 필요한 직무자임에도 제어시스템 접근 불가

Ⅱ

PC



PC 취약점 분석·평가 항목

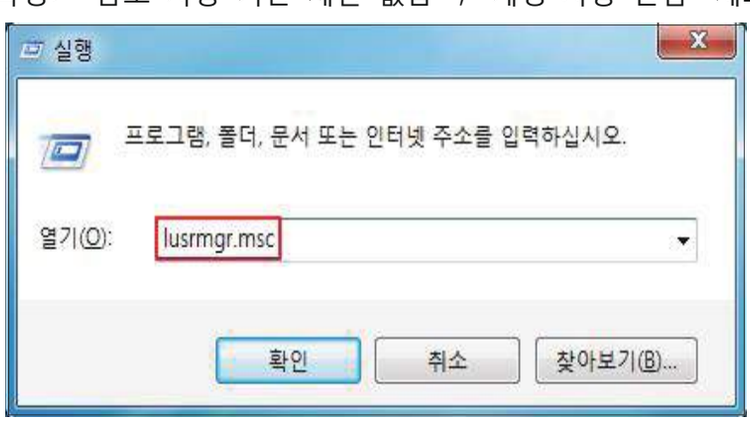
분류	점검항목	중요도	항목코드
1. 계정관리	패스워드의 주기적 변경	상	PC-01
	패스워드 정책이 해당 기관의 보안 정책에 적합하게 설정	상	PC-02
	복구 콘솔에서 자동 로그온을 금지하도록 설정하여 사용하고 있는가?	중	PC-15
2. 서비스관리	공유 폴더 제거	상	PC-03
	항목의 불필요한 서비스 제거	상	PC-04
	Windows Messenger(MSN, .NET 메신저 등)와 같은 상용메신저의 사용 금지	상	PC-05
	파일 시스템이 NTFS 포맷으로 되어 있는가?	중	PC-16
	대상 시스템이 Windows 서버를 제외한 다른 OS로 멀티부팅이 가능하지 않도록 설정하여 사용하는가?	중	PC-17
	브라우저 종료 시 임시 인터넷 파일 폴더의 내용을 삭제하도록 설정하여 사용하는가?	하	PC-18
3. 패치관리	HOT FIX 등 최신 보안패치 적용	상	PC-06
	최신 서비스팩 적용	상	PC-07
	MS-Office, 흔글, 어도비 아크로뱃 등의 응용 프로그램에 대한 최신 보안패치 및 벤더 권고사항 적용	상	PC-08
4. 보안관리	바이러스 백신 프로그램 설치 및 주기적 업데이트	상	PC-09
	바이러스 백신 프로그램에서 제공하는 실시간 감시 기능 활성화	상	PC-10
	OS에서 제공하는 침입차단 기능 활성화	상	PC-11
	화면보호기 대기 시간 설정 및 재시작 시 암호 보호 설정	상	PC-12
	CD, DVD, USB 메모리 등과 같은 미디어의 자동실행 방지 등 이동식 미디어에 대한 보안대책 수립	상	PC-13
	PC 내부의 미사용(3개월) ActiveX 제거	상	PC-14
	시스템 부팅 시 Windows Messenger가 자동으로 시작되지 않도록 설정되어 있는가?	중	PC-19
	원격 지원을 금지하도록 정책이 설정되어 있는가?	중	PC-20

PC

PC-01 (상)	1. 계정관리 > 1.1 패스워드의 주기적 변경
취약점 개요	
점검내용	■ 최대 암호 사용 기간이 "90일" 이하로 설정되어 있는지 점검
점검목적	■ 패스워드를 주기적으로 변경하여 암호 크래킹의 가능성을 낮추고, 불법으로 획득한 암호의 무단 사용을 방지하고자 함
보안위협	■ 동일한 패스워드를 변경하지 않고 오랫동안 사용할 경우 유출이나 무차별 대입공격에 당할 가능성이 높고 이전에 사용하던 패스워드를 재사용한다면 비밀번호 추측 공격에 의해 계정을 탈취당할 우려가 있음
참고	-
점검대상 및 판단기준	
대상	■ Windows XP, Windows 7, Windows 8.1, Windows 10
판단기준	**양호 :** 최대 암호 사용 기간이 "90일"이하로 설정되어 있는 경우
	취약 : 암호 사용 기간이 "제한 없음"이거나 "90일"을 초과하여 설정되어 있는 경우
조치방법	최대 암호 사용 기간 "90일" 설정 최소 암호 사용 기간 "1일" 설정 최근 암호 기억 설정 (권장 : 24개의 암호 기억) ※ 사용자가 새 암호를 변경하기 전에 이를 유지해야 하는 일수를 결정. 암호 변경 후 편의성 때문에 기존 암호로 다시 설정하는 경우가 많기 때문에 최소 사용 기간을 설정 ※ 이전 암호를 다시 사용한다면 변경 주기가 의미가 없기 때문에 기존에 사용하던 암호를 기억해서 사용하지 못하게 함.
점검 및 조치 사례	

■ **Windows XP, Windows 7, Windows 8.1, Windows 10**

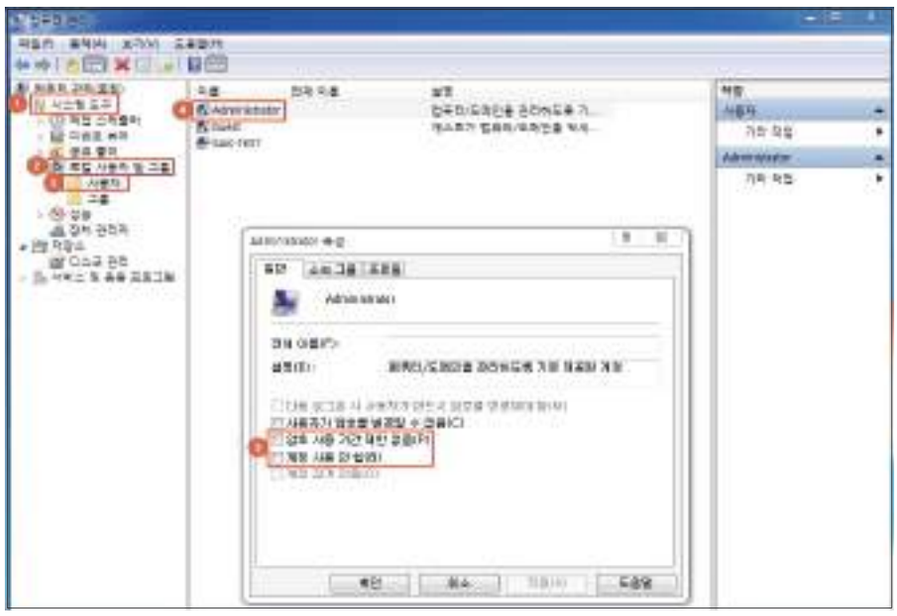
Step 1) 윈도우키+영문자R 키 입력> 실행> "lusrmgr.msc" 입력> 사용자> Administrator 우클릭> 속성> "암호 사용 기간 제한 없음" , "계정 사용 안함" 체크 해제



[실행창 > Lusrmgr.msc 입력]

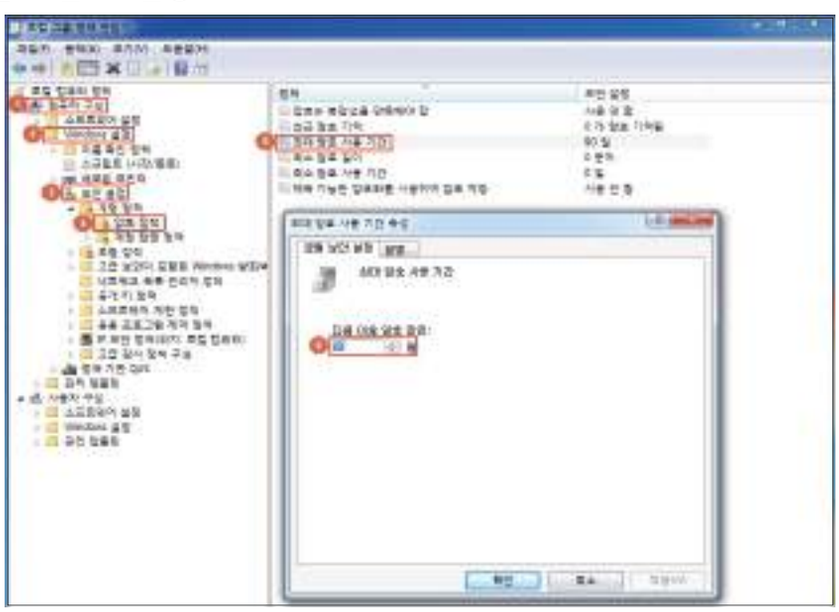
PC

PC-01 (상)	1. 계정관리 > 1.1 패스워드의 주기적 변경



[암호 사용 기간 제한 없음, 계정 사용 안함 체크 해제]

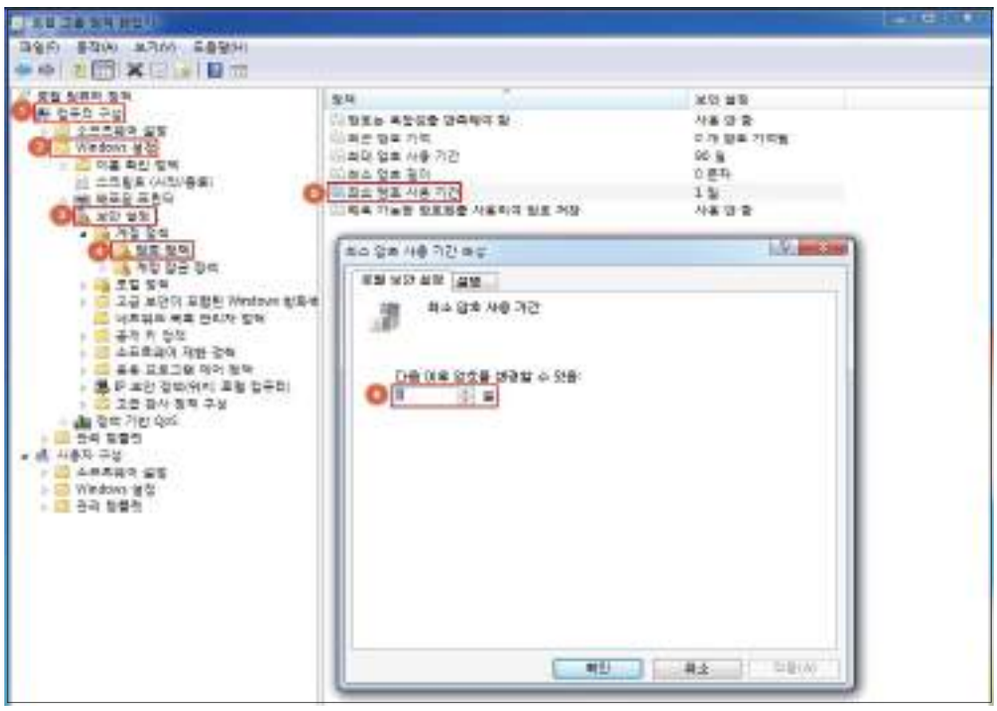
Step 2) 제어판> 관리 도구> 로컬 보안 정책> 보안 설정> 계정 정책> 암호 정책
(윈도우키+영문자R 키 입력 > 실행> "gpedit.msc" 입력> 컴퓨터 구성> Windows 설정> 보안 설정> 계정 정책> 암호 설정)
"최대 암호 사용 기간" 속성을 "90일" , "최근 암호 기억"을 "24개" , "최소 암호 사용 기간"을 "1일"로 설정



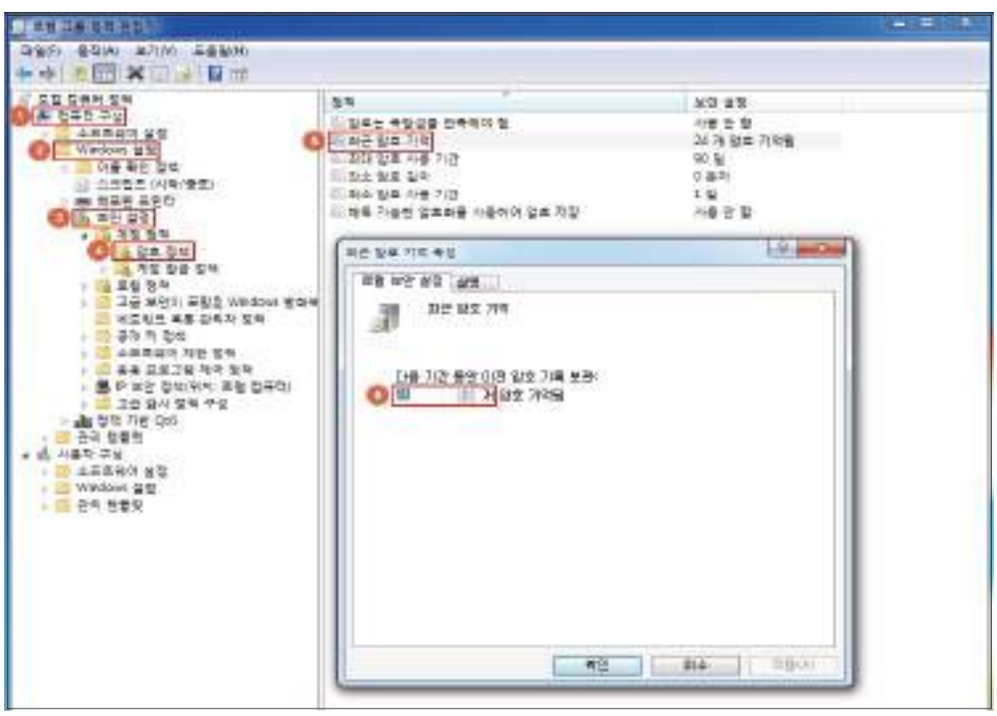
[최대 암호 사용 기간 90일 설정]

PC

PC-01 (상)	1. 계정관리 > 1.1 패스워드의 주기적 변경



[최소 암호 사용 기간을 1일로 설정]



[최근 암호 기억을 24개로 설정]

조치 시 영향	패스워드 변경 시 기존 사용했던 암호를 재사용 할 수 없음.

PC

PC-02 (상)	1. 계정관리 > 1.2 패스워드 정책이 해당 기관의 보안 정책에 적합하게 설정
취약점 개요	
점검내용	■ 최소 암호 길이가 보안 정책을 반영하여 설정되어 있는지 점검
점검목적	■ 안전한 패스워드(*패스워드 설정 기준 참조)를 사용함으로써 무작위 대입 공격, 사전공격 등 패스워드 탈취 목적의 공격에 대한 대비를 목적으로 함
보안위협	■ 무작위 대입 공격, 패스워드 추측 공격 등 패스워드가 비교적 단순하거나 비교적 자주 쓰이는 패스워드(예:P@ssw0rd 등)로 비인가 접근을 시도하는 공격들이 존재함
참고	※ **무작위 대입 공격(Brute Force Attack):** 컴퓨터로 암호를 해독하기 위해 가능한 모든 키를 하나하나 추론해 보는 시도 ※ **사전 공격(Dictionary attack):** 사전에 있는 단어를 입력하여 암호를 알아내거나 해독하는 컴퓨터 공격법
점검대상 및 판단기준	
대상	■ Windows XP, Windows 7, Windows 8.1, Windows 10
판단기준	**양호 :** 최소 암호 길이가 해당 기관의 보안 정책을 반영하여 설정되어 있는 경우
	취약 : 암호를 사용하지 않거나, 추측하기 쉬운 문자조합으로 이루어진 짧은 자릿수의 패스워드를 사용하는 경우
조치방법	최소 암호 길이를 해당 기관의 보안 정책에 적합하게 설정
점검 및 조치 사례	

■ **Windows XP, Windows 7, Windows 8.1, Windows 10**

< 패스워드 설정 기준 >

1. 영문, 숫자, 특수문자를 조합하여 계정명과 상이한 8자 이상의 패스워드 설정
   ※ 다음 각 항목의 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. 패스워드는 비인가자에 의한 추측이 어렵도록 다음의 사항을 반영하여 설계
   (1) Null(공백) 패스워드 사용 금지
   (2) 문자 또는 숫자만으로 구성 금지
   (3) 사용자 ID와 동일하거나 유사하지 않은 패스워드 금지
   (4) 연속적인 문자나 숫자 사용 (예) 1111, 1234, abcd) 사용 금지

PC

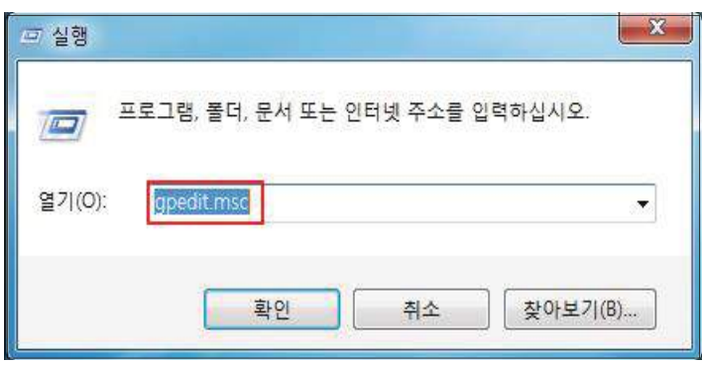
PC-02 (상)	1. 계정관리 > 1.2 패스워드 정책이 해당 기관의 보안 정책에 적합하게 설정

(5) 주기성 패스워드 재사용 금지
(6) 전화번호, 생일과 같이 추측하기 쉬운 개인정보를 패스워드로 사용 금지

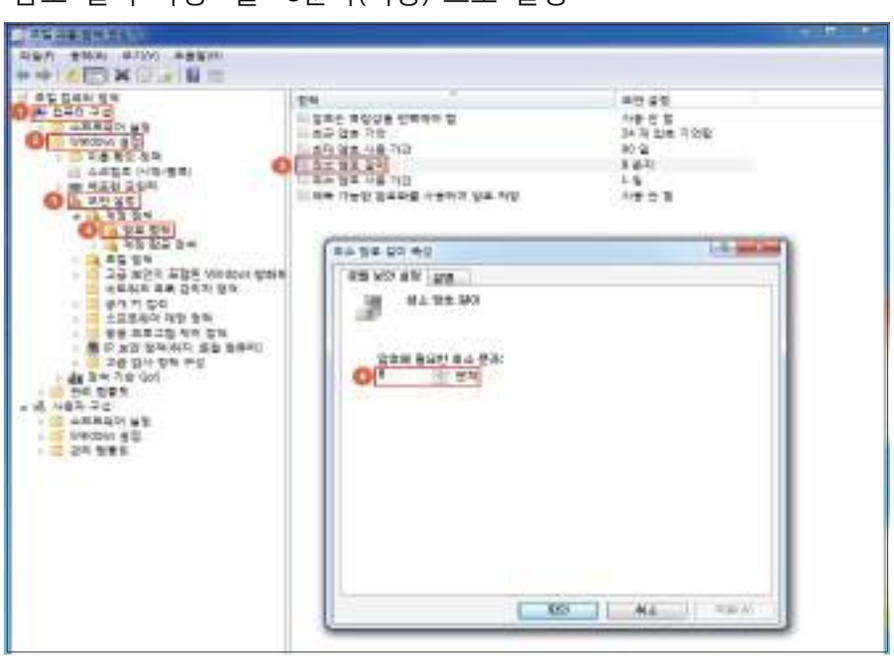
3. SAM파일에 암호를 저장하기 위해 사용되는 LANMan 알고리즘은 8자 단위로 글자를 나누어 암호화하기 때문에 8의 배수가 되는 암호 사용 권장 (8자로 이루어진 암호 사용 권장)

4. 아래와 같은 암호 설정 지양
Null, 계정과 동일하거나 유사한 스트링, 지역명, 부서명, 담당자명, 대표 업무명 “root”, “rootroot”, “root123”, “123root”, “admin”, “admin123”, “123admin”, “osadmin”, “adminos”

Step 1) 제어판> 관리 도구> 로컬 보안 정책> 보안 설정> 계정 정책> 암호 정책
(윈도우키+영문자R 키 입력 > 실행 > “gpedit.msc” 입력> 컴퓨터 구성> Windows 설정> 보안 설정> 계정 정책> 암호 설정)



Step 2)"최소 암호 길이 속성" 을 "8문자(이상)"으로 설정



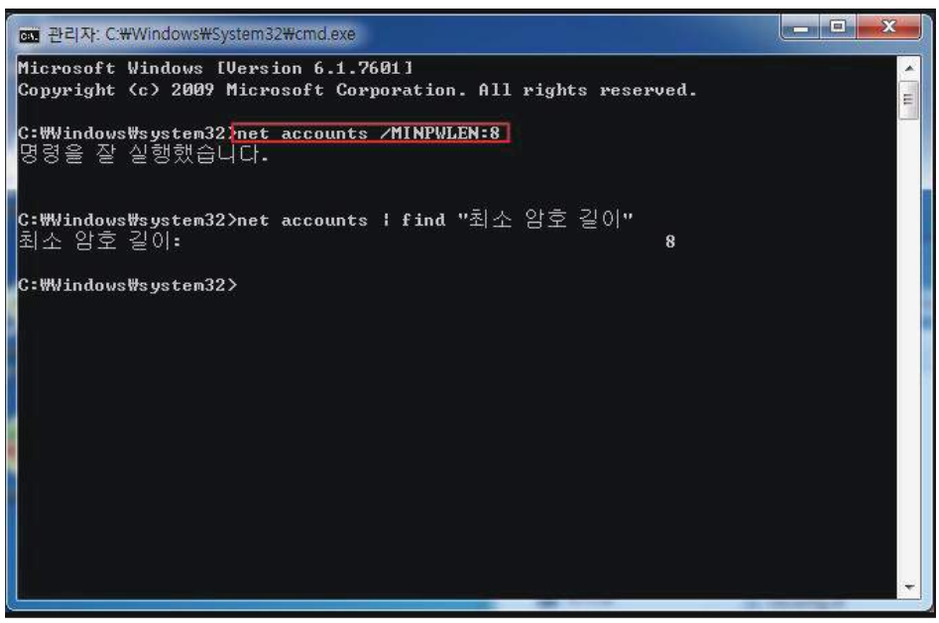
PC

PC

PC-02 (상)	1. 계정관리 > 1.2 패스워드 정책이 해당 기관의 보안 정책에 적합하게 설정

Step3) 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
- Windows 8 : 시작> 실행> "cmd" 입력> "net accounts /MINPWLEN:8" 입력
- Windows 10 : 시작> 실행> "cmd" 입력> "net accounts /MINPWLEN:8" 입력



조치 시 영향	일반적인 경우 영향 없음

PC

PC-03 (상)	2. 서비스 관리 > 2.1 공유폴더 제거
취약점 개요	
점검내용	■ 기본 공유 폴더(C$, D$, Admin$), 미사용 공유폴더가 존재하는지 점검하고 공유 폴더를 사용하는 경우 공유 폴더 접근 권한에 "Everyone"이 존재하거나 접근을 위한 암호가 설정되어 있는지 점검
점검목적	■ 사용하지 않는 불필요한 공유 폴더를 해제하거나 불가피하게 사용하고 있는 공유폴더의 경우 암호를 설정하는 등의 조치를 통해 인가된 사용자만 접근이 가능하게 함으로써 무분별한 접근을 제한함
보안위협	■ 시스템 기본 공유 폴더의 경우 기본 드라이브를 개방해놓고 사용하는 것과 동일함(예 : 실행창 -> ₩₩192.168.16.xxx₩c$ 으로 C드라이브 접근 가능) ■ 접근권한이 Everyone으로 설정된 공유 폴더는 정보 유출 및 악성코드 유포의 접점이 될 수 있음
참고	-
점검대상 및 판단기준	
대상	■ Windows XP, Windows 7, Windows 8.1, Windows 10
판단기준	**양호 :** 불필요한 공유 폴더가 존재하지 않거나 공유폴더에 접근권한 및 암호가 설정되어있는 경우
	취약 : 불필요한 공유 폴더가 존재하거나 접근권한 및 암호 설정 없이 공유폴더를 사용하는 경우
조치방법	공유 폴더 불필요 시 삭제 공유 폴더 필요 시 적절한 접근권한 부여 및 암호 설정 조치 후 AutoShareServer(또는, AutoShareWks)값 변경으로 자동 공유 방지
점검 및 조치 사례	
< 공유 폴더 설정 기준 > 1. C$, D$, Admin$ 등의 기본 공유 폴더 제거 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 3. 일반 공유 폴더 사용 시 공유 폴더 접근 권한에 "Everyone" 제거 4. 일반 공유 폴더 사용 시 접근이 필요한 계정에만 적절한 (읽기, 변경)권한 설정 5. 일반 공유 폴더 사용 시 공유 폴더 접근을 위한 암호 설정	

PC

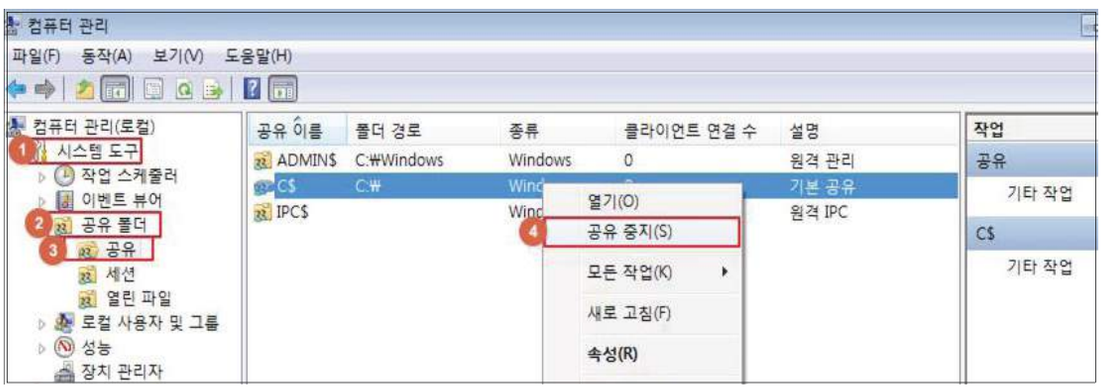
PC-03 (상)	2. 서비스 관리 > 2.1 공유폴더 제거

■ **Windows XP, Windows 7, Windows 8.1, Windows 10**

- **기본 공유 폴더 상태 확인 및 공유 중지**

Step 1)

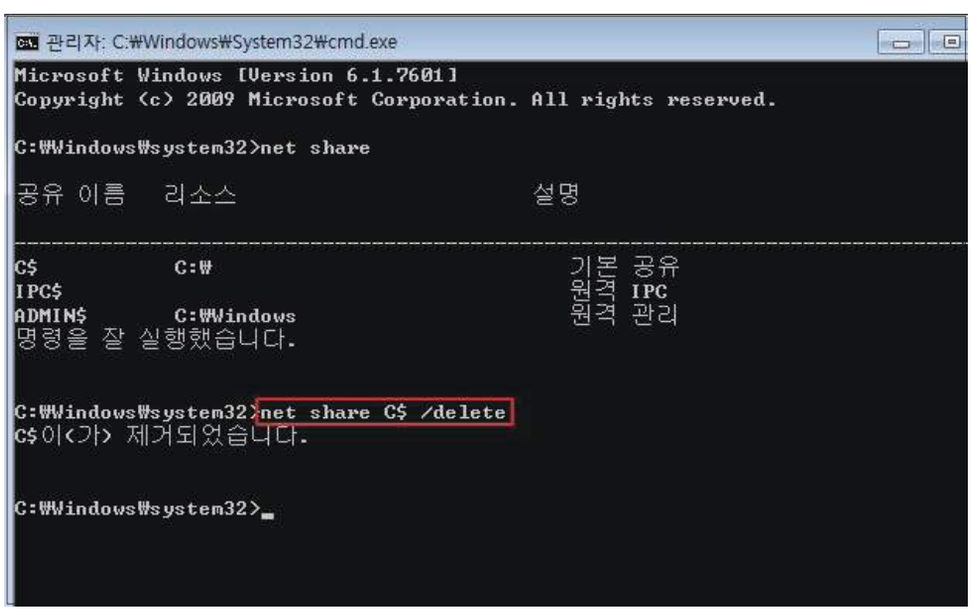
1. 제어판> 관리 도구> 컴퓨터 관리> 공유 폴더> 공유
   (시작> 실행> "fsmgmt.msc" 입력> 공유)
2. 불필요한 공유 폴더 확인> 해당 공유 폴더 우클릭> 공유 중지



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
   - Windows 8.1 : 관리자 권한으로 "cmd.exe" 실행 후 "net share" 입력
   - Windows 10 : 관리자 권한으로 "cmd.exe" 실행 후 "net share" 입력

   C:\net share 명령을 통해 공유 디렉터리 확인

   C:\net share "삭제할 공유 폴더명" / delete 명령을 통해 공유 디렉터리 삭제



PC

PC-03 (상)	2. 서비스 관리 > 2.1 공유폴더 제거

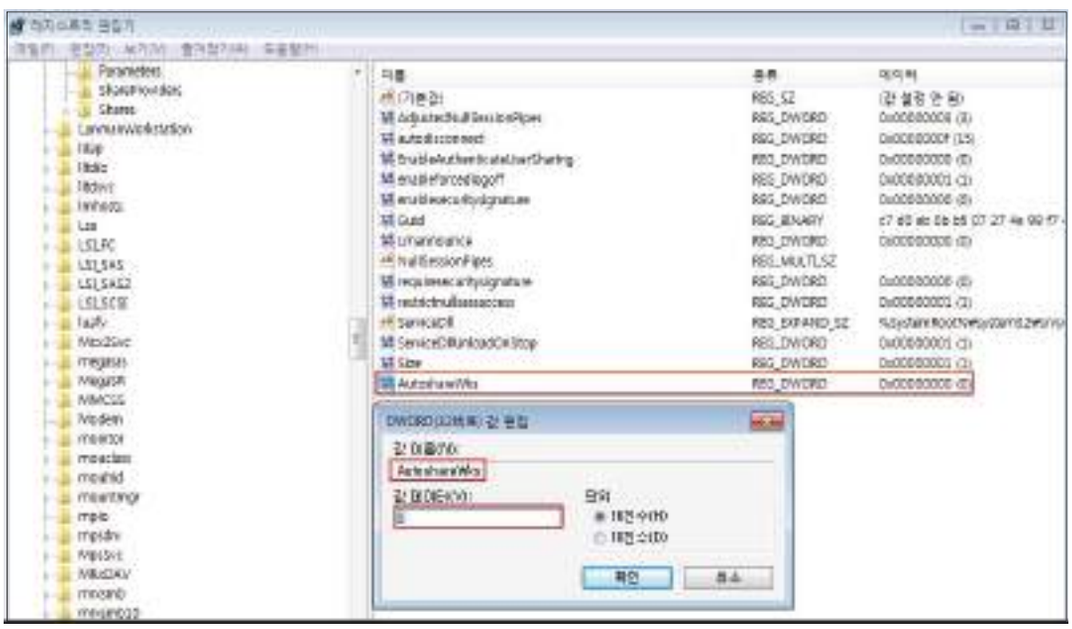
- 시스템 재부팅 후 기본 공유 폴더 자동 공유 방지 설정

  Step 1) 시작> 실행> "regedit" 입력

  Step 2) 레지스트리 경로

  HKLM\System\CurrentControlSet\Services\LanmanServer\Parameters

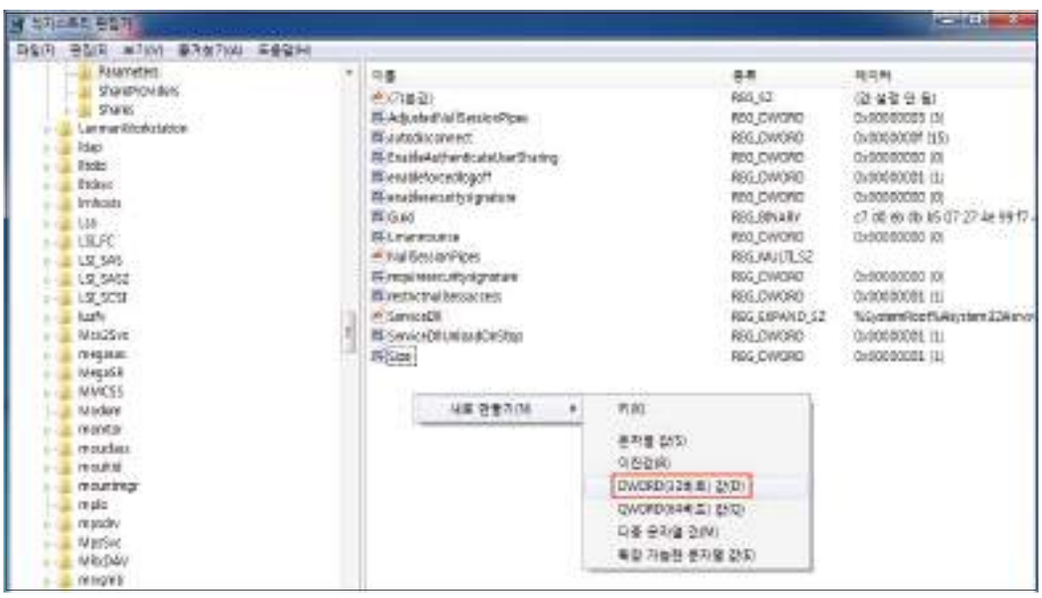
  Step 3) 설정 값 입력



  Step 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 보안성을 높일 수 있음



PC

PC-03 (상)	2. 서비스 관리 > 2.1 공유폴더 제거

※ 기본 공유에 대한 조치 시 반드시 [기본 공유 삭제], [비활성화 레지스트리 값]을 모두 설정함

- 일반 공유 폴더 확인 및 공유 중지

  Step 1) 제어판> 관리 도구> 컴퓨터 관리> 공유 폴더> 공유

  (시작> 실행> "fsmgmt.msc" 입력> 공유)

  Step 2) 불필요한 공유 폴더 확인> 해당 공유 폴더 우클릭> 공유 중지

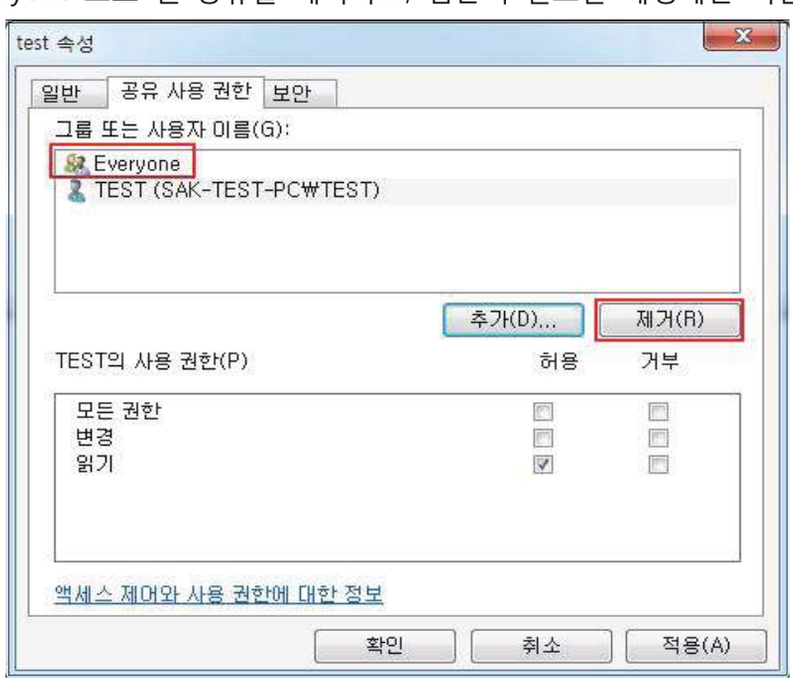
- 일반 공유 폴더 필요 시 권한 설정

  Step 1) 제어판> 관리 도구> 컴퓨터 관리> 공유 폴더> 공유

  (시작> 실행> "fsmgmt.msc" 입력> 공유)

  Step 2) 사용할 공유 폴더 확인 선택 후 우클릭> 속성> [공유] 탭> [공유 사용 권한] 탭

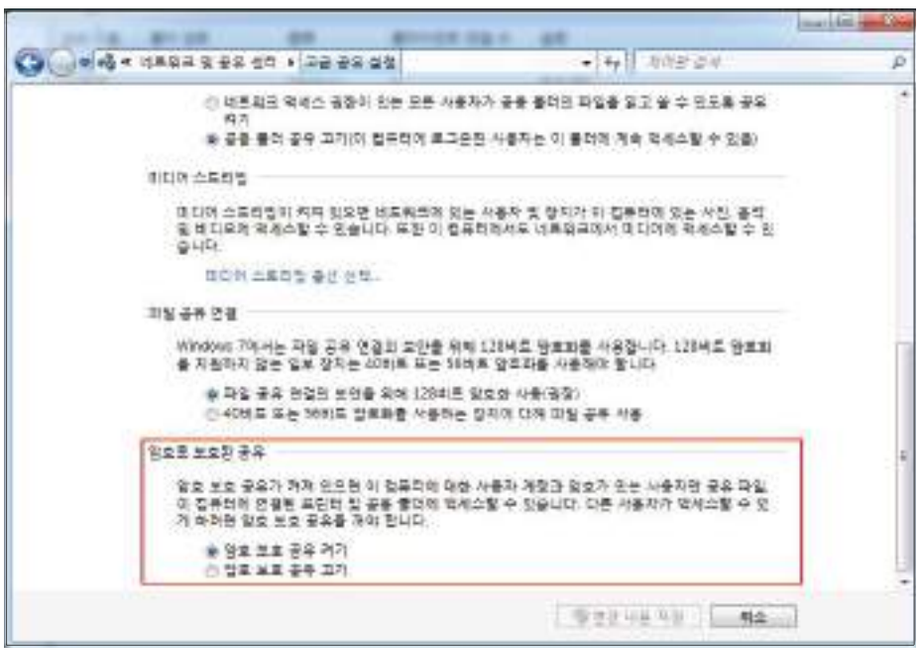
  "Everyone"으로 된 공유를 제거하고, 접근이 필요한 계정에만 적절한 권한 추가



PC

PC-03 (상)	2. 서비스 관리 > 2.1 공유폴더 제거

- 공유 폴더 접근 암호 설정
  Step 1) 제어판> 네트워크 및 공유 센터> 고급 공유 설정



  Step 2) "암호 보호 공유 켜기" 설정
  Step 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	일반적인 경우 영향 없음

PC

PC-04 (상)	2. 서비스 관리 > 2.2 불필요한 서비스 제거
취약점 개요	
점검내용	■ 사용하지 않는 서비스나 디폴트로 설치되어 실행되고 있는 서비스가 있는지 점검
점검목적	■ 사용하지 않는 서비스나 디폴트로 설치된 서비스들을 제거하여 시스템 자원의 낭비를 막고 해당 서비스 포트를 통한 침입을 방지
보안위협	■ 실질적으로 사용하지 않는 서비스들이 실행되어 시스템에 과부하가 발생함 ■ 불필요한 서비스의 경우 사용자가 알지도 못한 서비스들이 실행되고 있는 경우가 대부분, 이 경우 해당 서비스가 이미 취약한 버전의 서비스인지도 인지하지 못하고 사용함
참고	■ 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 ■ 시스템 관리자는 대상 시스템의 용도를 정확히 파악한 후 특별한 목적으로 사용하는 업무 관련 서비스를 제외한 다른 불필요한 서비스를 제거하여야 함 ※ OS 버전에 따라 '일반적으로 불필요한 서비스' 목록에 나열된 서비스가 제공되지 않을 수 있음
점검대상 및 판단기준	
대상	■ Windows XP, Windows 7, Windows 8.1, Windows 10
판단기준	**양호 :** 일반적으로 불필요한 서비스(아래 목록 참조)가 중지되어 있는 경우
	취약 : 일반적으로 불필요한 서비스(아래 목록 참조)가 구동 중인 경우
조치방법	불필요한 서비스 중지
점검 및 조치 사례	

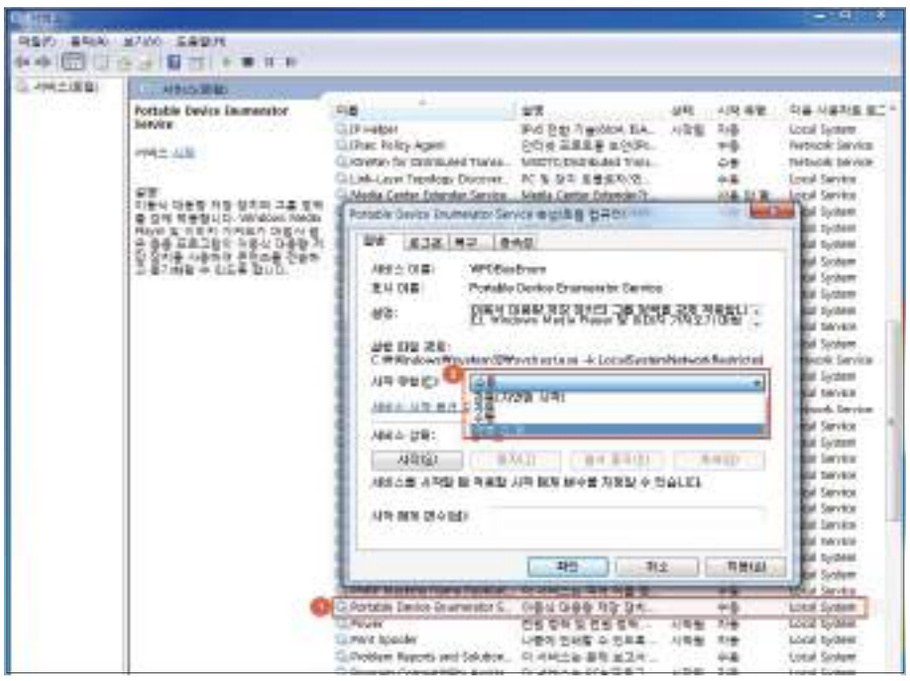
■ **Windows XP, Windows 7, Windows 8.1, Windows 10**

Step 1) 제어판> 관리 도구> 서비스> 해당 서비스 선택> 속성
(시작> 실행> "services.msc" 입력> 해당 서비스 선택> 속성)

Step 2) 불필요한 서비스 -> 중지 / 시작 유형 -> 사용 안 함

PC

PC-04 (상)	2. 서비스 관리 > 2.2 불필요한 서비스 제거



Step 3) 각 서비스마다 옵션을 설정할 수 있음
해당 서비스를 선택하고 더블 클릭하여 "시작 유형" 선택 및 "시작 시 로그온 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 해당 기능을 필요로 할 때만 시작됨
자동	부팅 시에 해당 장치 드라이버가 로드된 후에 운영체제에 의해 시작됨

※ 꼭 필요한 서비스만 사용하고 나머지는 "사용 안 함"으로 설정
※ 개인 방화벽 실행
※ 백신 등에서 제공하는 방화벽 기능 활성화 사용

※ 일반적으로 불필요한 서비스

서비스명	기능 및 설명
Alerter	네트워크상에서 사용자와 컴퓨터에 관리용 경고메시지를 전송하는 기능
Automatic Updates	중요한 윈도우 업데이트를 다운로드하고 설치할 수 있도록 하는 애플리케이션. 수동패치를 적용하거나, MS패치 관리 서버로 패치를 일괄적으로 관리하는 경우 불필요한 서비스
Clipbook	서버 내 Clipbook을 다른 클라이언트와 공유
Computer Browser	네트워크에 있는 모든 컴퓨터의 목록을 업데이트하고 관리하는 기능
Cryptographic Services	윈도우 파일의 서명을 확인하는 카탈로그 데이터베이스 서비스를 총괄

PC

PC-04 (상)	2. 서비스 관리 > 2.2 불필요한 서비스 제거

DHCP Client	IP 주소와 DNS 이름을 DHCP 서버에 등록하거나 DHCP 서버로부터 동적으로 IP주소를 가져오는 기능을 수행. 단독으로 시스템을 수행하며 고정IP를 사용하는 경우 불필요한 서비스
Distributed Link Tracking Client, Server	네트워크 도메인의 여러 컴퓨터나 일반컴퓨터에서 NTFS 파일간의 연결을 관리하는 도구. Active Directory가 구성되어 있지 않은 서버에서는 불필요한 서비스
DNS Client	컴퓨터에 대한 도메인 이름 시스템(DNS)이름을 확인하고 캐시에 보관하는기능. DNS서버가 아닌 시스템에서는 유명무실하나, IPSEC을 사용하는 경우 필요한 경우 있음
Error reporting Service	프로그램 오류가 시 응용프로그램의 오류를 MS에 보고한다는 내용을 표시하는 기능
Human Interface Device Access	키보드 또는 기타 멀티미디어 장치에 사전 정의된 버튼들을 사용하는 HID장치들을 위한 서비스
IMAPI CD-Burning COM Service	서버에 CD-RW 또는 DVD-RW가 장착되어 보조백업장치 역할을 하기 위해서 자체 레코딩 백업을 할 수 있음
Infrared Monitor	사용자 적외선 연결을 통해 파일 및 이미지를 공유할 수 있도록 함
Messenger	클라이언트와 서버 사이에 netsend 및 경고서비스 메시지를 전송하는 기능
NetMeeting Remote Desktop Sharing	윈도우9X 운영체제부터 인증된 사용자가 넷미팅을 사용해서 원격으로 컴퓨터에 접근할 수 있도록 하는 기능
Portable Media Serial Number	컴퓨터에 연결된 이동성 음악연주기(미디기기)의 등록번호를 복원하는 기능
Print Spooler	인쇄 과정에 있는 스풀링을 관리하는 서비스. 프린터가 있는 경우 필수 서비스이나, 프린터가 연결되지 않은 시스템에서는 불필요함
Remote Registry	원격 사용자가 이 컴퓨터에서 레지스트리 설정을 수정할 수 있도록 설정하는 애플리케이션
Simple TCP/IP Services	Echo, Discard, Character Generator, Daytime, Quote of the Day 지원
Universal Plug and Play Device Host	네트워크 장치에 대해 피어-투-피어 UPnP(범용 플러그 앤 플레이) 기능을 지원
Wireless Zero Configuration	802.11 어댑터에 대해 자동 구성을 공급하는 기본적인 도구

운영 중인 시스템에서 필수 서비스를 정의하는 것은 매우 복잡한 과정으로 서비스 사용 여부는 시스템의 영향성을 고려하여 신중하게 평가되어야 하므로 Microsoft에서 권고하는 가이드에 따라 전략적으로 적용하여야 함

※ https://technet.microsoft.com/ko-kr/library/dd547941.aspx (서비스 및 서비스 계정 보안 계획 가이드) 참고
윈도우 시스템 설치 시 기본적으로 설치되는 서비스에 대한 상세 설명은 아래 주소 참조
https://technet.microsoft.com/ko-kr/library/dd547949.aspx

조치 시 영향	일반적인 경우 영향 없음

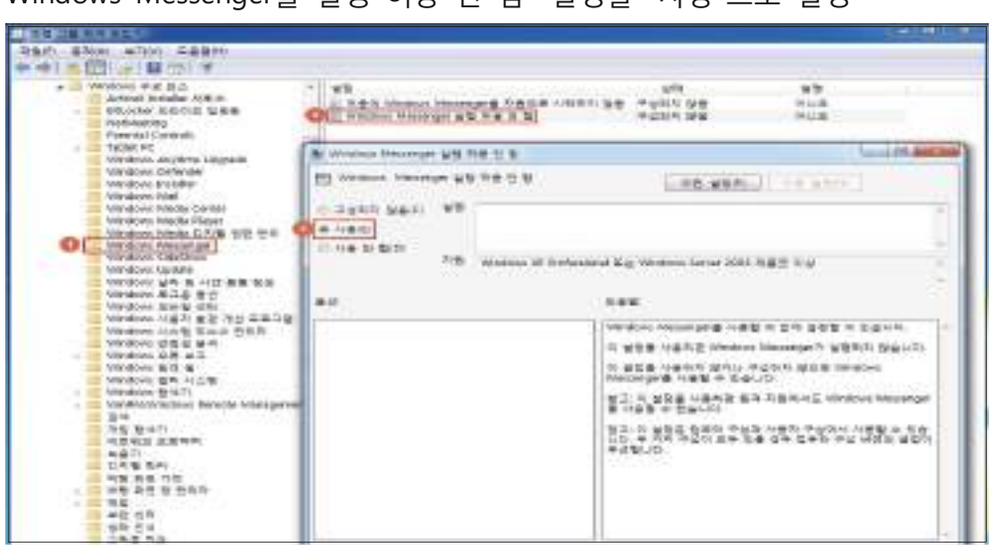
PC

PC-05 (상)	2. 서비스 관리 > 2.3 Windows Messenger(MSN, .NET 메신저 등)와 같은 상용 메신저의 사용 금지
취약점 개요	
점검내용	■ 사용자 PC에서 상용 메신저를 사용하고 있는지를 점검
점검목적	■ 상용 메신저 차단을 통하여 메신저를 이용한 개인정보 및 내부 주요 정보 유출을 막기 위함
보안위협	■ 일반 사용자 PC에서 메신저 차단을 하지 않을 경우, 메신저를 통해 주요 정보가 유출되거나, 악성코드가 유입될 가능성이 있음
참고	※ **메신저(Messenger):** 인터넷을 통해 실시간으로 대화를 나눌 수 있는 서비스. ※ **악성코드:** 컴퓨터에 악영향을 끼칠 수 있는 모든 소프트웨어의 총칭 ※ **상용메신저:** 네이트온, 카카오톡 PC 버전, skype 같은 메신저 프로그램
점검대상 및 판단기준	
대상	■ Windows XP, Windows 7, Windows 8.1, Windows 10
판단기준	**양호 :** Windows Messenger가 실행 중지된 상태이거나 상용 메신저가 설치되지 않은 경우
	취약 : Windows Messenger가 실행 중이거나 상용 메신저가 설치되어 있는 경우
조치방법	"Windows Messenger를 실행하지 않음" 설정 및 상용 메신저 삭제
점검 및 조치 사례	

■ **Windows XP, Windows 7, Windows 8.1, Windows 10**

Step 1) 시작> 실행> "gpedit.msc" 입력> 컴퓨터 구성> 관리 템플릿> Windows 구성 요소> Windows Messenger

Step 2) "Windows Messenger를 실행 허용 안 함" 설정을 "사용"으로 설정



PC

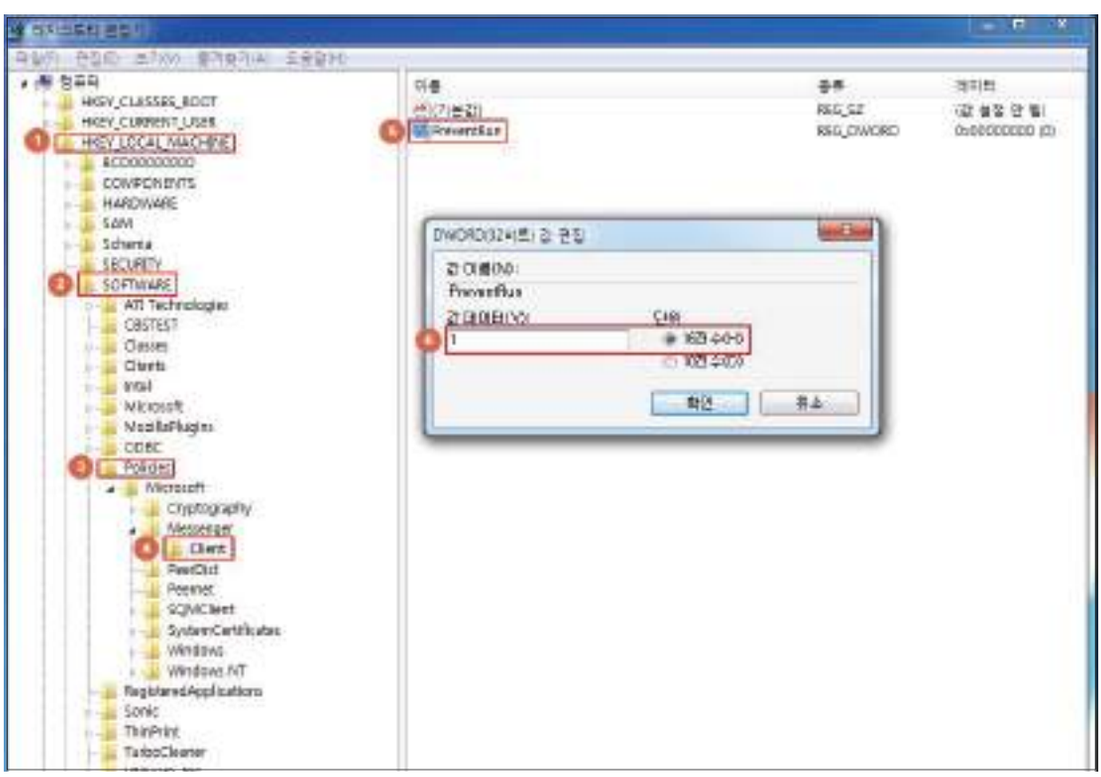
PC-05 (상)	2. 서비스 관리 > 2.3 Windows Messenger(MSN, .NET 메신저 등)와 같은 상용 메신저의 사용 금지

Step 3) 레지스트리 값으로 설정하는 방법

1. 시작> 실행> "regedit" 입력
2. 레지스트리 경로
   HKLM\Software\Policies\Microsoft\Messenger\Client
3. 설정 값 입력

Value name	PreventRun
Data Type	DWORD 값
Value	1 ※ 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

PC-05 (상)	2. 서비스 관리 > 2.3 Windows Messenger(MSN, .NET 메신저 등)와 같은 상용 메신저의 사용 금지

Step 4) 제어판 > 프로그램 및 기능에서 상용 메신저가 설치되어 있는지 확인 후 삭제

조치 시 영향	Windows Messenger 사용 불가 원격 지원에서도 Windows Messenger를 사용할 수 없음

PC

PC-06 (상)	3. 패치 관리 > 3.1 HOT FIX 등 최신 보안패치 적용
취약점 개요	
점검내용	■ 시스템에 관련한 공개된 취약점에 대한 최신 보안패치를 적용하였는지 점검
점검목적	■ 공개된 취약점을 통한 침해사고 발생을 방지하기 위함
보안위협	■ HOT Fix 및 최신 보안패치 적용을 시키지 않을 경우, 이미 공개된 취약점을 통하여 비인가자의 시스템 접근 및 관리자 권한 획득이 가능해짐
참고	※ **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 ※ **업데이트(Update):** 문제를 예방 또는 해결하거나 컴퓨터 작동 방식을 향상시키거나 컴퓨팅 경험을 향상시킬 수 있도록 추가되는 소프트웨어를 말함 ※ **https://technet.microsoft.com/ko-kr/security/advisory:** 게시 또는 업데이트된 모든 보안 권고 내용을 설명한 웹페이지
점검대상 및 판단기준	
대상	■ Windows XP, Windows 7, Windows 8.1, Windows 10
판단기준	**양호 :** HOT FIX 설치 및 자동 업데이트 설정이 되어 있고 내부적으로 관리 절차를 수립하여 이행하고 있는 경우
	취약 : HOT FIX가 설치되어 있지 않거나 내부적으로 관리 절차가 수립되어 있지 않은 경우
조치방법	Windows Update 사이트에 접속하여 최신 패치 존재 여부 확인 및 패치 적용
점검 및 조치 사례	
■ **Windows XP** Step 1) 인터넷에 연결되는 경우 Windows Update 사이트에 접속하여 최신 패치 존재 여부 확인 Step 2) 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

PC-06 (상)	3. 패치 관리 > 3.1 HOT FIX 등 최신 보안패치 적용

■ **Windows 7, Windows 8.1, Windows 10**

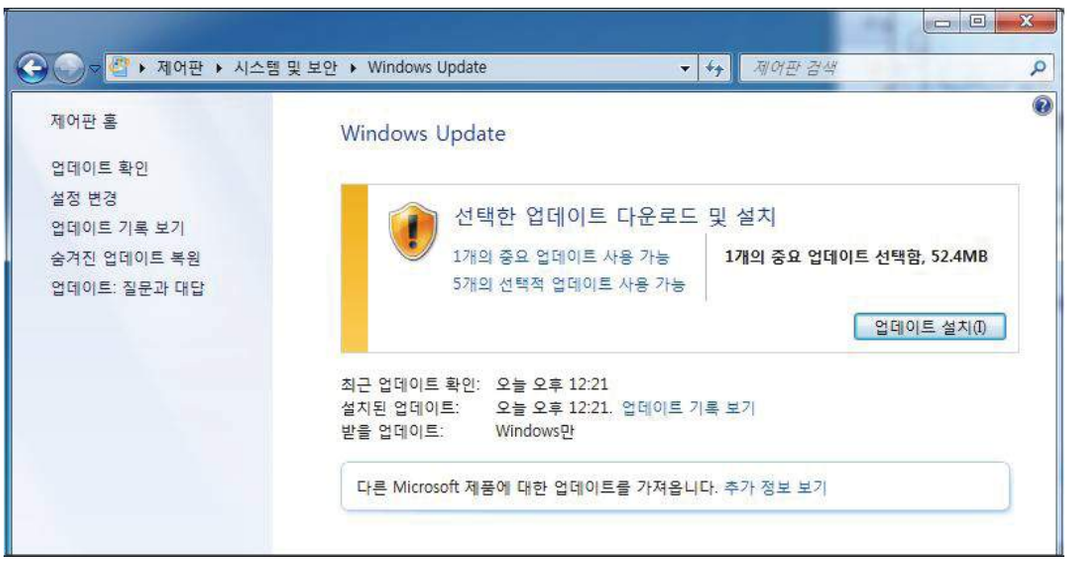
Step 1) 인터넷에 연결되는 경우 Windows Update 사이트에 접속하여 최신 패치 존재 여부 확인

Step 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

PC

PC-06 (상)	3. 패치 관리 > 3.1 HOT FIX 등 최신 보안패치 적용

Step 3) 업데이트 확인 후 미설치 된 HOT FIX, 최신 보안 업데이트 등의 설치



※윔(Worm), 랜섬웨어(Ransomware) 등의 위협을 피하기 위해 네트워크를 물리적으로 단절한 후 서비스팩 설치 및 업데이트 진행을 권장함

윔(Worm): 컴퓨터 바이러스의 하나로 컴퓨터 바이러스와는 달리 다른 프로그램을 감염시키지 않고 자기 자신을 복제하면서 통신망 등을 통해 널리 퍼지는 부정 프로그램을 말함

랜섬웨어(Ransomeware): 악성코드(malware)의 일종으로, 이에 감염된 컴퓨터는 시스템에 대한 접근이 제한되며 이를 해제하기 위해서는 악성 코드 제작자에게 대가로 금품을 제공해야 하는 악성 프로그램을 말함

조치 시 영향	일반적인 경우 영향 없음

PC

PC-07 (상)	3. 패치관리 > 3.2 최신 서비스팩 적용
취약점 개요	
점검내용	■ 시스템에 최신 서비스팩이 적용되어 있는지 점검
점검목적	■ 최신 서비스팩이 적용되어 있는지 점검하여 시스템 취약점을 이용한 공격(익스플로잇)에 대비가 되어 있는지 확인하기 위함
보안위협	■ 최신 서비스팩이 적용되지 않았을 경우 비인가자의 시스템 취약점을 이용한 공격(익스플로잇)에 노출될 수 있음
참고	※ **서비스 팩:** 운영체제 응용프로그램의 기능 추가 및 버그나 보안 취약점을 해결한 패치 파일을 단일 묶음으로 배포하는 패키지 ※ **익스플로잇:** 컴퓨터의 소프트웨어나 하드웨어 및 컴퓨터 관련 전자 제품의 버그, 보안 취약점 등 설계상 결함을 이용해 공격자의 의도된 동작을 수행하도록 만들어진 프로그램
점검대상 및 판단기준	
대상	■ Windows XP, Windows 7
판단기준	**양호 :** 최신 서비스팩이 적용 되어 있고 내부적으로 관리 절차를 수립하여 이행하고 있는 경우
	취약 : 최신 서비스팩이 적용 되어 있지 않거나 내부적으로 관리 절차가 수립되어 있지 않은 경우
조치방법	Windows Update 사이트에 접속하여 최신 서비스팩 여부 확인 및 적용
점검 및 조치 사례	
■ **Windows XP, Windows 7** Step 1) 현재 시스템에 설치되어 있는 서비스팩 확인 실행> "winver" 입력> Windows 정보 확인 2017년 11월 현재 최신 서비스팩 현황(Windows 7: SP1, 2020년 연장지원종료)	

PC

PC-07 (상)	3. 패치관리 > 3.2 최신 서비스팩 적용

Step 2) 서비스팩 확인 후 최신 버전이 아닐 경우 다운로드하여 설치

※ 윔(Worm), 랜섬웨어(Ransomware) 등의 위협을 피하기 위해 네트워크를 물리적으로 단절한 후 서비스팩 설치 및 업데이트 진행을 권장함

조치 시 영향	일반적인 경우 영향 없음

PC

PC-08 (상)	3. 패치관리 > 3.3 MS-Office, 훈글, 어도비 아크로뱃 등의 응용 프로그램에 대한 최신 보안 패치 및 벤더 권고사항 적용
취약점 개요	
점검내용	■ 운영체제에 설치된 응용프로그램(MS-Office, 한글, 어도비, 아크로뱃 등)의 최신 보안패치가 되어 있는지 점검
점검목적	■ 응용프로그램의 최신 보안 패치 여부를 점검하여 응용프로그램 취약점을 이용한 공격(익스플로잇)에 대한 대비를 하고 있는지 확인하기 위함
보안위협	■ 응용프로그램의 최신 보안 패치가 이루어지지 않아 응용프로그램의 취약점이 존재할 경우 비인가자가 공격(익스플로잇)을 통해 시스템 접근 권한을 획득할 수 있는 위험이 존재함
참고	-
점검대상 및 판단기준	
대상	■ Windows XP, Windows 7, Windows 8.1, Windows 10
판단기준	**양호 :** 설치된 응용 프로그램의 최신 패치가 적용되어 있고 내부적으로 관리 절차를 수립하여 이행하고 있는 경우
	취약 : 설치된 응용 프로그램의 최신 패치가 적용되어 있지 않거나 내부적으로 관리 절차가 수립되어 있지 않은 경우
조치방법	설치된 응용 프로그램의 최신 보안 패치 적용
점검 및 조치 사례	

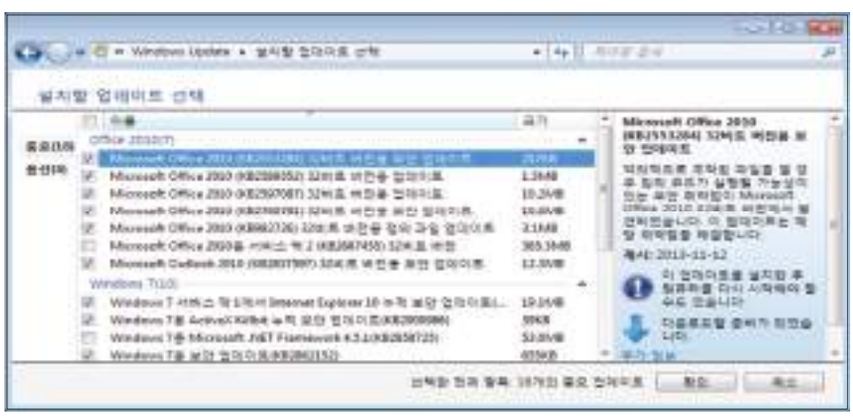
■ **Windows XP, Windows 7, Windows 8.1, Windows 10**

조치순서 1. MS-Office 관련 업데이트

Step 1) MS-Offcie 관련 업데이트 적용 여부 확인

- Windows XP: Windows XP: 제어판> 프로그램 추가/제거> "중요 업데이트" 확인
- Windows 7, 8.1: 제어판> Windows Update> 업데이트 확인> "중요 업데이트" 확인
- Windows 10: 설정> 업데이트 및 복구> 업데이트 확인

Step 2) MS-Office 관련 업데이트 적용



PC

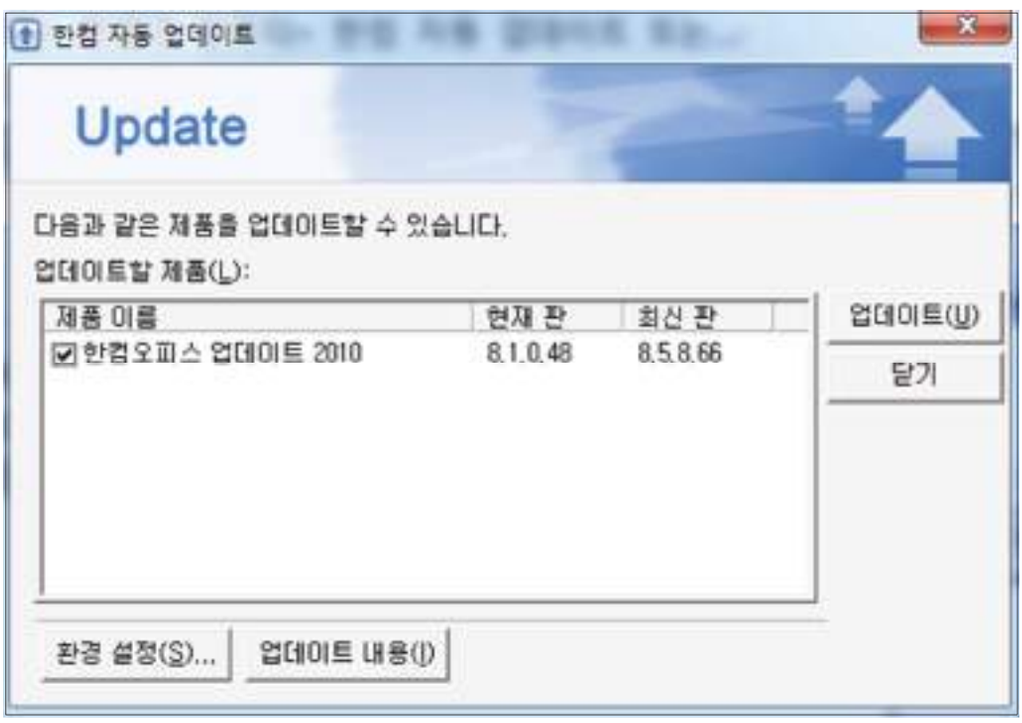
PC-08 (상)	3. 패치관리 > 3.3 MS-Office, 흔글, 어도비 아크로뱃 등의 응용 프로그램에 대한 최신 보안 패치 및 벤더 권고사항 적용

조치순서 2. 한글 업데이트

Step 1) 한글 업데이트 적용 여부 확인

- Windows 7, 8.1: 시작> 프로그램> 한글> 업데이트 실행
- Windows 10: 시작> 모든 앱> 한글> 업데이트 실행

Step 2) 한글 업데이트 적용



조치순서 3. 어도비 아크로뱃 업데이트

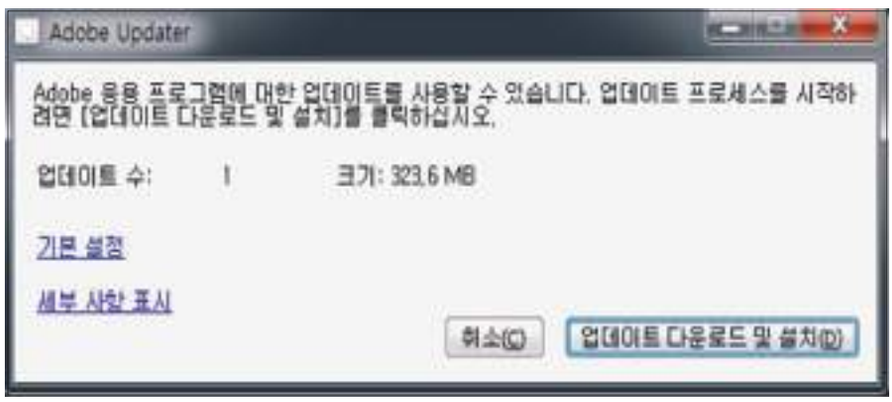
Step 1) 어도비 아크로뱃 업데이트 적용 여부 확인

- Adobe Reader 실행> 도움말> 업데이트 확인

PC

PC-08 (상)	3. 패치관리 > 3.3 MS-Office, 한글, 어도비 아크로뱃 등의 응용 프로그램에 대한 최신 보안 패치 및 벤더 권고사항 적용

Step 2) 어도비 아크로뱃 업데이트 적용



[업데이트 다운로드 및 설치]

[업데이트 다운로드 화면]

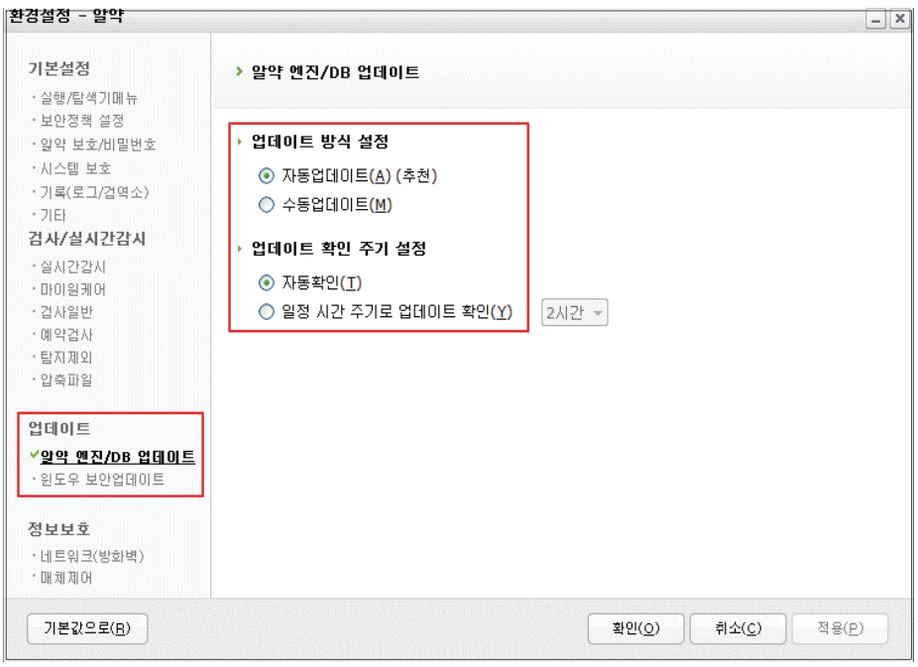
조치 시 영향	일반적인 경우 영향 없음

PC

PC-09 (상)	4. 보안 관리 > 4.1 바이러스 백신 프로그램 설치 및 주기적 업데이트
취약점 개요	
점검내용	■ 시스템에 백신이 설치되어 있는지 점검 ■ 설치된 백신이 주기적으로 자동 업데이트되도록 설정되어 있는지 백신의 환경 설정 점검
점검목적	■ 시스템의 백신 설치 여부와 설치된 백신이 주기적으로 업데이트가 되는지 점검하여 악성코드(바이러스, 웜, 랜섬웨어, 스파이웨어 등) 감염에 대한 대비를 하고 있는지 확인하기 위함
보안위협	■ 백신이 설치되지 않았거나, 백신이 설치되었어도 주기적으로 최신 업데이트가 이루어지지 않았을 경우 악성코드(바이러스, 웜, 랜섬웨어, 스파이웨어 등)의 감염이 발생하여 시스템의 중요한 파일이나 폴더의 유출 및 삭제가 발생할 위험이 존재함
참고	※ **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 ※ **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 ※ **랜섬웨어:** 사용자 파일을 암호화하여 접근을 제한하고 암호화된 파일을 복호화 할 때 복호화 비용을 요구하는 악성 소프트웨어의 한 종류 ※ **스파이웨어:** 사용자의 동의 없이 설치되어 컴퓨터의 정보를 수집하고 전송하는 악성 소프트웨어
점검대상 및 판단기준	
대상	■ Windows XP, Windows 7, Windows 8.1, Windows 10
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
점검 및 조치 사례	
Windows XP, Windows 7, Windows 8.1, Windows 10 Step 1) 백신의 업데이트 기능 활성화	

PC

PC-09 (상)	4. 보안 관리 > 4.1 바이러스 백신 프로그램 설치 및 주기적 업데이트



■ **Windows XP (V3 스마트 업데이트 사용 예시)**

Step 1) [V3] 실행> [업데이트] 실행

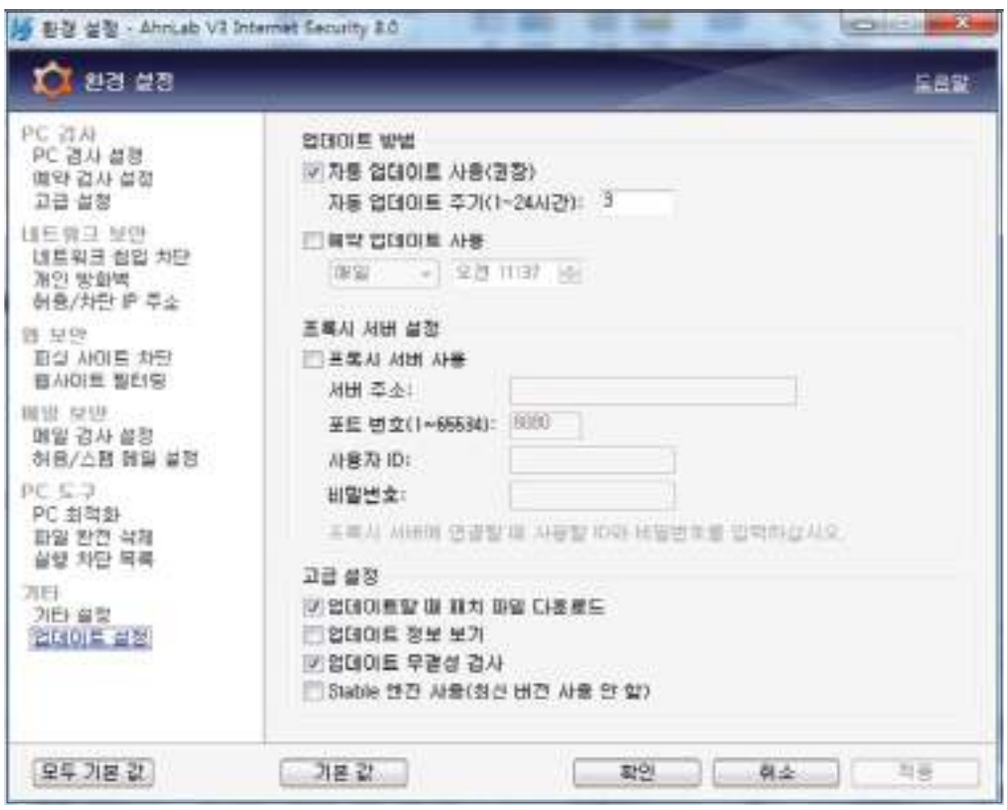
■ **Windows 7 (V3 Internet Security 8.0 사용 예시)**

Step 1) V3 Internet security 8.0 설치 여부 및 업데이트 설정 확인

Step 2) V3 Internet security 8.0 업데이트 적용

PC

PC-09 (상)	4. 보안 관리 > 4.1 바이러스 백신 프로그램 설치 및 주기적 업데이트



[환경 설정]

[업데이트 설정]

조치 시 영향	일반적인 경우 영향 없음

PC

PC-10 (상)	4. 보안 관리 > 4.2 바이러스 백신 프로그램에서 제공하는 실시간 감시 기능 활성화
취약점 개요	
점검내용	■ 시스템에 설치된 백신 프로그램의 환경 설정에 실시간 감시 기능이 적용되어 있는지 점검
점검목적	■ 사용자가 인터넷(이동식 저장 매체 포함)을 통해 파일을 다운로드하거나 다운로드 받은 파일을 실행할 경우 백신 프로그램이 악성코드 감염을 실시간으로 점검하고 있는지 확인하기 위함
보안위협	■ 백신 프로그램의 실시간 감시 기능이 적용되어 있지 않을 경우, 악성코드에 대해 실시간 감지가 이루어지지 않아 시스템 사용자가 인터넷(이동식 저장 매체 포함)을 통한 파일 다운로드나 실행 시 악성코드가 감염될 위험이 존재함
참고	-
점검대상 및 판단기준	
대상	■ Windows XP, Windows 7, Windows 8.1, Windows 10
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
점검 및 조치 사례	

Windows XP, Windows 7, Windows 8.1, Windows 10

Step 1) 백신의 실시간 감시 기능 활성화

PC

PC

PC-10 (상)	4. 보안 관리 > 4.2 바이러스 백신 프로그램에서 제공하는 실시간 감시 기능 활성화

■ **Windows XP (V3 스마트 업데이트 사용 예시)**

Step 1) 백신의 실시간 검사 기능 활성화

■ **Windows 7 (V3 Internet Security 8.0 사용 예시)**

Step 1) 백신의 실시간 검사 기능 활성화

조치 시 영향	일반적인 경우 영향 없음

PC

PC-11 (상)	4. 보안 관리 > 4.3 OS에서 제공하는 침입차단 기능 활성화
취약점 개요	
점검내용	■ 시스템의 방화벽 기능이 활성화되어 있는지 점검
점검목적	■ 방화벽 기능 활성화 여부를 점검하여 시스템에서 외부망의 비인가 접근 및 외부망으로 통신을 시도하는 프로그램에 대해 통제하고 있는지 확인하기 위함
보안위협	■ 방화벽 기능이 비활성화되어 있을 경우, 외부 및 내부의 접근통제가 되지 않아 유해 정보가 유입되거나 시스템 사용자의 파일이나 폴더가 외부로 유출될 위험이 존재함
참고	※ **방화벽:** 인터넷 또는 외부 네트워크에서 유입되는 트래픽을 통제하는 솔루션으로써 외부의 불법 침입으로부터 내부의 정보 자산을 보호하고 외부로부터 유해정보 유입을 차단하기 위한 정책과 이를 지원하는 하드웨어와 소프트웨어를 총칭함
점검대상 및 판단기준	
대상	■ Windows XP, Windows 7, Windows 8.1, Windows 10
판단기준	**양호 :** Windows 방화벽 "사용"으로 설정되어 있는 경우 또는 유·무료 기타 방화벽을 사용하고 있는 경우
	취약 : Windows 방화벽 "사용 안 함"으로 설정되어 있는 경우 또는 유·무료 기타 방화벽을 사용하고 있지 않는 경우
조치방법	Windows 방화벽 "사용"으로 설정 또는 유·무료 기타 방화벽을 사용
점검 및 조치 사례	

<조치유형 1. 제어판을 통해서 설정>

■ Windows xp, Windows 7, Windows 8.1, Windows 10

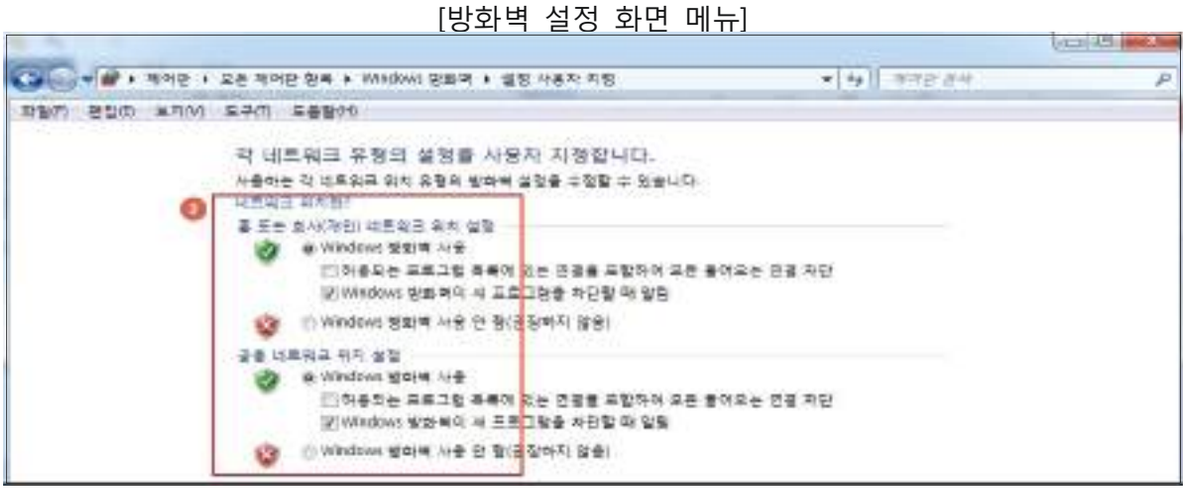
Step 1) 시작> 제어판> Windows 방화벽> Windows 방화벽 설정 또는 해제
(모든 윈도우즈 공통 방법: 시작> 실행> "`firewall.cpl`" 입력)

Step 2) Windows 방화벽 "사용" 설정(Windows xp 의 경우 [일반]탭에서 "사용(권장)" 설정)

PC

PC-11 (상)	4. 보안 관리 > 4.3 OS에서 제공하는 침입차단 기능 활성화

[방화벽 설정 화면 메뉴]



[방화벽 설정 화면]

<조치유형 2. 레지스트리 값으로 설정하는 방법>

■ Windows 7, Windows 8.1, Windows 10

Step 1) 시작> 실행> "regedit" 입력

Step 2) 레지스트리 경로

```
HKLM\SYSTEM\CurrentControlSet\Services\SharedAccess\Parameters\
FirewallPolicy\StandardProfile
```

Step 3) 설정값 입력

Value name	EnableFirewall
Data Type	DWORD 값
Value	1

[방화벽 사용 설정]

조치 시 영향	일반적인 경우 영향 없음

PC

PC-12 (상)	4. 보안관리 > 4.4 화면보호기 대기 시간을 5~10분으로 설정 및 재시작 시 암호로 보호하도록 설정
취약점 개요	
점검내용	■ 화면보호기 대기 시간 및 화면보호기 재시작 시 암호 설정 여부 점검
점검목적	■ 사용자가 일정 시간 동안 아무런 작업을 수행하지 않을 경우, 자동으로 로그오프 되거나 워크스테이션이 잠기도록 함
보안위협	■ 화면보호기가 작동하지 않거나 재시작 시 암호를 설정하지 않는다면, 사용자가 자리를 비운 사이 임의의 사용자가 해당 시스템에 접근하여 중요 정보를 유출하거나, 악의적인 행위를 통해 시스템 운영에 악영향을 미칠 수 있음
참고	※ **악의적인 행위:** 시스템 파일 또는 시스템 폴더 삭제, 응용프로그램 폴더 삭제 등
점검대상 및 판단기준	
대상	■ Windows XP, Windows 7, Windows 8.1, Windows 10
판단기준	**양호 :** 화면보호기 설정(대기시간 10분 이하) 및 암호로 보호가 설정되어 있는 경우
	취약 : 화면보호기 설정(대기시간 10분 초과) 및 암호로 보호가 설정되어 있지 않은 경우
조치방법	화면보호기 설정 및 암호화 보호 설정
점검 및 조치 사례	

■ **Windows 7, 8.1**

Step 1) 시작> 제어판> 개인설정> 화면보호기

- 화면보호기 실행 기타 방법1: 윈도우+R> control 입력> 제어판> 개인설정> 화면보호기
- 화면보호기 실행 기타 방법2: 바탕화면> 마우스 우클릭 > 개인설정 > 화면보호기

PC

PC-12 (상)	4. 보안관리 > 4.4 화면보호기 대기 시간을 5~10분으로 설정 및 재시작 시 암호로 보호하도록 설정

Step 2) 대기 시간을 5분 ~ 10분 사이로 설정 후 "다시 시작할 때 로그온 화면 표시(R)" 체크

■ **Windows 10**

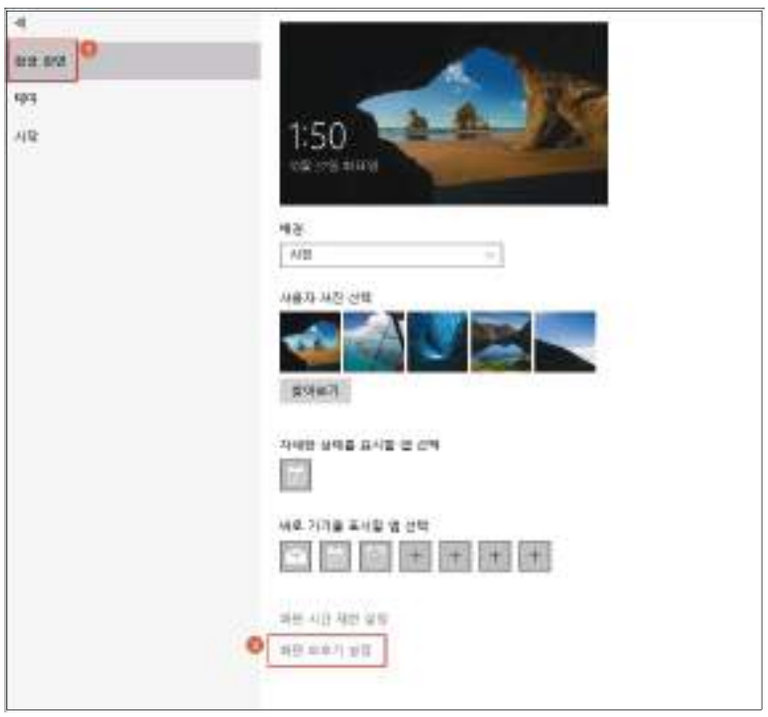
Step 1) 시작(또는 화면 왼쪽 아래 윈도우아이콘)> 설정> 개인설정> 잠금화면> 화면보호기 설정

- 화면보호기 실행 기타 방법1: 바탕화면> 마우스 우클릭> 개인설정> 잠금화면> 화면보호기 설정

[화면보호기 설정하기 위한 개인설정 메뉴]

PC

PC-12 (상)	4. 보안관리 > 4.4 화면보호기 대기 시간을 5~10분으로 설정 및 재시작 시 암호로 보호하도록 설정



[화면보호기 설정]

[화면보호기 시간 및 암호 설정]

조치 시 영향	일반적인 경우 영향 없음

PC

PC-13 (상)	4. 보안관리 > 4.5 CD, DVD, USB메모리 등과 같은 미디어의 자동실행 방지 등 이동식 미디어에 대한 보안대책 수립
취약점 개요	
점검내용	■ 이동식 미디어에 대한 보안대책 수립 여부 점검
점검목적	■ CD/DVD, USB 메모리 등과 같은 이동식 미디어를 USB port에 연결 시 자동 실행을 차단하도록 함
보안위협	■ CD/DVD, USB 메모리 등과 같은 이동식 미디어가 자동 실행되는 경우 미디어에 탑재된 Autorun.inf 파일을 통해 다른 응용 프로그램이 자동 실행될 수 있음 ■ 이동식 미디어가 사용 될 때 읽기 기능을 통해 바이러스 감염이 발생할 수 있고, 쓰기 기능을 통하여 주요 정보 유출이 발생할 수 있음
참고	※ **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 ※ **다른 응용 프로그램:** 사용자에게 피해를 일으키는 특정 프로그램을 말하며, 대부분 USB 관련 악성 코드들은 autorun.inf 파일을 통해 자동 실행되도록 제작됨
점검대상 및 판단기준	
대상	■ Windows XP, Windows 7, Windows 8.1, Windows 10
판단기준	**양호 :** 미디어 사용 시 자동 실행되지 않고 내부적으로 관리 절차를 수립하여 이행하고 있는 경우
	취약 : 미디어 사용 시 자동 실행되거나 내부적으로 관리 절차가 수립되어 있지 않은 경우
조치방법	미디어 자동실행 방지 설정
점검 및 조치 사례	

■ **Windows XP**

- 로컬 그룹 정책

  Step 1) 시작> 설정> 제어판> 관리도구> 서비스
  (시작> 실행> "gpedit.msc" 입력> 컴퓨터 구성> 관리 템플릿> Windows 구성 요소> 자동 실행 정책)

  Step 2) "자동 실행 사용 안 함" 정책을 "사용-모든 드라이브"로 설정

- 레지스트리설정

■ **Windows 7, Windows 8.1, Windows 10**

Step 1) 시작> 설정> 제어판> 관리도구> 서비스
(시작> 실행> "gpedit.msc" 입력> 컴퓨터 구성> 관리 템플릿> Windows 구성 요소> 자동 실행 정책)

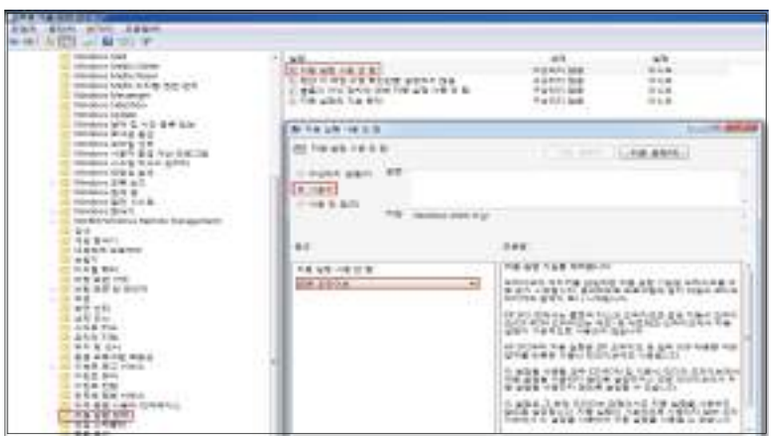
PC

PC-13 (상)	4. 보안관리 > 4.5 CD, DVD, USB메모리 등과 같은 미디어의 자동실행 방지 등 이동식 미디어에 대한 보안대책 수립

Step 2) "자동 실행 사용 안 함" 정책을 "사용-모든 드라이브"로 설정

Step 3) 레지스트리 값으로 설정하는 방법

1. 시작> 실행> "regedit" 입력



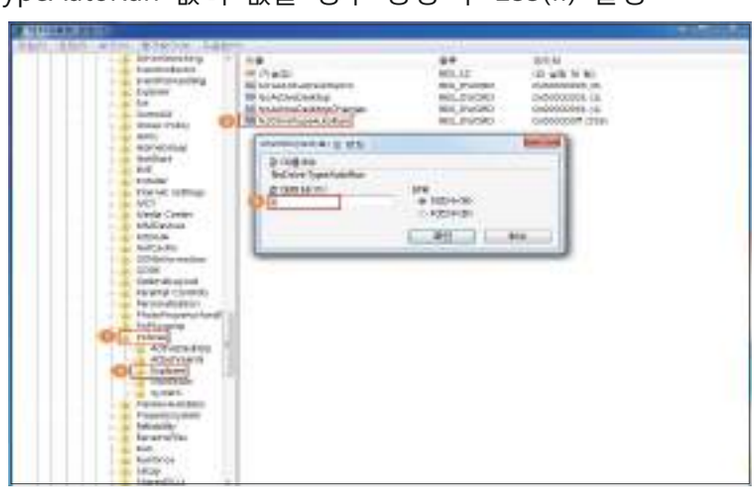
2. 레지스트리 경로

   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



Step 4) 제어판에서 자동 실행 기능 설정

시작> 제어판> 자동 실행> "모든 미디어 및 장치에 자동 실행 사용(U)" 체크 해제

조치 시 영향	일반적인 경우 영향 없음

PC

PC-14 (상)	4. 보안관리 > 4.6 PC 내부의 미사용(3개월) ActiveX 제거
취약점 개요	
점검내용	■ 장기간(3개월) 사용하지 않은 ActiveX 존재 여부 점검
점검목적	■ 장기간(3개월) 사용하지 않은 ActiveX 삭제
보안위협	■ 장기간 사용하지 않은 ActiveX 가 존재하고 있을 때 해당 ActiveX 에 취약점이 존재하는 경우, 악의적인 사용자가 이를 악용하여 시스템 해킹을 진행할 수 있음
참고	※ **액티브X(ActiveX):** 마이크로소프트사가 개발한 재사용 가능한 객체 지향적인 소프트웨어 구성요소 개발에 사용되는 기술로 인터넷 사이트로부터 다운로드 받은 콘텐츠들을 이용하는 동영상 시청, 금융결제 등을 사용하는데 이용됨
점검대상 및 판단기준	
대상	■ Windows XP, Windows 7, Windows 8.1, Windows 10
판단기준	**양호 :** 설치된 ActiveX를 주기적(매달 1번 권고)으로 점검하고 불필요한 ActiveX를 삭제하는 경우
	취약 : 설치된 ActiveX에 대한 주기적인 점검 및 삭제가 이루어지지 않는 경우
조치방법	불필요한 ActiveX 삭제 ※ 사용되지 않는 기간에 관계없이 불필요한 ActiveX의 경우 삭제 권고 ※ "Clean ActiveX" 등의 점검 프로그램을 통해 ActiveX 점검 가능 (http://service1.nis.go.kr/safe/securityRecomm.jsp?pArticleNo=1357&pListNo=121&mode=view)
점검 및 조치 사례	

■ **Windows XP, Windows 7, Windows 8.1, Windows 10**

Step 1) 국가사이버안전센터 홈페이지 접속> 자료실(1)> 보안권고문(2)> 121번(3)> 첨부파일 "Setup_CleanAX.exe" 다운로드(4)> 다운받은 "Setup_CleanAX.exe" 설치

PC

PC-14 (상)	4. 보안관리 > 4.6 PC 내부의 미사용(3개월) ActiveX 제거

Step 2) 설치된 'CleanAX' 실행 > 조회 기간 선택(1) > 불필요하여 삭제할 ActiveX 선택(2) > 삭제(3) 버튼 클릭

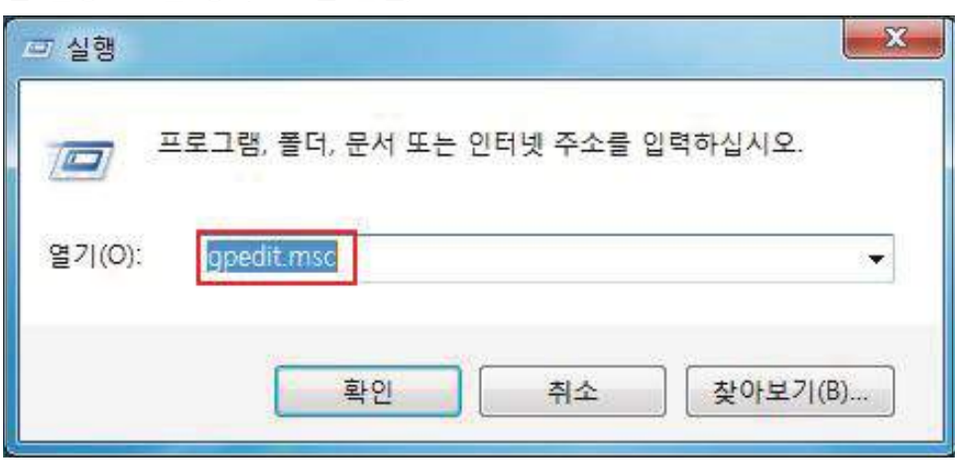
조치 시 영향	삭제된 ActiveX 사용 불가 (사용 시 설치 후 사용)

PC

PC-15 (중)	1. 계정관리 > 1.3 복구 콘솔에서 자동 로그온을 금지하도록 설정하여 사용하고 있는가?
취약점 개요	
점검내용	■ 윈도우 복구 콘솔 자동 로그인 설정이 허용되어 있는지 점검
점검목적	■ 복구 콘솔 자동 로그온 허용을 "사용 안 함"으로 설정함으로써 비인가자의 복구 콘솔을 통한 관리자 권한 탈취 등의 위험을 방지하기 위함
보안위협	■ 윈도우 복구 콘솔(Recovery Console) 자동 로그온 설정은 시스템 액세스 허가 전 Administrator 계정의 암호 제공 여부를 결정하는 것으로 이 옵션을 사용하면 비인가자의 경우에도 복구 콘솔을 이용해 관리자 권한으로 시스템에 자동으로 로그온 할 수 있음
참고	※ **복구 콘솔(Recovery Console):** 윈도우 2000, 윈도우 XP, 윈도우 서버 2003 운영체제의 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 명령줄 인터페이스를 이용하여 제한된 영역의 작업을 수행할 수 있음
점검대상 및 판단기준	
대상	■ Windows XP, Windows 7, Windows 8.1, Windows 10
판단기준	**양호 :** 복구 콘솔 자동 로그온 허용이 "사용 안 함"으로 설정되어 있는 경우
	취약 : 복구 콘솔 자동 로그온 허용이 "사용"으로 설정되어 있는 경우
조치방법	복구 콘솔 자동 로그온 허용 "사용 안 함"으로 설정
점검 및 조치 사례	

■ **Windows XP, Windows 7, Windows 8.1, Windows 10**

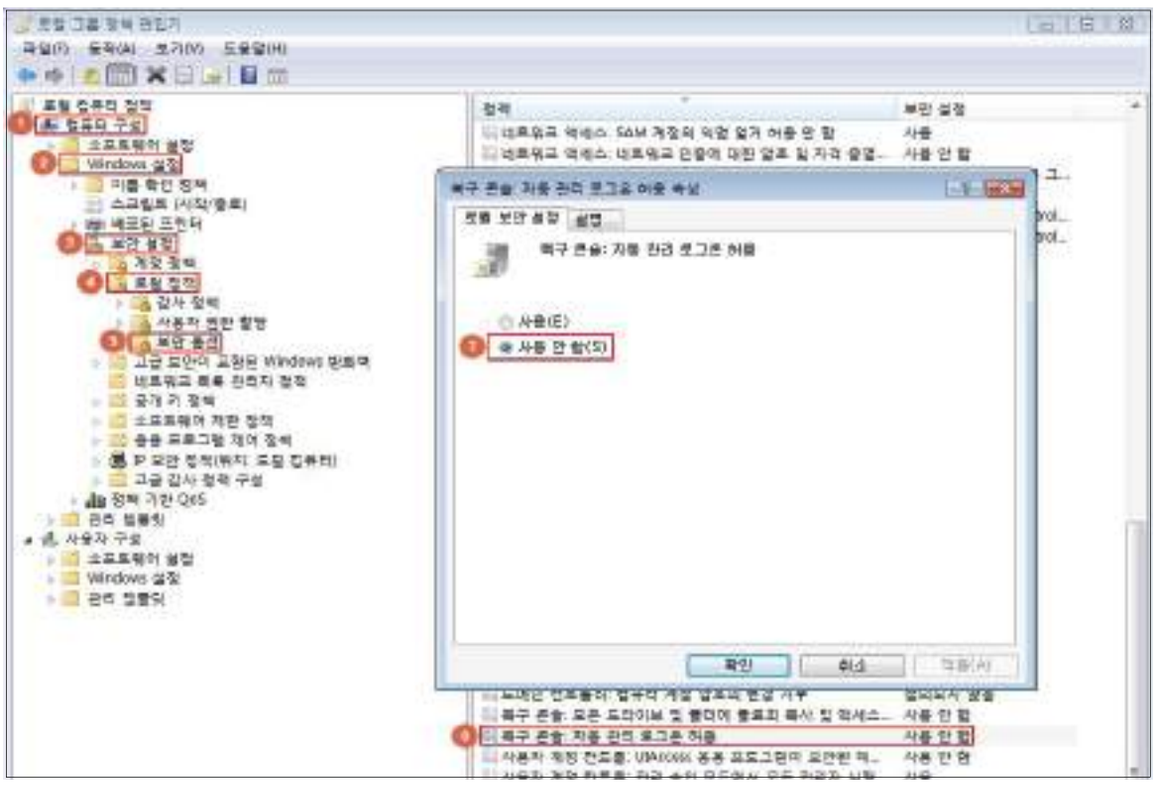
Step 1) 제어판> 관리 도구> 로컬 보안 정책> 보안 설정> 로컬 정책> 보안 옵션
(윈도우키+영문자R 키 입력> 실행> "gpedit.msc" 입력> 컴퓨터 구성> Windows 설정> 보안 설정> 로컬 정책> 보안 옵션)



PC

PC-15 (중)	1. 계정관리 > 1.3 복구 콘솔에서 자동 로그온을 금지하도록 설정하여 사용하고 있는가?

Step 2) 복구 콘솔 : 자동 관리 로그온 허용 속성 : "사용 안 함" 설정



Step 3) 레지스트리 값으로 설정하는 방법

1. 윈도우키+영문자R 키 입력 > 실행 > "regedit" 입력
2. HKLM\SOFTWARE\Microsoft\WindowsNT\CurrentVersion\Setup\RecoveryConsole
3. 설정 값 입력

Value name	SecurityLevel
Data Type	DWORD 값
Value	0(zero)

조치 시 영향	일반적인 경우 영향 없음

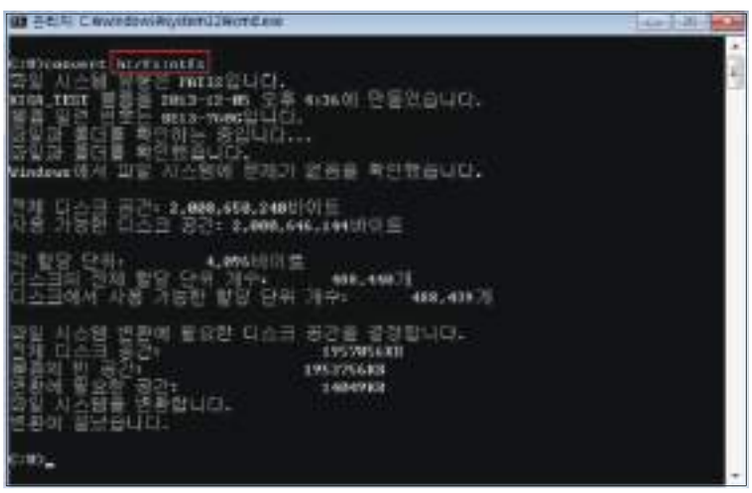
PC

PC-16 (중)	2. 서비스 관리 > 2.4 파일 시스템이 NTFS 포맷으로 되어 있는가?
취약점 개요	
점검내용	■ 하드 디스크의 파일 시스템이 NTFS를 사용하고 있는 지를 점검
점검목적	■ 보안성 기능이 없는 FAT32를 지양하고 사용 권한 및 암호화를 통해 특정 파일에 대한 특정 사용자의 액세스를 제한 할 수 있는 NTFS를 사용하여 보안성을 강화하기 위함
보안위협	■ FAT32 파일 시스템을 사용하는 경우, 사용자의 컴퓨터에 액세스하는 사람은 누구나 컴퓨터 안에 있는 파일을 읽을 수 있으므로, 중요 파일에 접근할 수 없는 비인가자가 주요 정보를 유출할 수 있음
참고	■ 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
점검대상 및 판단기준	
대상	■ Windows XP, Windows 7, Windows 8.1, Windows 10
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
점검 및 조치 사례	
■ **Windows XP, Windows 7, Windows 8.1 , Windows 10** Step 1) 디스크 볼륨의 파일 시스템이 "NTFS"인지 확인 제어판> 관리 도구> 컴퓨터 관리> 저장소> 디스크 관리 (시작> 실행> "diskmgmt.msc" 입력> 디스크 관리) Step 2) 모든 디스크 볼륨의 파일 시스템이 "NTFS"가 아닌 경우 취약점이 존재하므로, 모든 디스크 볼륨에 대해 파일 시스템을 "NTFS"로 변경	

PC

PC-16 (중)	2. 서비스 관리 > 2.4 파일 시스템이 NTFS 포맷으로 되어 있는가?

Step 3) 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
- Windows 8.1: 관리자 권한으로 "cmd.exe" 실행 후 "convert 드라이브명:/fs:ntfs" 입력
- Windows 10: 관리자 권한으로 "cmd.exe" 실행 후 "convert 드라이브명:/fs:ntfs" 입력

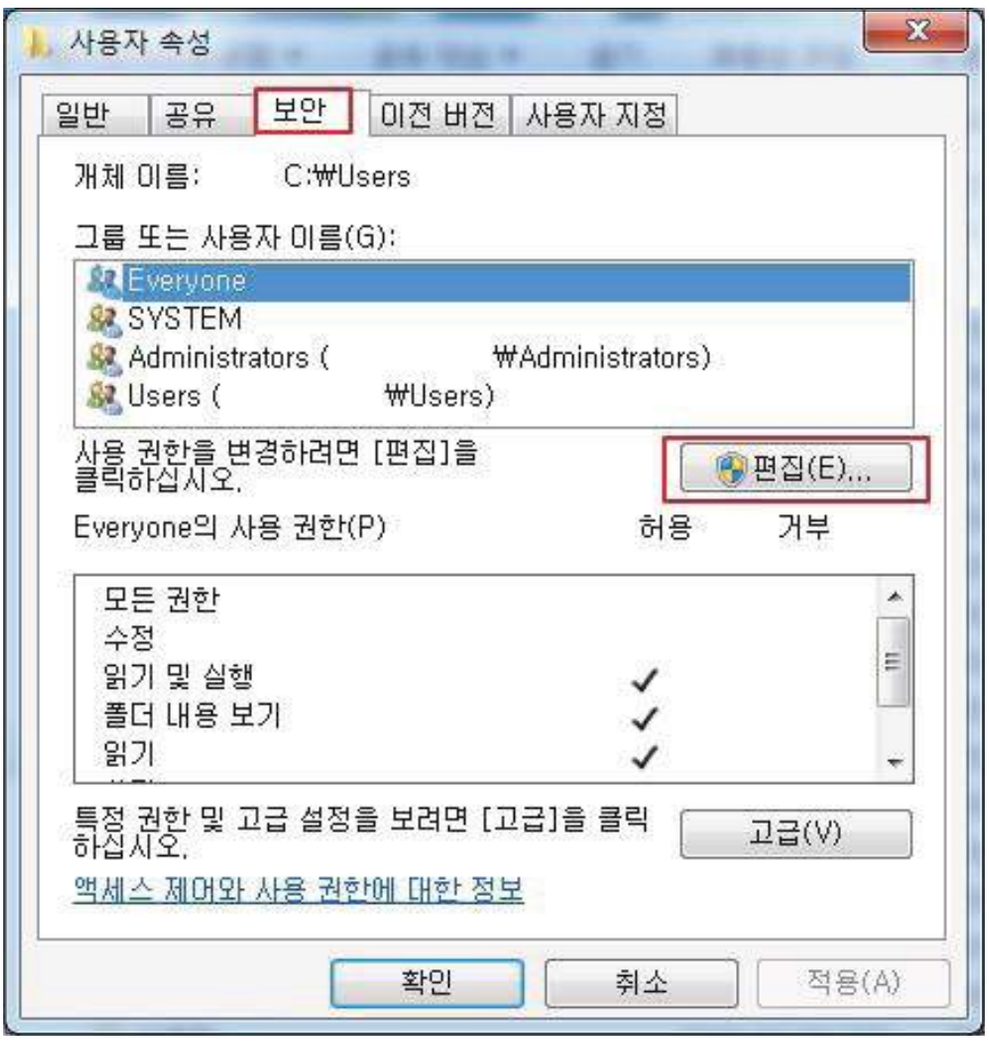
(예) convert h: /fs/ntfs 입력하면 H 드라이브는 NTFS 형식으로 포맷됨

Step 4) NTFS 변경 후 폴더 및 파일에 적합한 ACL 적용

1. 폴더나 파일을 마우스 오른쪽 버튼 클릭 후 단축메뉴에서 [속성] 선택
2. [속성] 대화상자에서 [보안] 탭을 선택
3. 편집을 눌러 그룹이나 계정에 맞는 권한으로 변경

PC

PC-16 (중)	2. 서비스 관리 > 2.4 파일 시스템이 NTFS 포맷으로 되어 있는가?



※ 최근 OS에서는 convert.exe 기능은 기본적으로 제공하나 FAT32 파일시스템을 지원하지 않고 exFAT 파일시스템을 지원함

조치 시 영향	일반적인 경우 영향 없음

PC

PC-17 (중)	2. 서비스 관리 > 2.5 대상 시스템이 Windows 서버를 제외한 다른 OS로 멀티 부팅이 가능하지 않도록 설정하여 사용하는가?
취약점 개요	
점검내용	■ 사용자 PC에 하나의 OS만 설치되어 있는지 점검
점검목적	■ 사용자 PC에서 멀티 부팅을 사용하는지를 점검하여 다른 OS를 이용한 주요 파일 시스템 접근을 차단하기 위함
보안위협	■ 멀티 부팅이 가능한 경우, 공격자는 해당 PC의 주요 OS이외에 다른 OS로 부팅하여 중요한 정보가 들어 있는 파일 시스템에 접근하여 주요 정보를 획득할 수 있음
참고	※ **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 갖춤으로써 하드웨어 비용을 크게 낮출 수 있을 뿐만 아니라 새로운 운영 체제를 "별도의 포맷, 다시 설치 과정 없이" 사용할 수 있다는 장점이 있음
점검대상 및 판단기준	
대상	■ Windows XP, Windows 7, Windows 8.1, Windows 10
판단기준	**양호 :** PC 내에 하나의 OS만 설치되어 있는 경우
	취약 : PC 내에 2개 이상의 OS가 설치되어 있는 경우
조치방법	하나의 OS만 설치하여 운영함
점검 및 조치 사례	

■ **Windows XP, Windows 7, Windows 8.1 , Windows 10**

Step 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)

Step 2) "기본 운영 체제" 드롭다운 메뉴에서 2개 이상의 OS가 표시되면 취약점 존재

Step 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

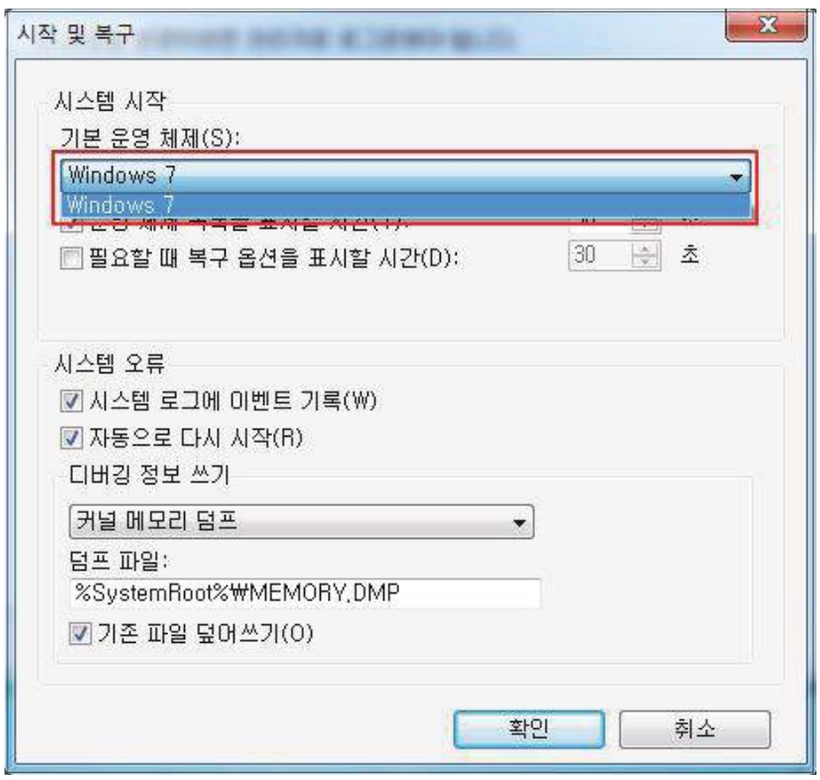
※ CMD 명령어를 이용한 멀티 부팅 Windows의 정보 확인 방법 (※ 관리자 권한으로 cmd 실행 방법 부록 참조)

- Windows 7: 관리자 권한으로 "cmd.exe" 실행 후 "bcdedit" 입력

PC

PC-17 (중)	2. 서비스 관리 > 2.5 대상 시스템이 Windows 서버를 제외한 다른 OS로 멀티 부팅이 가능하지 않도록 설정하여 사용하는가?

- Windows XP: 시작> 실행> "cmd" 입력> "bcdedit" 입력
- Windows 8.1: 관리자 권한으로 "cmd.exe" 실행 후 "bcdedit" 입력
- Windows 10: 시작> 실행> "cmd" 입력> "bcdedit" 입력



조치 시 영향	일반적인 경우 영향 없음

PC

PC-18 (하)	2. 서비스 관리 > 2.6 브라우저 종료 시 임시 인터넷 파일 폴더의 내용을 삭제하도록 설정하여 사용하는가?
취약점 개요	
점검내용	■ 브라우저 인터넷 옵션에 있는 고급 설정에 "브라우저를 닫을 때 임시 인터넷 파일 폴더 비우기" 기능이 활성화 되어 있는지 점검
점검목적	■ 브라우저 사용 시 생성되는 임시 인터넷 파일 삭제를 통하여 웹 양식에 입력한 정보(예: 이름 및 주소), 자동 로그인을 위한 웹 사이트 암호 정보 등을 삭제하여 개인정보의 보안을 향상시키기 위함
보안위협	■ 임시 인터넷 파일 폴더 내용을 삭제하지 않을 경우, 다른 계정에 저장된 임시 인터넷 파일 폴더를 통해 이메일 주소, 웹 사이트 접근 기록 등의 개인정보를 획득할 수 있음
참고	※ **임시 인터넷 파일:** 웹페이지 방문 시 화면에 나타나는 웹페이지 파일이나 이미지, 플래시 등을 저장한 파일
점검대상 및 판단기준	
대상	■ Windows XP, Windows 7, Windows 8.1, Windows 10
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
점검 및 조치 사례	

■ **Windows XP, Windows 7, Windows 8.1 , Windows 10**

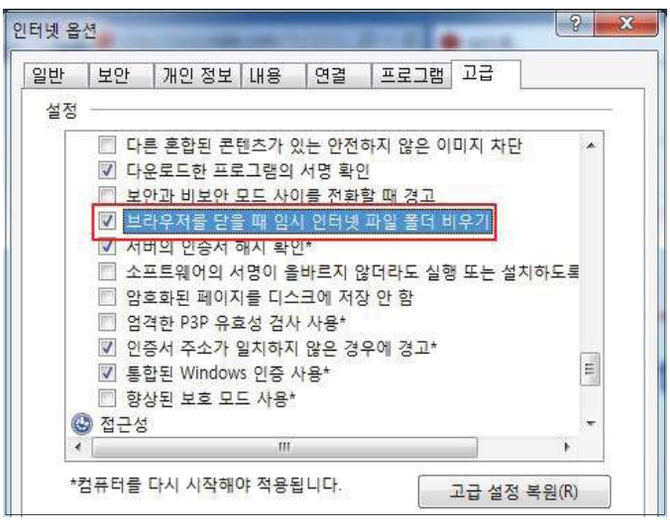
Step 1) 인터넷 제어판에서 "브라우저를 닫을 때 임시 인터넷 파일 폴더 비우기" 설정 여부 확인
시작> 실행> "gpedit.msc" 입력> 컴퓨터 구성> 관리 템플릿> Windows 구성 요소> Internet Explorer> 인터넷 제어판> 고급 페이지

Step 2) "브라우저를 닫을 때 임시 인터넷 파일 폴더 비우기"를 선택하여 "사용"으로 속성 변경
※ 해당 인터넷 제어판 메뉴는 버전에 따라 존재하지 않는 경우도 있음

Step 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

PC

PC-18 (하)	2. 서비스 관리 > 2.6 브라우저 종료 시 임시 인터넷 파일 폴더의 내용을 삭제하도록 설정하여 사용하는가?

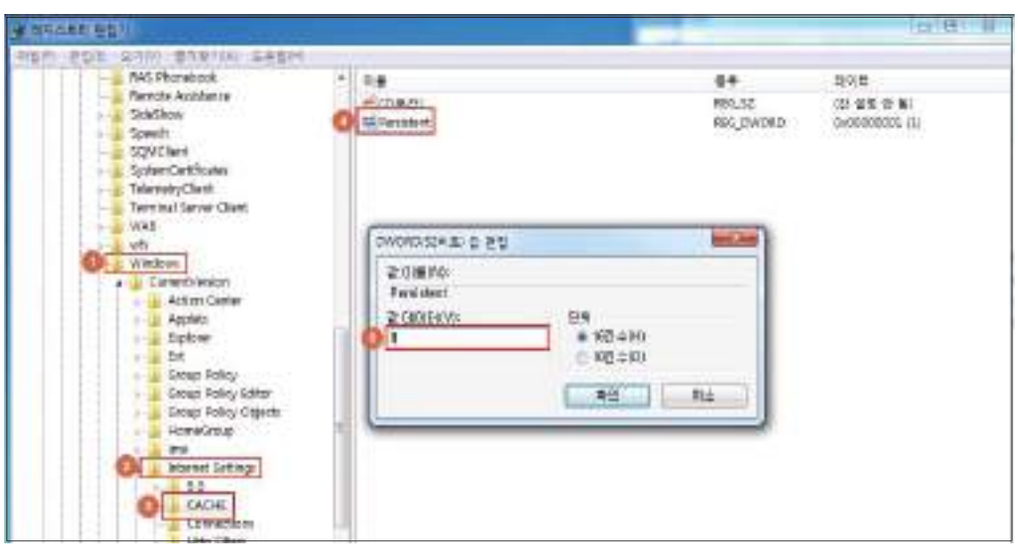


Step 4) 레지스트리 값으로 설정하는 방법

1. 시작> 실행> “regedit” 입력
2. 레지스트리 경로

   `HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\InternetSettings\Cache`
3. 설정 값 입력

Value name	Persistent
Data Type	DWORD 값
Value	0(zero)



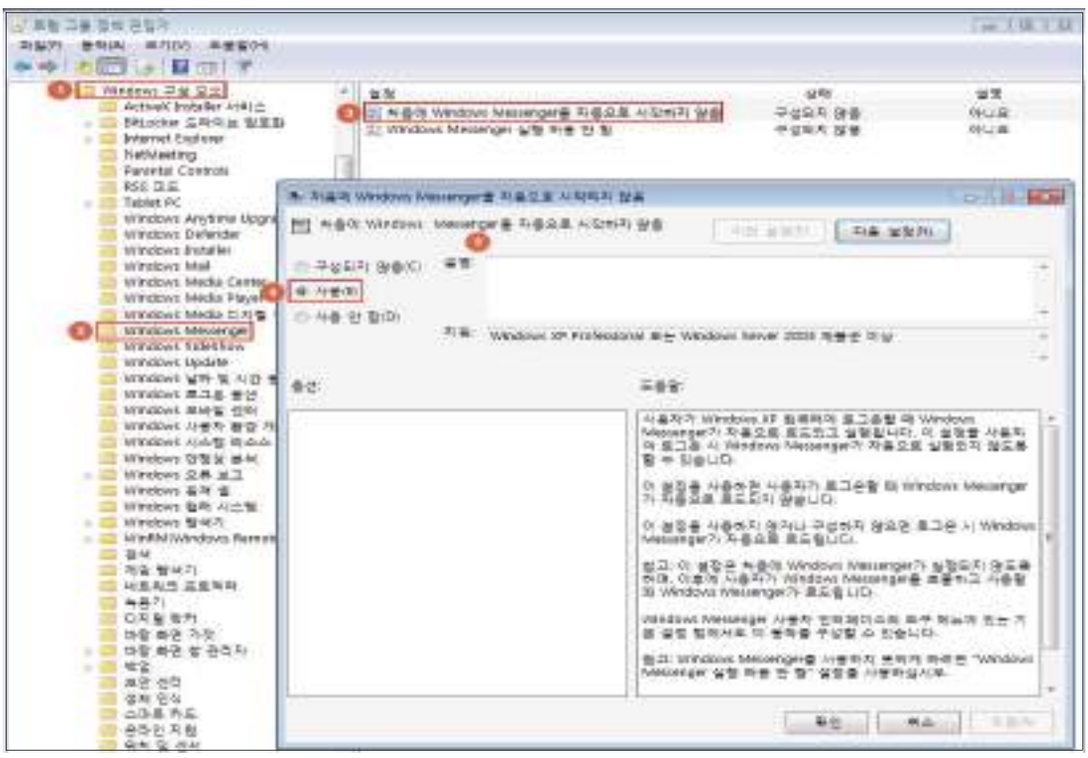
조치 시 영향	일반적인 경우 영향 없음

PC

PC-19 (중)	4. 보안관리 > 4.7 시스템 부팅 시 Windows Messenger가 자동으로 시작되지 않도록 설정되어 있는가?
취약점 개요	
점검내용	■ 시스템 부팅 시 Windows Messenger 자동시작 여부 점검
점검목적	■ 시스템 부팅 시 Windows Messenger 자동시작을 차단함
보안위협	■ Windows Messenger 통해 정보 유출 및 악성코드 유입이 발생 할 수 있음
참고	※ **Windows Messenger:** 컴퓨터 네트워크의 다른 사용자에게 인스턴트 메시지를 보내는 프로그램으로 스팸, 악의적인 소프트웨어 배포 및 중요한 데이터의 노출과 같은 용도로 사용되는 취약성이 존재함
점검대상 및 판단기준	
대상	■ Windows XP, Windows 7, Windows 8.1, Windows 10
판단기준	**양호 :** Windows Messenger 자동시작 금지 설정이 되어있는 경우
	취약 : Windows Messenger 자동시작 금지 설정이 되어있지 않는 경우
조치방법	▪ Windows Messenger 자동시작 금지 설정 ※ 기반시설 시스템은 Windows Messenger 사용을 원칙적으로 금지하나, 부득이 사용해야 할 경우 Messenger 자동시작을 금지하여 사용해야 함 ※ 관련 점검 항목 : PC-06(상)
점검 및 조치 사례	
<조치유형 1. 로컬 그룹 정책 편집기로 설정하는 방법> **■ Windows XP, Windows 7 , Windows 8.1 , Windows 10** Step 1) 시작> 실행> "gpedit.msc" 입력> 컴퓨터 구성> 관리 템플릿> Windows 구성 요소> Windows Messenger Step 2) "Windows Messenger를 자동으로 시작하지 않음" 설정을 "사용"으로 설정	

PC

PC-19 (중)	4. 보안관리 > 4.7 시스템 부팅 시 Windows Messenger가 자동으로 시작되지 않도록 설정되어 있는가?



<조치유형 2. 레지스트리 값으로 설정하는 방법>

■ Windows XP, Windows 7 , Windows 8.1 , Windows 10

Step 1) 레지스트리 값으로 설정하는 방법

1. 시작> 실행> "regedit" 입력
2. 레지스트리 경로

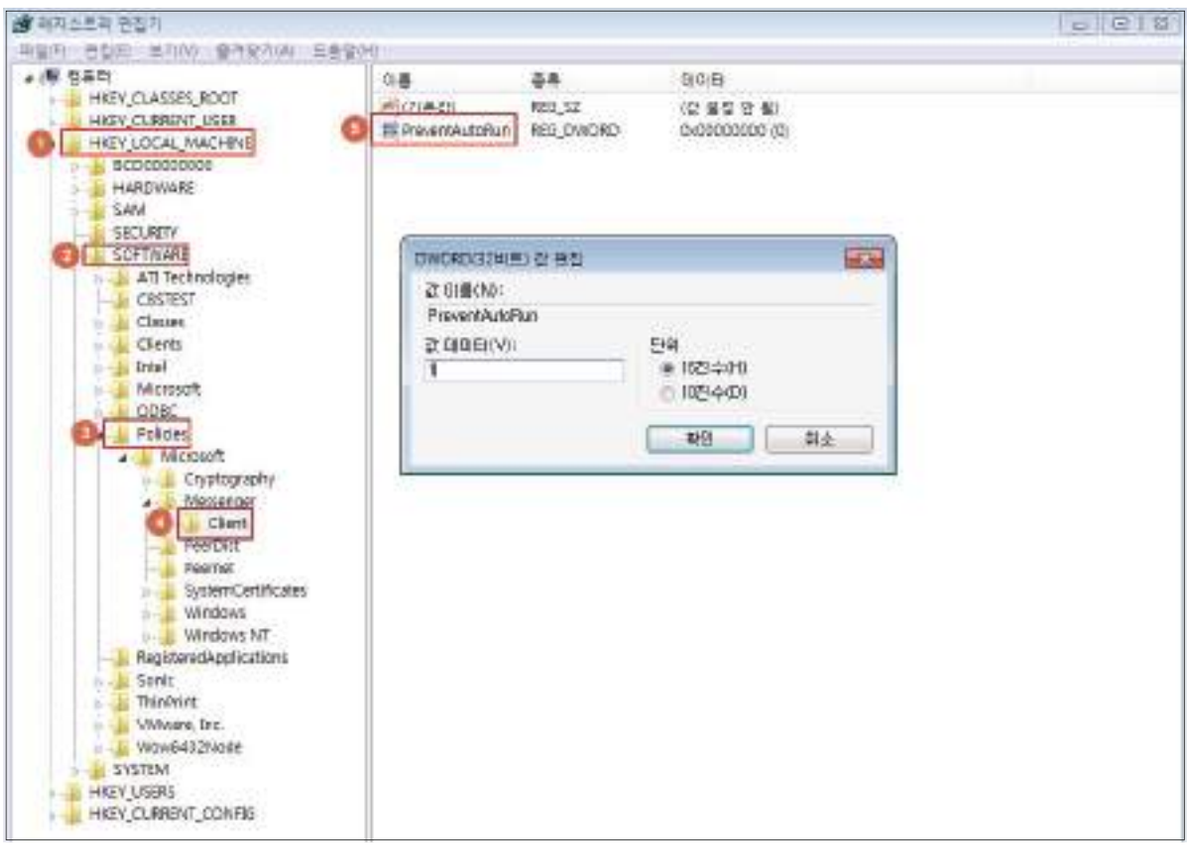
   `HKLM\Software\Policies\Microsoft\Messenger\Client`
3. 설정 값 입력

Value name	PreventAutoRun
Data Type	DWORD 값
Value	1 ※ 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

PC-19 (중)	4. 보안관리 > 4.7 시스템 부팅 시 Windows Messenger가 자동으로 시작되지 않도록 설정되어 있는가?



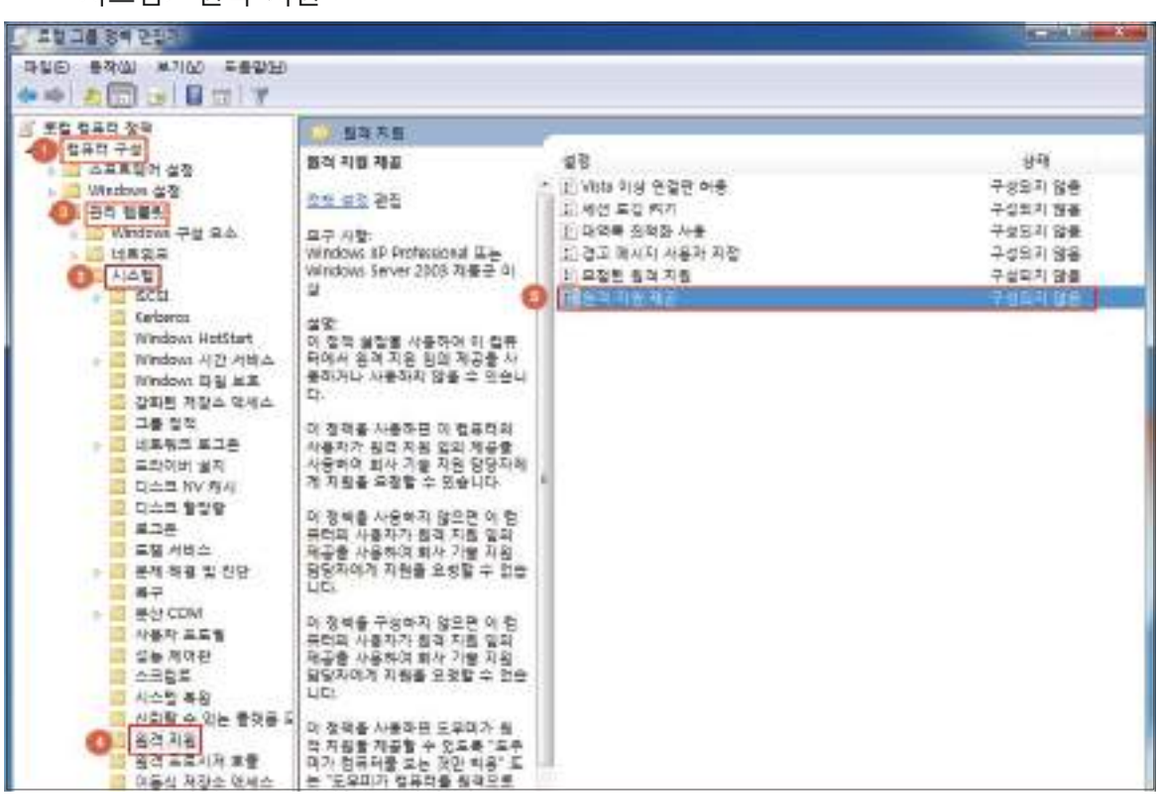
조치 시 영향	일반적인 경우 영향 없음

PC

PC-20 (중)	4. 보안관리 > 4.8 원격 지원을 금지하도록 정책이 설정되어 있는가?
취약점 개요	
점검내용	■ 원격 지원을 사용하지 않도록 설정하고 있는지 점검
점검목적	■ 원격 지원 기능을 비활성화 함
보안위협	■ 원격 지원 기능이 활성화 되어 비인가자에게 원격에서의 접근이 허용될 경우, 시스템 제어 권한이 악용될 수 있음
참고	-
점검대상 및 판단기준	
대상	■ Windows XP, Windows 7, Windows 8.1, Windows 10
판단기준	**양호 :** 원격 지원이 "사용 안 함"으로 설정 되어 있는 경우
	취약 : 원격 지원이 "사용"으로 설정 되어 있는 경우
조치방법	원격 지원 서비스 비활성화
점검 및 조치 사례	

■ **Windows XP, Windows 7, Windows 8.1, Windows 10**

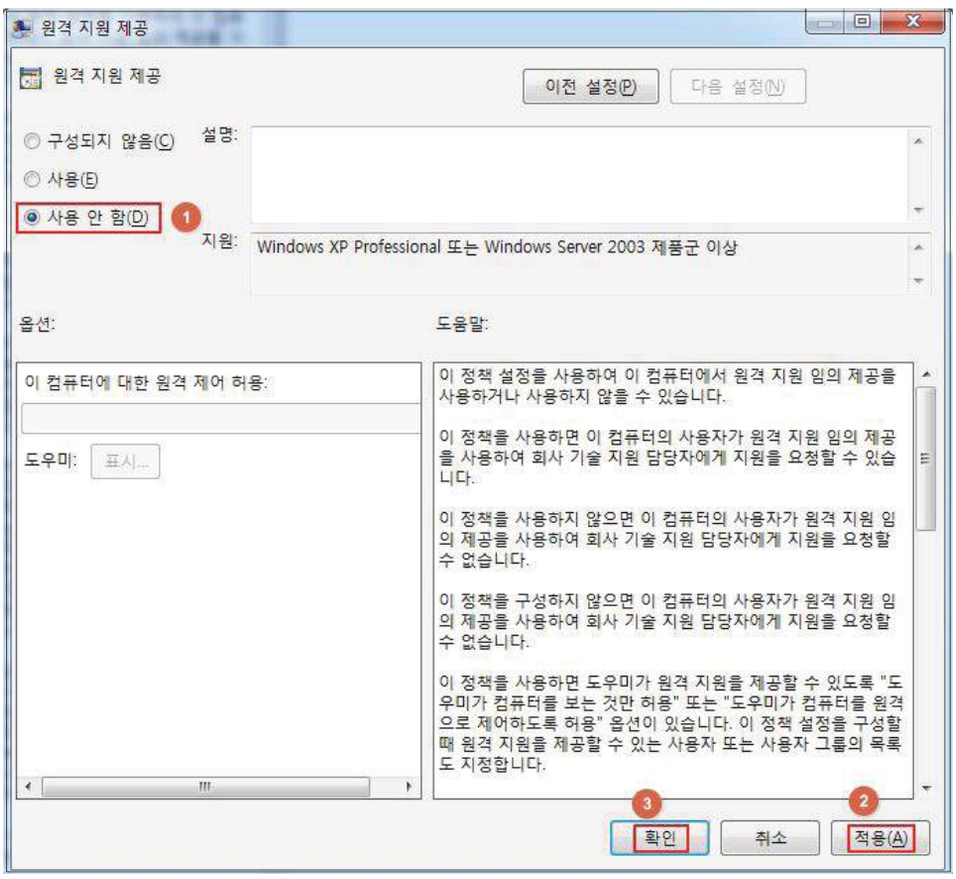
Step 1) 윈도우키+영문자R 키 입력> 실행> "gpedit.msc" 입력> 컴퓨터 구성> 관리 템플릿> 시스템> 원격 지원



PC

PC-20 (중)	4. 보안관리 > 4.8 원격 지원을 금지하도록 정책이 설정되어 있는가?

Step 2) "원격 지원 제공"을 "사용 안 함"으로 설정



조치 시 영향	원격 지원 기능 사용 불가

부록

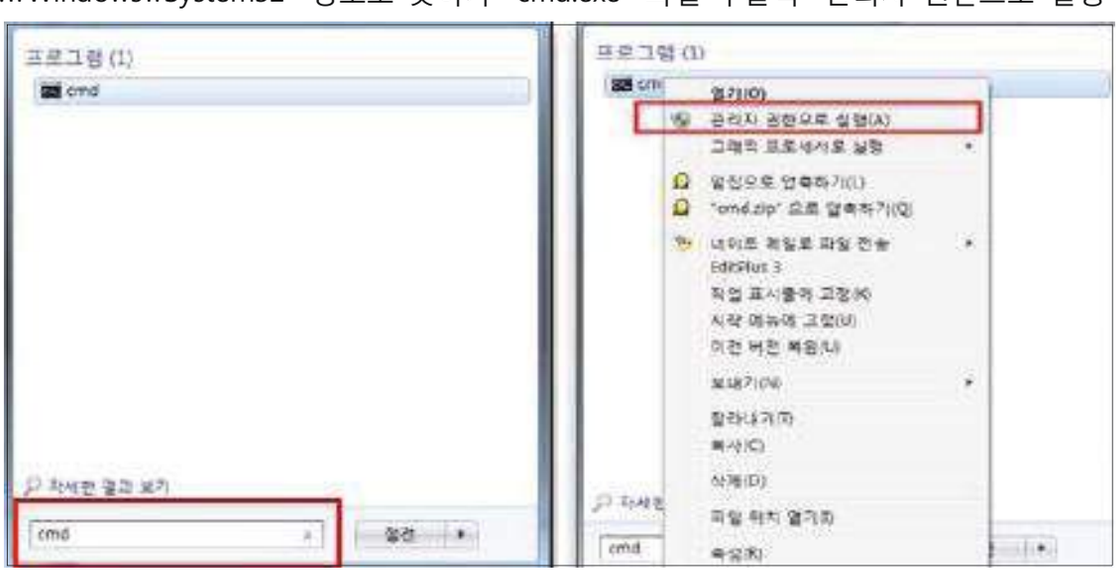
01. Windows 빠른실행 명령어 모음
(※ Windows 에디션에 따라 명령어 실행 여부에 차이가 있을 수 있음)

문자표	charmap	네트워크 연결	ncpa.cpl
제어판	control	컴퓨터 관리	compmgmt.msc
마우스 속성	main.cpl	장치 관리자	devmgmt.msc
전원 옵션	powercfg.cpl	성능 모니터뷰	perfmon.msc
관리 도구	control admintools	정책의 결과와 집합	rsop.msc
레지스트리 편집기	regedit	공유 폴더	fsmgmt.msc
윈도우 버전 확인	winver	디스크 관리	diskmgmt.msc
작업 관리자	taskmgr	디스크 조각 모음(XP)	dfrg.msc
이벤트 뷰어	eventvwr	디스크 조각 모음	dfrgui
사용자 계정	netplwiz	디스크 정리	cleanmgr
시스템 정보	msinfo32	로컬 컴퓨터 정책	gpedit.msc
서비스 관리자	services.msc	로컬 사용자 및 그룹	lusrmgr.msc
인터넷 속성	inetcpl.cpl	로컬 보안 설정	secpol.msc
시스템 등록정보	sysdm.cpl	시스템 구성	msconfig
포로그램 추가/제거	appwiz.cpl	방화벽	firewall.cpl
디스플레이 등록정보	desk.cpl	관리센터	wscui.cpl
사운드 및 오디오 장치	mmsys.cpl	폴더옵션	control folders
원격 데스크톱 연결	mstsc	날짜 및 시간	timedate.cpl

02. 관리자 권한으로 cmd 명령어를 실행하는 방법

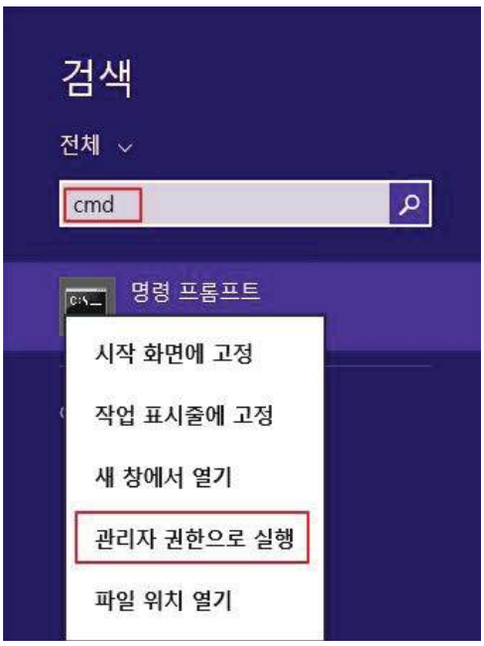
※ Windows 7

시작> "cmd.exe"검색> 우클릭> "관리자 권한으로 실행" 또는,
"C:₩Windows₩System32" 경로로 찾아가 "cmd.exe" 파일 우클릭 "관리자 권한으로 실행"



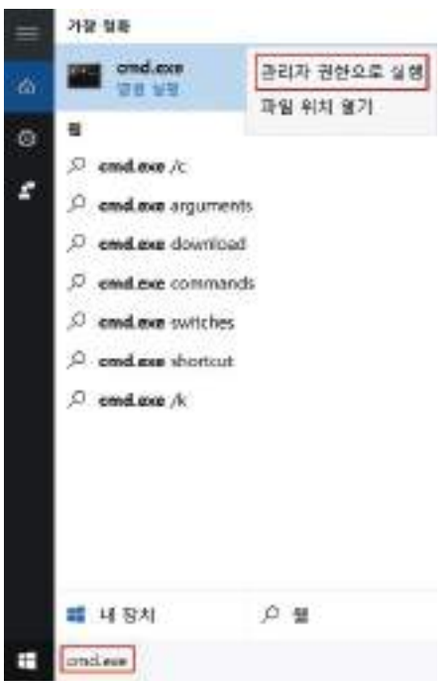
※ Windows 8.1

시작> 화면 우측 돋보기 클릭 > "cmd.exe" 검색> 우클릭> "관리자 권한으로 실행" 또는, 시작> 전체앱(화면 좌측 화살표 클릭)> 윈도우 시스템> 명령 프롬프트> 우클릭> "관리자 권한으로 실행"



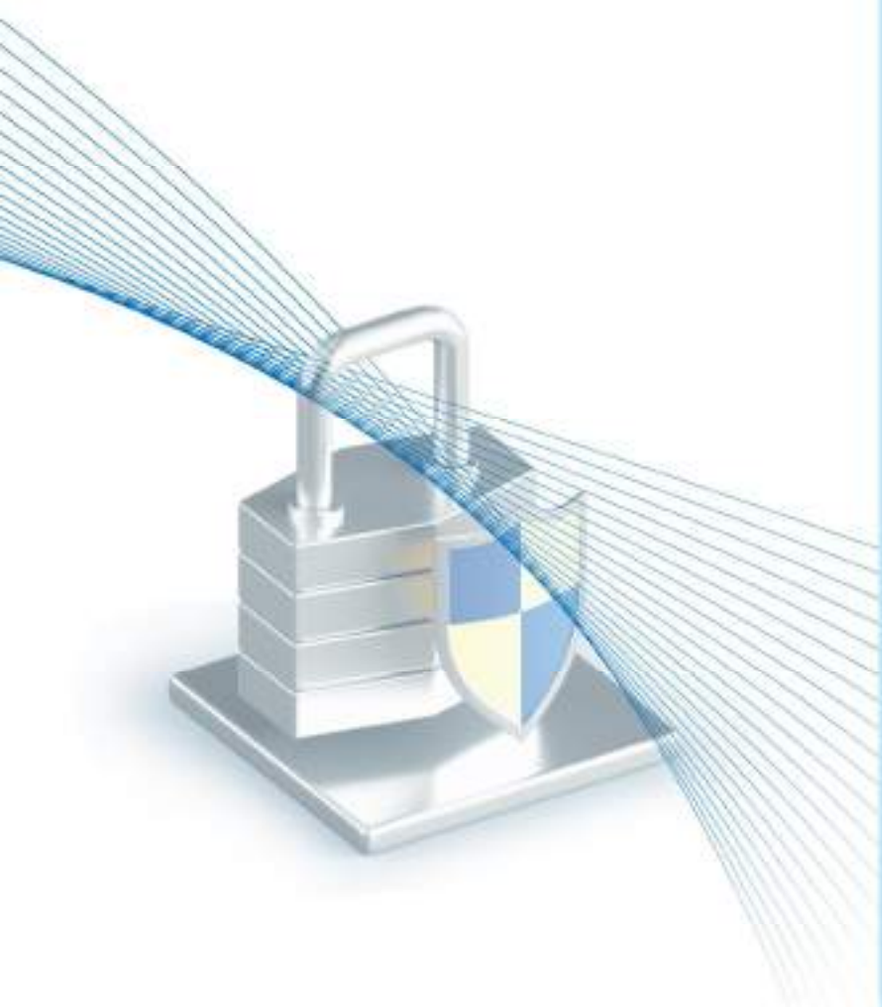
※ Windows 10

시작 우측 웹 및 Windows 검색> "cmd.exe" 검색> 우클릭> "관리자 권한으로 실행" 또는, 시작> 모든 앱> Windows 시스템> 명령 프롬프트> 우클릭> 자세히> "관리자 권한으로 실행"



Ⅱ

DBMS



DBMS 취약점 분석·평가 항목

분류	점검항목	항목 중요도	항목코드
1. 계정관리	기본 계정의 패스워드, 권한 등을 변경하여 사용	상	D-01
	scott 등의 Demonstration 및 불필요 계정을 제거하거나 잠금 설정 후 사용	상	D-02
	패스워드의 사용기간 및 복잡도를 기관 정책에 맞도록 설정	상	D-03
	데이터베이스 관리자 권한을 꼭 필요한 계정 및 그룹에 허용	상	D-04
	패스워드 재사용에 대한 제약이 설정되어 있는가?	중	D-12
	DB 사용자 계정 개별적 부여하여 사용하고 있는가?	중	D-13
2. 접근관리	원격에서 DB 서버로의 접속 제한	상	D-05
	DBA 이외의 인가되지 않은 사용자 시스템 테이블에 접근할 수 없도록 설정	상	D-06
	오라클 데이터베이스의 경우 리스너의 패스워드를 설정하여 사용	상	D-07
	불필요한 ODBC/OLE-DB 데이터 소스와 드라이브 제거하고 사용하고 있는가?	중	D-14
	일정 횟수의 로그인 실패 시 이에 대한 잠금정책이 설정되어 있는가?	중	D-15
	데이터베이스의 주요 파일 보호 등을 위해 DB 계정의 umask를 022 이상으로 설정하여 있는가?	하	D-16
	데이터베이스의 주요 설정파일, 패스워드 파일 등과 같은 주요 파일들의 접근 권한 설정되어 있는가?	중	D-17
	관리자 이외의 사용자가 오라클 리스너의 접속을 통해 리스너 로그 및 trace 파일에 대한 변경이 가능하지 않는가?	하	D-18
3. 옵션관리	응용프로그램 또는 DBA 계정의 Role 이 Public으로 설정되지 않도록 조정	상	D-08
	OS_ROLES, REMOTE_OS_AUTHENTICATION, REMOTE_OS_ROLES를 FALSE로 설정	상	D-09
	패스워드 확인함수가 설정되어 적용되는가?	중	D-19
	인가되지 않은 Object Owner 가 존재하지 않는가?	하	D-20
	grant option 이 role 에 의해 부여되도록 설정되어 있는가?	중	D-21
	데이터베이스의 자원 제한 기능을 TRUE 로 설정하고 있는가?	하	D-22
4. 패치관리	데이터베이스에 대해 최신 보안패치와 밴더 권고사항을 모두 적용	상	D-10
	데이터베이스의 접근, 변경, 삭제 등의 감사기록이 기관의 감사기록 정책에 적합하도록 설정	상	D-11
	보안에 취약하지 않은 버전의 데이터베이스를 사용하고 있는가?	중	D-23
5. 로그관리	Audit Table은 데이터베이스 관리자 계정에 속해 있도록 설정되어 있는가?	하	D-24

DBMS

D-01 (상)	1. 계정 관리 > 1.1 기본 계정의 패스워드, 정책 등을 변경하여 사용
취약점 개요	
점검내용	■ DBMS 기본 계정의 디폴트 패스워드 및 권한 정책을 변경하여 사용하는지 점검
점검목적	■ DBMS 기본 계정의 디폴트 패스워드 및 권한 정책 변경 사용 유무를 점검하여 비인가자의 디폴트 패스워드 대입 공격을 차단하고 있는지 확인하기 위함
보안위협	■ DBMS 기본 계정 디폴트 패스워드 및 권한 정책을 변경하지 않을 경우 비인가자가 인터넷 통해 DBMS 기본 계정의 디폴트 패스워드를 획득하여 디폴트 패스워드를 그대로 사용하고 있는 DB에 접근하여 기본 계정에 부여된 권한의 취약점을 이용하여 DB 정보를 유출 할 수 있는 위험이 존재함
참고	※ **기본 계정:** DB 설치 후 초기에 기본으로 생성되어 있는 DBMS 관리용 계정(예 sa) ※ **디폴트 패스워드:** 관리자 계정(예: sa)에 기본으로 지정되어 있는 패스워드
점검대상 및 판단기준	
대상	■ Oracle, MSSQL, MySQL, ALTIBASE, TIBERO 등
판단기준	**양호 :** 기본 계정의 디폴트 패스워드 및 권한 정책을 변경하여 사용하는 경우
	취약 : 기본 계정의 디폴트 패스워드 및 권한 정책을 변경하지 않고 사용하는 경우
조치방법	기본(관리자) 계정의 디폴트 패스워드 및 권한 정책 변경
점검 및 조치 사례	

■ **Oracle**

Step 1) 사용되는 계정인 경우 계정의 기본 패스워드 변경 후 사용

SQL> `alter user username identified by new_passwd;`

※ 그 이외에 객체 권한 부여 , 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	Password
scott	tiger or tigger	system	manager
dbsnmp	dbsnmp	sys	changeon_install
tracesvr	trace	outln	outln
ordplugins	ordplugins	ordsys	ordsys
ctxsys	ctxsys	mdsys	mdsys
adams	wood	blake	papr
clark	clth	jones	steel
lbacsys	lbacsys		

DBMS

D-01 (상)	1. 계정 관리 > 1.1 기본 계정의 패스워드, 정책 등을 변경하여 사용

■ **MSSQL**

Step 1) sa 계정 패스워드 변경

```
Alter login sa with password='new password';
```

■ **MySQL**

Step 1) 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');
```

■ **Altibase**

조치방법 1.

Step 1) 다음 명령어를 통해 패스워드 정책 설정 여부 확인

```
select * from system_.sys_users_;
```

Step 2) alter user 명령어로 패스워드 변경

알티베이스 서버에 sys 유저로 접속 후 alter user 명령어로 패스워드를 변경

```
ALTER USER sys IDENTIFIED BY "New_passwd";
```

조치방법 2.

Step 1) altipasswd 명령어로 패스워드 변경

알티베이스 서버 온라인 상태에서 수행

```
$ altipasswd
Previous Password : old_password
New Password : new_password
Retype New Password : new_password
```

■ **Tibero**

Step 1) sys 계정 패스워드 변경

```
ALTER USER sys IDENTIFIED BY  "New_passwd";
```

※ 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

D-01 (상)	1. 계정 관리 > 1.1 기본 계정의 패스워드, 정책 등을 변경하여 사용
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

D-02 (상)	1. 계정 관리 > 1.2 scott 등의 Demonstration 및 불필요 계정을 제거하거나 잠금 설정 후 사용
취약점 개요	
점검내용	■ DBMS에 존재하는 계정 중 DB 관리나 운용에 사용하지 않는 불필요한 계정이 존재하는지 점검
점검목적	■ 불필요한 계정 존재 유무를 점검하여 불필요한 계정 정보(패스워드)의 유출 시 발생할 수 있는 비인가자의 DB 접근에 대비되어 있는지 확인하기 위함
보안위협	■ DB 관리나 운용에 사용하지 않는 불필요한 계정이 존재할 경우 비인가자가 불필요한 계정을 이용하여 DB에 접근하여 데이터를 열람, 삭제, 수정할 위험이 존재함
참고	※ **불필요한 계정:** SCOTT, PM, ADAMS, CLARK 등의 Demonstration 계정 및 퇴사나 직무 변경 등으로 더 이상 사용하지 않는 계정
점검대상 및 판단기준	
대상	■ Oracle, MSSQL, MySQL, ALTIBASE, TIBERO 등
판단기준	**양호 :** 계정 정보를 확인하여 불필요한 계정이 없는 경우
	취약 : 인가되지 않은 계정, 퇴직자 계정, 테스트 계정 등 불필요한 계정이 존재하는 경우
조치방법	계정별 용도를 파악한 후 불필요한 계정 삭제
점검 및 조치 사례	

■ **Oracle**

Step 1) 불필요한 Demonstration 계정 및 오브젝트 삭제

```
SQL> DROP USER '삭제할 계정';
```

Step 2) 계정 잠금/만료

```
SQL> ALTER USER '잠금/만료 계정' ACCOUNT LOCK PASSWORD EXPIRE;
```

■ **MSSQL**

Step 1) 불필요한 계정 삭제

```
Exec sp_droplogin '삭제할 계정';
```

■ **MySQL**

Step 1) 불필요한 계정 삭제

```
mysql> Delete from user where user='삭제할 계정';
```

D-02 (상)	1. 계정 관리 > 1.2 scott 등의 Demonstration 및 불필요 계정을 제거하거나 잠금 설정 후 사용

■ **Altibase**

Step 1) 모든 사용자 확인

```
select * from system_.sys_users_;
```

Step 2) 불필요한 계정 삭제

```
DROP USER user_name CASCADE;
```

■ **Tibero**

Step 1) 모든 사용자 확인

Tibero에서는 사용자의 정보를 제공하기 위해 아래 나열된 정적 뷰를 제공하고 있음. DBA나 일반 사용자 모두 사용할 수 있다.

정적 뷰	설명
ALL_USERS	데이터베이스의 모든 사용자의 기본적인 정보를 조회하는 뷰
DBA_USERS	데이터베이스의 모든 사용자의 자세한 정보를 조회하는 뷰
USER_USERS	현재 사용자의 정보를 조회하는 뷰

```
select * from all_users;
select * from dba_users;
select * from user_users;
```

Step 2) 불필요한 계정 삭제

```
DROP USER user_name CASCADE;
```

조치 시 영향	Demonstration 계정 / 오브젝트 사용 불가 / 삭제된 계정 사용 불가

DBMS

D-03 (상)	1. 계정 관리 > 1.3 패스워드의 사용기간 및 복잡도를 기관 정책에 맞도록 설정
취약점 개요	
점검내용	■ 기관 정책에 맞게 패스워드 사용기간 및 복잡도 설정이 적용되어 있는지 점검
점검목적	■ 패스워드 사용기간 및 복잡도 설정 유무를 점검하여 비인가자의 패스워드 추측 공격(무작위 대입 공격, 사전 대입 공격 등)에 대한 대비가 되어 있는지 확인하기 위함
보안위협	■ 패스워드 사용기간 및 복잡도 설정이 되어 있지 않을 경우 비인가자가 패스워드 추측 공격을 통해 획득한 계정의 패스워드를 이용하여 DB에 접근할 수 있는 위험이 존재함
참고	※ **무작위 대입 공격(Brute Force Attack):** 특정 암호를 해독하기 위해 가능한 모든 값을대입하는 공격 방법 ※ **사전 대입 공격(Dictionary Attack):** 사전에 있는 단어를 입력하여 패스워드를 알아내거나 암호를 해독하는데 사용되는 컴퓨터 공격 방법
점검대상 및 판단기준	
대상	■ Oracle, MSSQL, MySQL, ALTIBASE, TIBERO 등
판단기준	**양호 :** 기관 정책에 맞게 패스워드 사용기간 및 복잡도 설정이 적용되어 있는 경우
	취약 : 기관 정책에 맞게 패스워드 사용기간 및 복잡도 설정이 적용되어 있지 않은 경우
조치방법	기관 정책에 맞게 패스워드 사용기간 및 복잡도 정책 설정
점검 및 조치 사례	

■ **Oracle**

Step 1) PASSWORD_LIFE_TIME 프로파일 파라미터 변경

```
SQL> ALTER PROFILE LIMIT PASSWORD_LIFE_TIME xx;
```

Step 2) 프로파일 값과 관련된 사용자 변경

```
SQL> ALTER USER PROFILE;
```

STEP 3) 패스워드 설정 변경

```
SQL> CREATE PROFILE grace_5 LIMIT;
FAILED_LOGIN_ATTEMPTS 3 (패스워드 실패 3번 까지만 가능)
PASSWORD_LIFE_TIME 30 (30일 동안만 패스워드 사용 가능)
PASSWORD_REUSE_TIME 30 (사용한 패스워드 30일 후부터 재사용 가능)
PASSWORD_VERIFY_FUNCTION verify_function
PASSWORD_GRACE_TIME 5 ; (life time이 끝나고 5일 동안 메시지를 보여줌)
```

D-03 (상)	1. 계정 관리 > 1.3 패스워드의 사용기간 및 복잡도를 기관 정책에 맞도록 설정

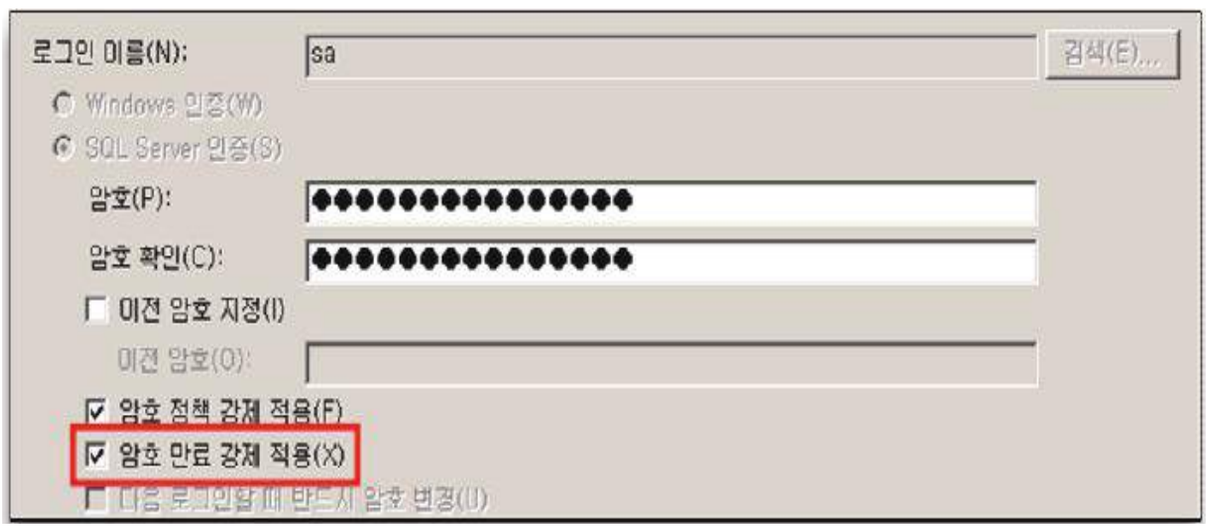
■ **MSSQL**

Step 1) 패스워드 변경 주기가 60일 이내로 설정되지 않은 경우 패스워드 변경 주기 설정

MSSQL에서 '암호 만료 강제 적용'을 체크함으로써 주기적으로 변경이 가능하며, 변경기간은 OS의 '암호정책'에서 적용 받으므로 '암호 정책 > 최대 암호 사용 기간' 설정도 같이 변경해야 함

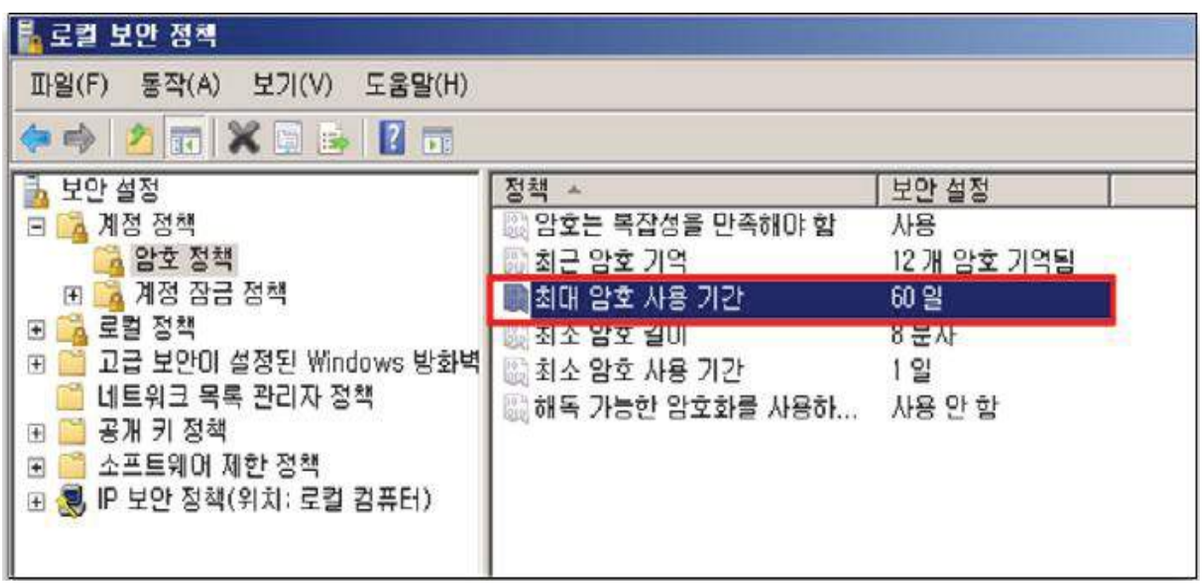
Step 2) 암호 만료 강제 적용

[보안]> [로그인]> [각 로그인 계정]> [속성]> 암호 만료 강제 적용: 설정(체크) 확인



STEP 3) OS의 암호 정책 설정

[관리도구]> [로컬 보안 정책]> [보안 설정]> [계정 정책]> [암호 정책]> '최대 암호 사용 기간 : '60일' 설정



DBMS

D-03 (상)	1. 계정 관리 > 1.3 패스워드의 사용기간 및 복잡도를 기관 정책에 맞도록 설정

■ **MySQL**

Step 1) 패스워드 설정 규칙 적용

패스워드 설정 규칙에 맞추어 패스워드를 설정할 수 있도록 시스템 차원에서 기능 제공

Step 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)

STEP 3) 패스워드 변경기능 구현

사용자가 패스워드 설정규칙 내에서 스스로 패스워드를 변경할 수 있도록 기능 제공 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;
```

■ **Altibase**

조치방법 1. 사용자별 패스워드 정책 변경

Step 1) 다음 명령어를 통해 패스워드 정책 설정 여부 확인

```
select * from system_.sys_users_;
```

Step 2) 아래 프로퍼티에 대해 패스워드 정책 설정

```
CASE_SENSITIVE_PASSWORD
FAILED_LOGIN_ATTEMPTS
PASSWORD_LOCK_TIME
PASSWORD_LIFE_TIME
PASSWORD_GRACE_TIME
PASSWORD_REUSE_TIME
PASSWORD_REUSE_MAX
PASSWORD_VERIFY_FUNCTION
```

정책 적용 시 다음 명령어를 사용

ALTER USER 유저명 LIMIT (프러퍼티 숫자);

적용 예)

```
ALTER USER TESTUSER LIMIT
        (FAILED_LOGIN_ATTEMPTS 7, PASSWORD_LOCK_TIME 7);
```

D-03 (상)	1. 계정 관리 > 1.3 패스워드의 사용기간 및 복잡도를 기관 정책에 맞도록 설정

조치방법 2. ALTIBASE HDB 프러퍼티 파일

Step 1) `$ALTIBASE_HOME/conf/altibase.properties`를 변경

※ ALTIBASE HDB 서버가 실행되지 않은 상태에서 할 수 있는 정적인 환경 설정 방법

※ 프로퍼티 파일에서 해당 구성 요소를 특정 값으로 설정한 후 ALTIBASE HDB 서버를 재구동해야 수정된 값이 ALTIBASE HDB 서버에 반영

■ **Tibero**

Step 1) 사용자별 패스워드 프로파일 적용 여부 확인

```
select * from dba_users;
```

#	USERNAME	USER_ID	PASS...	A	L...	E..	DEFAULT_TA...	CREATED	PROFILE	DEFAULT_T
1	SYS	0	VI9t1I...	C	<...	<..	SYSTEM	2015/11/23	<NULL>	TEMP
2	SYSCAT	13	VI9t1I...	C	<...	<..	SYSTEM	2015/11/23	<NULL>	TEMP
3	SYSGIS	14	VI9t1I...	C	<...	<..	SYSTEM	2015/11/23	<NULL>	TEMP
4	OUTLN	15	VI9t1I...	C	<...	<..	USR	2015/11/23	<NULL>	TEMP
5	TIBERO	18	+N2T...	C	<...	<..	USR	2015/11/23	<NULL>	TEMP
6	TIBERO1	19	+N2T...	C	<...	<..	USR	2015/11/23	<NULL>	TEMP
7	TESTUSER	20	hLb0j...	C	<...	<..	USR	2015/11/23	<NULL>	TEMP
8	TEST1	21	hLb0j...	C	<...	<..	USR	2015/11/23	DEFAULT	TEMP

Step 2) 설정되어 있을 경우 프로파일 설정 내용 확인

```
select * from dba_profiles;
```

#	PROFILE	RESOURCE_NAME	RESOURCE_TYPE	LIMIT
1	DEFAULT	FAILED_LOGIN_ATTEMPTS	PASSWORD	UNLIMITED
2	DEFAULT	PASSWORD_LIFE_TIME	PASSWORD	UNLIMITED
3	DEFAULT	PASSWORD_REUSE_TIME	PASSWORD	UNLIMITED
4	DEFAULT	PASSWORD_REUSE_MAX	PASSWORD	UNLIMITED
5	DEFAULT	PASSWORD_VERIFY_FUNC...	PASSWORD	NULL_VERIFY_FUNCTION
6	DEFAULT	PASSWORD_LOCK_TIME	PASSWORD	1
7	DEFAULT	PASSWORD_GRACE_TIME	PASSWORD	UNLIMITED
8	DEFAULT	LOGIN_PERIOD	PASSWORD	UNLIMITED

STEP 3) 설정되어 있지 않을 경우 프로파일 생성 시(또는 수정 시 alter profile) 패스워드 정책 설정 정책 적용 시 다음 명령어를 사용

```
CREATE PROFILE prof LIMIT
```

적용 예)

```
CREATE PROFILE prof LIMIT
        failed_login_attempts 3
        password_lock_time 1/1440
        password_life_time 90
        password_reuse_time unlimited
        password_reuse_max 10
        password_grace_time 10
        password_verify_function verify_function;
```

조치 시 영향	주기적인 패스워드 변경 필요

DBMS

D-04 (상)	1. 계정 관리 > 1.4 데이터베이스 관리자 권한을 꼭 필요한 계정 및 그룹에 허용
취약점 개요	
점검내용	■ 관리자 권한이 필요한 계정 및 그룹에만 관리자 권한을 부여하였는지 점검
점검목적	■ 관리자 권한이 필요한 계정과 그룹에만 관리자 권한을 부여하였는지 점검하여 관리자 권한의 남용을 방지하여 계정 유출로 인한 비인가자의 DB 접근 가능성을 최소화 하고자 함
보안위협	■ 관리자 권한이 필요한 계정 및 그룹에만 관리자 권한을 부여하지 않을 경우 관리자 권한이 부여된 계정이 비인가자에게 유출될 경우 DB에 접근할 수 있는 위험이 존재함
참고	-
점검대상 및 판단기준	
대상	■ Oracle, MSSQL, MySQL, ALTIBASE, TIBERO 등
판단기준	**양호 :** 관리자 권한이 필요한 계정 및 그룹에만 관리자 권한이 부여된 경우
	취약 : 관리자 권한이 필요 없는 계정 및 그룹에 권한이 부여된 경우
조치방법	관리자 권한이 필요한 계정 및 그룹에만 관리자 권한 부여
점검 및 조치 사례	

■ **Oracle**

Step 1) SYSDBA 권한 점검

```
SQL> 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)

Step 2) Admin에 부적합 계정 존재 여부 점검

```
SQL> 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)

Step 3) 관리자 권한이 불필요한 계정에서 관련 권한을 제거

※ 불필요하게 시스템 권한을 부여한 계정의 권한 변경 필요
※ 시스템 권한 부여가 필요한 경우 필요한 테이블별 권한 부여
※ 인가된 사용자는 관리자 권한에 role을 grant한 후, 시스템 권한을 grant하고 role을 인가된 사용자에게 grant 함

DBMS

D-04 (상)	1. 계정 관리 > 1.4 데이터베이스 관리자 권한을 꼭 필요한 계정 및 그룹에 허용

■ **MSSQL**

Step 1) sysadmin 서버 역할의 계정 목록을 확인 후 해당 서버 역할에 불필요한 계정이 있는 경우 서버 역할에서 삭제

sysadmin 서버 역할에서 불필요한 계정 삭제

(명령어) `Exec sp_droprolemember 'user_name', 'sysadmin';`

(예) `Exec sp_dropsrvrolemember 'user01', 'sysadmin';`

(user01 계정을 sysadmin 서버 역할에서 삭제)

■ **MySQL**

Step 1) mysql.user 테이블에 적용된 권한은 모든 데이터베이스에 적용되므로 host, user, password를 제외한 나머지 권한은 허용하지 않음('N')으로 설정

1. 사용자 등록

```
mysql> insert into mysql.user (host, name, password) values('%', 'user name', password ('password'); ※ 디폴트로 모든 권한 'N' 설정
```

2. 권한 변경

```
mysql> update mysql.user set <권한>='N' where user='user name';
```

Step 2) 각 사용자는 접근하고자 하는 DB를 mysql.db에 등록 후 접근 권한을 부여하여 사용

1. 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', 'Y', 'Y', 'Y');
mysql> flush privileges;
```

2. DB 권한 업데이트

```
mysql> update mysql.db set <권한>='Y' where db=<DB name> and user='user name';
mysql> flush privileges;
```

■ **Altibase**

Step 1) 계정별 부여된 시스템 권한 목록 확인 후, 아래 명령어 모두 입력

```
select * from system_.sys_grant_system_;
select * from system_.sys_users_;
select * from system_.sys_privileges_;
```

Step 2) sys_users_ 결과값에서 user_id 확인

Step 3) sys_grant_system_ 결과값에서 user_id 와 동일한 grantee_id 확인하여 priv_id 확인

Step 4) 일반사용자 계정 생성 시 시스템에 의해 부여되는 기본 권한 외 입력되어 있을 경우 해당 권한 삭제

DBMS

D-04 (상)	1. 계정 관리 > 1.4 데이터베이스 관리자 권한을 꼭 필요한 계정 및 그룹에 허용

시스템에 의해 자동으로 부여되는 권한	privileged_id
create session	215
create table	217
create sequence	210
create procedure	205
create view	229
create trigger	241
create synonym	245
create materialized view	252
create library	256

■ **Tibero**

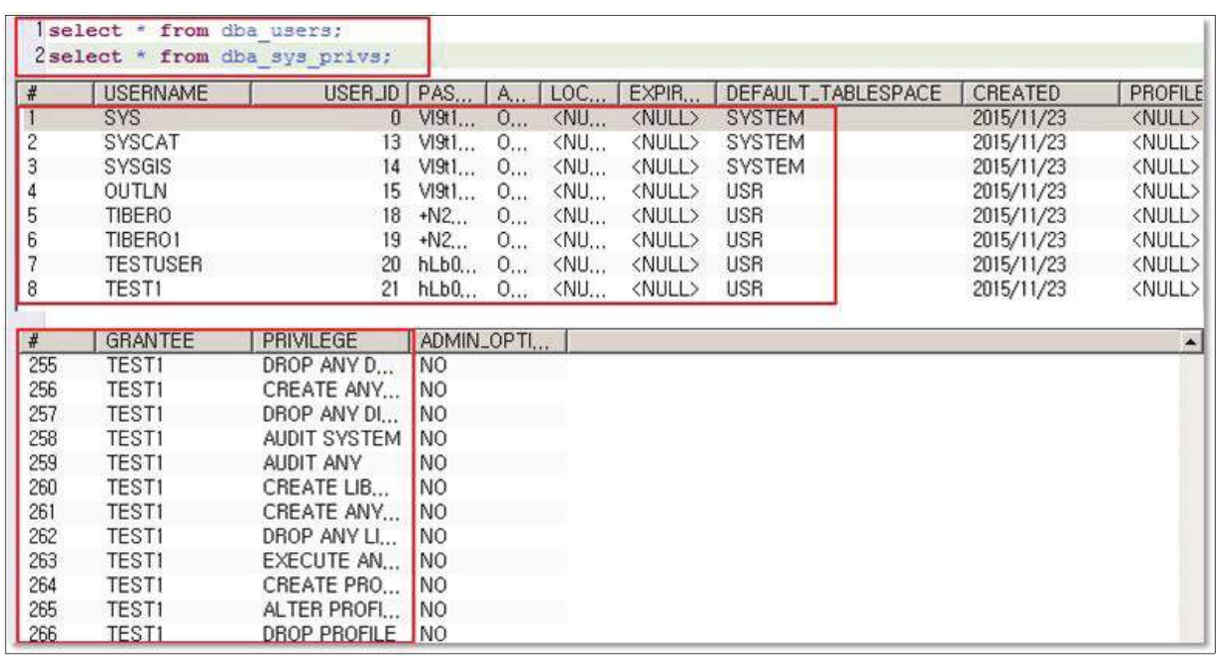
Step 1) 계정별 부여된 시스템 권한 목록 확인 후, 아래 명령어 모두 입력

```
select * from dba_users;
select * from dba_sys_privs;
```

Step 2) dbs_users 결과값에서 시스템 계정, 일반 계정 확인

Step 3) dba_sys_privs 결과값에서 일반 계정임에도 시스템 권한을 불필요하게 부여받고 있는지 확인

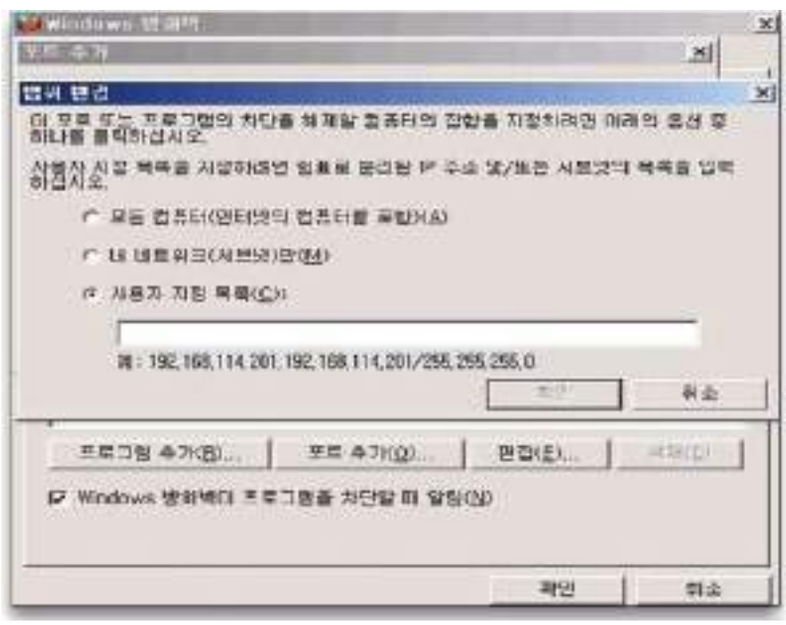
Step 4) 일반 계정에 불필요한 시스템 권한이 부여되어 있을 경우 권한 삭제



조치 시 영향	일반적으로 영향 없음

D-05 (상)	2. 접근 관리 > 2.1 원격에서 DB 서버로의 접속 제한
취약점 개요	
점검내용	■ 지정된 IP주소 만 DB 서버에 접근 가능하도록 설정되어 있는지 점검
점검목적	■ 지정된 IP주소 만 DB 서버에 접근 가능하도록 설정되어 있는지 점검하여 비인가자의 DB 서버 접근을 원천적으로 차단하고자 함
보안위협	■ DB 서버 접속 시 IP주소 제한이 적용되지 않은 경우 비인가자가 내·외부망 위치에 상관없이 DB 서버에 접근할 수 있는 위험이 존재함
참고	-
점검대상 및 판단기준	
대상	■ OS, Oracle, MySQL, ALTIBASE, TIBERO 등
판단기준	**양호 :** DB서버에 지정된 IP주소에서만 접근 가능하도록 제한한 경우
	취약 : DB서버에 지정된 IP주소에서만 접근 가능하도록 제한하지 않은 경우
조치방법	DB서버에 대해 지정된 IP주소에서만 접근 가능 하도록 설정
점검 및 조치 사례	

■ **OS**



Step 1) 특정 IP주소에서만 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

DBMS

D-05 (상)	2. 접근 관리 > 2.1 원격에서 DB 서버로의 접속 제한

■ **Oracle**

Step 1) 원격 OS 인증 방식이 불필요한 경우, SYS 계정으로 접속하여 'REMOTE_OS_AUTHENT=FALSE'로 설정

1. spfile 사용하는 경우 아래와 같이 설정

```
SQL> ALTER SYSTEM SET REMOTE_OS_AUTHENT=FALSE SCOPE=spfile;
```

2. pfile 사용하는 경우 init<SID>.ora 파일 안에 아래와 같이 설정

```
SQL> ALTER SYSTEM SET REMOTE_OS_AUTHENT=FALSE;
```

Step 2) OS 원격 인증 방식이 필요한 경우

1. 방화벽을 통한 원격 접근 IP주소 제한
2. NAT(Network Address Translation)를 사용하여 비공인 IP주소 부여 후 외부 접근 제한

■ **MySQL**

Step 1) mysql.user 테이블과 mysql.db 테이블을 조회하여 host가 "%"인 필드 삭제하고 접속 IP주소를 지정하여 등록

```
mysql> delete from user where host='%';
mysql> delete from db where host='%';
```

■ **Altibase**

ALTIBASE HDB 프러퍼티 파일을 수정하여 접근제어를 적용

Step 1) $ALTIBASE_HOME/conf/altibase.properties를 변경

Step 2) IP access control lists 에서 내부 정책에 맞게 수정

※ ALTIBASE HDB 서버가 실행되지 않은 상태에서 할 수 있는 정적인 환경 설정 방법

※ 프로퍼티 파일에서 해당 구성 요소를 특정 값으로 설정한 후 ALTIBASE HDB 서버를 재구동해야 수정된 값이 ALTIBASE HDB 서버에 반영

```
#============================================================
#  IP access control lists
#============================================================
# 1. The maximum number of entries is 128.
# 2. The IP addresses you specify must be valid addresses.
# 3. By default, all IPs are permitted to access the server.
# 4. The localhost addresses 127.0.0.1 and ::1 are always permitted.
# 5. If both a permit and a deny entry exist for the same IP, then
#    the permit entry will take precedence over the deny entry.
# 6. To deny access to all IPv4-addrs, add the following entry:
#     access_list = deny      0.0.0.0                 0.0.0.0
# 7. IPv6 addrs are meaningful only on servers on which IPv6 is enabled.
# 8. When using IPv6 addresses, do not use IPv4-mapped IPv6 addresses.
#
#  format
# IPv4 form: <permit|deny>, IPv4 addr, mask(d.d.d.d)
# IPv6 form: <permit|deny>, IPv6 addr, the length of prefix bits to be compared
#============================================================
# examples of IPv4 addresses.
#access_list = deny      0.0.0.0                 0.0.0.0
#access_list = permit    192.168.3.0             255.255.255.0
#access_list = permit    192.168.1.0             255.255.255.0
#access_list = permit    192.168.1.131           255.255.255.255
#============================================================
# examples of IPv6 addresses.
# deny all IPv6 addrs starting with 0 at bit0
#access_list = deny      ::1                     1
# deny all IPv6 addrs starting with 1 at bit0
#access_list = deny      fe80::                  1
#access_list = permit    ::1                     128
# permit all IPv6 addrs starting with 0xfe80
#access_list = permit    fe80::                  16
#============================================================
```

D-05 (상)	2. 접근 관리 > 2.1 원격에서 DB 서버로의 접속 제한

■ **Tibero**

※ 초기화 파라미터에 설정된 IP 주소에 따라 클라이언트의 네트워크 접속을 허용하거나 차단

※ $TB_SID 는 tibero 설치 시 입력한 데이터베이스 이름과 동일 / c:/tibero/tibero5/config/데이터베이스.tip

조치방법 1. LSNR_INVITED_IP

특정한 IP 주소를 갖는 클라이언트는 허용, 그 외 차단

Step 1) $TB_SID.tip 파일 안에 다음 예시 내용을 참조하여 입력

```
LSNR_INVITED_IP=192.168.1.1;192.168.2.0/24;192.1.0.0/16
```

※ LSNR_INVITED_IP의 최대 길이는 255자이다. 256 이상의 IP 주소를 설정할 경우에는 LSNR_INVITED_IP_FILE을 사용

조치방법 2. LSNR_INVITED_IP_FILE

특정 파일에 접속을 허용하는 IP 주소 목록을 기재한 후 해당 파일의 절대 경로를 적어주면 그 파일을 읽어서 INVITED_IP를 설정

Step 1) /home/tibero/invited_ip.txt 파일에 다음 예시 내용을 참조하여 입력

192.168.1.1
192.168.2.0/24
192.1.0.0/16

Step 2) $TB_SID.tip 파일에 invited_ip.txt 파일의 전체 경로를 입력

```
LSNR_INVITED_IP_FILE=/home/tibero/invited_ip.txt
```

조치방법 3. LSNR_DENIED_IP

특정한 IP 주소를 갖는 클라이언트의 네트워크 접속은 차단, 그 밖의 접속은 허용

Step 1) $TB_SID.tip 파일 안에 다음 예시 내용을 참조하여 입력

```
LSNR_DENIED_IP=192.168.1.1;192.168.2.0/24;192.1.0.0/16
```

조치방법 4. LSNR_DENIED_IP_FILE

특정 파일에 접속을 허용하지 않는 IP 주소 목록을 기재한 후 해당 파일의 절대 경로를 적어주면 그 파일을 읽어서 DENITED_IP를 설정

Step 1) /home/tibero/denied_ip.txt 파일에 다음 예시 내용을 참조하여 입력

192.168.1.1
192.168.2.0/24
192.1.0.0/16

Step 2) $TB_SID.tip 파일에 denied_ip.txt 파일의 전체 경로를 입력

```
LSNR_DENIED_IP_FILE=/home/tibero/denied_ip.txt
```

DBMS

D-05 (상)	2. 접근 관리 > 2.1 원격에서 DB 서버로의 접속 제한
● $TB_SID.tip 파일에 LSNR_INVITED_IP와 LSNR_DENIED_IP가 모두 설정되어 있는 경우 LSNR_DENIED_IP의 설정은 무시되며 LSNR_INVITED_IP만 적용된다. 즉, LSNR_INVITED_IP에 설정된 IP 주소의 클라이언트를 제외하고는 모든 접속이 차단된다. ● $TB_SID.tip 파일에 LSNR_INVITED_IP와 LSNR_DENIED_IP가 모두 설정되지 않은 경우 모든 클라이언트의 네트워크 접속이 허용된다. ● 루프백 주소(loopback address, 127.0.0.1)에서 접속하는 경우 LSNR_INVITED_IP 또는 LSNR_DENIED_IP의 설정과는 무관하게 항상 허용된다. ● Tibero 서버를 운영하는 중에 서버를 다시 기동하지 않고 LSNR_INVITED_IP 또는 LSNR_DENIED_IP의 설정을 변경하려는 경우 우선 $TB_SID.tip 파일에 LSNR_INVITED_IP 또는 LSNR_DENIED_IP의설정을 변경한 후 파일을 저장하고 다음의 명령을 실행한다. `- alter system listener parameter reload;` 위의 명령을 실행하면 $TB_SID.tip 파일에서 LSNR_INVITED_IP 또는 LSNR_DENIED_IP의 내용을 다시 읽어 변경된 내용을 실시간으로 적용한다.	
조치 시 영향	허용되지 않은 IP에서 접속 제한

D-06 (상)	2. 접근 관리 > 2.2 DBA 이외의 인가되지 않은 사용자가 시스템 테이블에 접근할 수 없도록 설정
취약점 개요	
점검내용	■ 시스템 테이블에 일반 사용자 계정이 접근할 수 없도록 설정되어 있는지 점검
점검목적	■ 시스템 테이블의 일반 사용자 계정 접근 제한 설정 적용 여부를 점검하여 일반 사용자 계정 유출 시 발생할 수 있는 비인가자의 시스템 테이블 접근 위험을 차단하기 위함
보안위협	■ 시스템 테이블의 일반 사용자 계정 접근 제한 설정이 되어 있지 않을 경우 객체, 사용자, 테이블 및 뷰, 작업 내역 등의 시스템 테이블에 저장된 정보가 누출될 수 있음
참고	-
점검대상 및 판단기준	
대상	■ Oracle, MSSQL, MySQL, ALTIBASE, TIBERO 등
판단기준	**양호 :** 시스템 테이블이 DBA 만 접근 가능하도록 설정되어 있는 경우
	취약 : 시스템 테이블이 DBA 외 일반 사용자 계정이 접근 가능하도록 설정되어 있는 경우
조치방법	-

점검 및 조치 사례

■ **Oracle, Tibero**

Step 1) DBA만 접근 가능한 테이블의 권한 확인(SQL*Plus)

```
SQL> select grantee, privilege, owner, table_name from dba_tab_privs where (o
wner='SYS' or table_name like 'DBA_%') and privilege <> 'EXECUTE' and grantee
not in ('PUBLIC', 'AQ_ADMINISTRATOR_ROLE', 'AQ_USER_ROLE', 'AURORA$JIS$UTILI
TY$', 'OSE$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', 'SELEC
T_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)

Step 2) 불필요하게 테이블 접근 권한이 사용자 계정에 할당된 경우(SQL*Plus)

```
SQL> REVOKE 권한 on 객체 FROM User;
```

DBMS

D-06 (상)	2. 접근 관리 > 2.2 DBA 이외의 인가되지 않은 사용자가 시스템 테이블에 접근할 수 없도록 설정

■ **MSSQL**

Step 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];
```

Step 2) 시스템 테이블에 접근하기 위해서는 stored procedure 또는, information_schema views를 통해 접근해야 함

Step 3) 시스템 테이블에 접근 가능한 stored procedure는 사용이 제한되어야 함

■ **MySQL**

Step 1) 일반 사용자로부터 mysql.user 테이블 모든 접근 권한 제거

```
mysql> revoke all on mysql.user from '[user name]'@'[hosts]';
mysql> flush privileges
```

Step 2) 일반 사용자로부터 mysql.user 테이블 접근 권한 제거

```
mysql> revoke [권한] on mysql.user from [user name];
mysql> flush privileges
```

■ **Altibase**

Step 1) sys_tables_ 조회하여 system_ 외 접근 계정 유무 확인

```
select * from system_.sys_tables_;
```

Step 2) 불필요 계정 접근 시 해당 접근 해제

조치 시 영향	일반 계정으로 시스템 테이블 접근 불가

D-07 (상)	2. 접근관리 > 2.3 리스너의 패스워드를 설정하여 사용
취약점 개요	
점검내용	■ 오라클 데이터베이스 Listener의 패스워드 설정 여부 점검
점검목적	■ Listener의 Owner는 DBA가 아니더라도 Listener를 shutdown 시키거나 DB 서버에 임의의 파일을 생성할 수 있으며, 원격에서 LSNRCTL 유틸리티를 사용하여 listener.ora 파일에 대한 변경이 가능하므로 Listener에 패스워드를 설정하여 비인가자가 이를 수정하지 못하도록 하기 위함
보안위협	■ Listener에 패스워드가 설정되지 않은 경우 DoS, 정보 획득, Listener 프로세서를 중지시킬 수 있는 위험이 있으므로 반드시 Listener 패스워드 설정 필요
참고	※ **오라클 Listener**: 클라이언트가 원격에서 오라클 DB에 접근할 때 접근 요청을 처리하기 위한 서버 쪽 프로세스, 혹은 네트워크 인터페이스를 말하며 일반적으로 TCP/1521 포트를 사용함 ※ **listener.ora**: 오라클 서버에서 클라이언트의 요청을 듣고, 클라이언트와의 통신 환경을 설정하는 파일
점검대상 및 판단기준	
대상	■ Oracle
판단기준	**양호:** Listener의 패스워드가 설정되어 있는 경우
	취약: Listener의 패스워드가 설정되어 있지 않은 경우
조치방법	Listener 패스워드 설정
점검 및 조치 사례	

■ **Oracle**

Step 1) Listener 패스워드 설정

```
LSNRCTL> change_password
  Old password:<Old Password> Not displayed
  New password:<New password> Not displayed
  Reenter new password:<New password> Not displayed
  Connecting
  (DESCRIPTION=(ADDRESS=(PROTOCOL=TCP)(HOST=prolin1)(PORT=1521)(IP=FIRST)))
  Password change for LISTENER
  The command completed successfully
LSNRCTL> set password
LSNRCTL> save_config
```

DBMS

D-07 (상)	2. 접근관리 > 2.3 리스너의 패스워드를 설정하여 사용
Step 2) Listener 매개변수 설정 1. $TNS_ADMIN/listener.ora 파일 안에 아래 Option 추가 PASSWORDS_<listener name>=<Encrypted Password> ADMIN_RESTRICTIONS_<listener name>=ON 2. LSNRCTL> reload Listener 재시작	
조치 시 영향	일반적인 경우 영향 없음

D-08 (상)	3. 옵션관리 > 3.1 응용프로그램 또는 DBA 계정의 Role 이 Public으로 설정되지 않도록 설정
취약점 개요	
점검내용	■ 응용프로그램 또는 DBA 계정의 Role을 Public으로 설정했는지를 점검
점검목적	■ 응용프로그램 또는 DBA 계정의 Role을 점검하여 일반계정으로 응용프로그램 테이블이나 DBA 테이블의 접근을 차단하기 위함
보안위협	■ 응용프로그램 또는 DBA 계정의 Role이 Public으로 설정되어 있으면, 일반계정에서도 응용프로그램 테이블 및 DBA 테이블로 접근할 수 있어 주요 정보 유출이 발생할 수 있음
참고	※ **Role**: 사용자에게 허가 할 수 있는 권한들의 집합
점검대상 및 판단기준	
대상	■ Oracle, MSSQL, ALTIBASE, TIBERO 등
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
점검 및 조치 사례	

■ **Oracle**

Step 1) DBA Role 설정 확인(SQL*Plus)

```
SQL> Select granted_role from dba_role_privs where grantee='PUBLIC';
```

위와 같이 롤(Role)이 설정되어 있는 경우 취약

Step 2) public 그룹의 권한 취소(SQL*Plus)

```
SQL> Revoke role from public;
```

■ **MSSQL**

Step 1) 각 Object의 사용 권한이 불필요하게 Public, Guest에 부여된 경우 권한 제거

Use database name

1. 권한 제거

```
REVOKE <권한> on <object> FROM public|guest;
```

2. 권한 부여

```
GRANT <권한> on <object> TO public|guest;
```

(예) syscolumns 테이블에 대한 SELECT 권한 제거

```
USE master
REVOKE select on sys.syscolumns FROM public;
```

DBMS

D-08 (상)	3. 옵션관리 > 3.1 응용프로그램 또는 DBA 계정의 Role 이 Public으로 설정되지 않도록 설정

※ 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

■ Altibase

Step 1) 사용자 정보를 조회하여 객체 권한, 시스템 권한이 public 또는 guest 에게 부여되어 있는지 확인

```
select * from system_.sys_users_;
select * from system_.sys_grant_object_;
select * from system_.sys_grant_system_;
```

GRANTOR_ID : 권한을 부여한 사용자의 식별자로, SYS_USERS_ 메타 테이블의 한 USER_ID 값과 동일하다.

GRANTEE_ID : 권한을 부여받은 사용자의 식별자로, SYS_USERS_ 메타 테이블의 한 USER_ID 값과 동일하다. 단, 객체 권한을 public 에게 부여한 경우, SYS_USERS_ 메타 테이블에 존재하지 않는 USER_ID 값인 "0"이 칼럼에 나타난다.

Step 2) 불필요 권한 회수

```
revoke 권한 on 객체 from 유저
```

■ Tibero

Step 1) 사용자 정보를 조회하여 role 부여가 적절한지 확인

```
select * from dba_role_privs;
select * from user_role_privs;
```

Step 2) 불필요 권한 회수

```
revoke 권한 from 유저;
```

※ USER_ROLE_PRIVS : 현재 사용자나 PUBLIC 사용자에 부여된 역할의 정보를 조회하는 뷰

조치 시 영향	일반적으로 영향 없음

D-09 (상)	3. 옵션관리 > 3.2 OS_ROLES, REMOTE_OS_AUTHENTICATION, REMOTE_OS_ROLES를 FALSE로 설정
취약점 개요	
점검내용	■ OS_ROLES, REMOTE_OS_AUTHENTICATION, REMOTE_OS_ROLES의 설정이 false 인지 여부를 점검
점검목적	■ OS_ROLES, REMOTE_OS_AUTHENTICATION, REMOTE_OS_ROLES의 설정을 점검하여 비인가자들의 데이터베이스 접근을 막고 데이터베이스 관리자에 의한 사용자 Role 설정이 가능하게 하기 위함
보안위협	■ OS_ROLES가 TRUE로 설정된 경우, 데이터베이스 접근 제어로 컨트롤되지 않는 OS 그룹에 의해 grant된 퍼미션이 허락됨 ■ REMOTE_OS_ROLES가 TRUE로 설정된 경우, 원격 사용자가 OS의 다른 사용자로 속여 데이터베이스에 접근할 수 있음 ■ REMOTE_OS_AUTHENT가 TRUE로 설정된 경우, 신뢰하는 원격 호스트에서 인증 절차 없이 데이터베이스에 접속할 수 있음
참고	※ **OS_ROLES**: OS 그룹에 의한 사용자의 롤 부여를 가능하게 할지를 설정 ※ **REMOTE_OS_AUTHENT**: 원격지의 OS 인증 허용여부를 설정 ※ **REMOTE_OS_ROLES**: OS가 원격 클라이언트에 대한 롤을 지정할 수 있게 할지를 설정
점검대상 및 판단기준	
대상	■ Oracle
판단기준	**양호 :** OS_ROLES, REMOTE_OS_AUTHENTICATION, REMOTE_OS_ROLES 설정이 FALSE로 되어있는 경우
	취약 : OS_ROLES, REMOTE_OS_AUTHENTICATION, REMOTE_OS_ROLES 정이 TRUE로 되어있는 경우
조치방법	OS_ROLES, REMOTE_OS_AUTHENTICATION, REMOTE_OS_ROLES 설정을 FALSE로 설정
점검 및 조치 사례	

■ **Oracle**

Step 1) 설정 확인(SQL*Plus)

1. OS_ROLES
   - `SQL> Show parameter os_roles;`
   - `SQL> select value from v$parameter where name='os_roles';`
   - OS_ROLES 파라미터를 FALSE로 설정

     `#vi /Oracle_HomeDirectory/admin/pfile/init.ora`에서 `OS_Role=False` 추가

DBMS

D-09 (상)	3. 옵션관리 > 3.2 OS_ROLES, REMOTE_OS_AUTHENTICATION, REMOTE_OS_ROLES를 FALSE로 설정
2. REMOTE_OS_AUTHENTICATION - SQL> Show parameter remote_os_authent; - SQL> Select value from v$parameter where name='remote_os_authent'; - init.ora 파일에서 remote_os_authent=FALSE 추가 pfile='$full_path/init.ora' 버전 9i 이후 버전은 SPFILE을 재생성해야 하므로, DBMS를 Shutdown 시키면 spfile이 재생성 됨 3. REMOTE_OS_ROLES - SQL> Show parameter remote_os_roles; - SQL> Select value from v$parameter where name='remote_os_roles'; - init.ora 파일에 remote_os_roles=FALSE 추가	
조치 시 영향	일반적으로 영향 없음

DBMS

D-10 (상)	4. 패치관리 > 4.1 데이터베이스에 대해 최신 보안패치와 밴더 권고사항을 모두 적용
취약점 개요	
점검내용	■ 최신 패치 및 벤더 권고사항 적용 여부 점검
점검목적	■ 정책에 따른 최신 보안패치 및 벤더 권고사항을 적용하여 데이터베이스의 보안성을 향상시키고자 함
보안위협	■ 데이터베이스의 주요 보안 패치 등을 설치하지 않은 경우, 공격자가 알려진 취약점을 이용하여 데이터베이스에 접근 가능함.
참고	-
점검대상 및 판단기준	
대상	■ Oracle, MSSQL, MySQL, ALTIBASE, TIBERO 등
판단기준	**양호 :** 정책에 따른 버전별 최신 패치를 적용하고 내부적으로 관리 절차를 수립하여 이행하고 있는 경우
	취약 : 정책에 따른 버전별 최신 패치를 적용하지 않거나 내부적으로 관리 절차를 수립하지 않은 경우
조치방법	데이터베이스에 대한 버전을 확인 후 업그레이드 및 패치 적용
점검 및 조치 사례	

■ **Oracle**

Step 1) ORACLE_HOME에 설치된 Oracle 제품 컴포넌트를 조회하거나, 적용된 임시 패치를 조회할 때는 lsinventory 명령어를 사용함

1. Oracle 제공 패치 명령을 이용하여 확인함

```
$opatchlsinventory[ -all ] [ -detail ]
[ -invPtrLoc ]
[ -jre ] [ -oh ]
```

all : ORACLE_BASE 밑에 설치된 모든 ORACLE_HOME 정보를 표시

detail : 설치된 패치 내에 포함된 라이브러리 파일까지 표시하므로 패치 적용 시 충돌되는 객체 파일을 확인 가능함

- **Unix 시스템**

```
$ORACLE_HOME/OPatch/opatchlsinventory –detail
```

- **Windows 시스템**

```
%ORACLE_HOME%\OPatch\opatchlsinventory -detail
```

http://metalink.oracle.com에서 최신 패치 버전 확인 후 opatch 명령을 통해 도출된 결과를 비교함

DBMS

D-10 (상)	4. 패치관리 > 4.1 데이터베이스에 대해 최신 보안패치와 밴더 권고사항을 모두 적용

- 버전이 9.2.0, 10.2.0, or 10.1.0이 아니면 아주 취약함
- Oracle 10g Release 2의 patchset level이 10.2.0.1이나 이후 버전이 아니면 취약함
- Oracle 10g Release 1의 patchset level이 10.1.0.4이나 이후 버전이 아니면 취약함
- Oracle 9i Release 2의 patchset level이 9.2.0.6이나 이후 버전이 아니면 취약함
- Oracle 9.0이 Oracle 9iAS 또는 Oracle AS10g를 지원하기 위해 사용되면 취약함

DBMS 버전	적용 패치 버전
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**

DBMS 버전	적용 패치 버전
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

D-10 (상)	4. 패치관리 > 4.1 데이터베이스에 대해 최신 보안패치와 밴더 권고사항을 모두 적용

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

■ **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 패치 된 릴리즈 사이트 http://downloads.mysql.com/archives.php
버그 현황 사이트 http://bugs.mysql.com/bugstats.php

■ **Altibase**

Step 1) 시스템에서 제품 버전 현황 확인

```
select * from v$database;
```

Step 2 Altibase 최신 패치 노트 확인
http://support.Altibase.com/kr/patch-note

Step 3) 패키지 인스톨러를 이용한 제품 패치
Altibase HDB 는 제품 패치를 위한 설치 파일이 따로 존재하지 않는다. 인스톨러를 시작할 때 설치 형태를 풀(full) 패키지 또는 패치로 선택할 수 있다. Altibase 고객지원서비스 포털 (http://support.Altibase.com/)을 방문하여 본인의 운영 체제에 적합한 인스톨러를 다운로드 받을 수 있음

DBMS

D-10 (상)	4. 패치관리 > 4.1 데이터베이스에 대해 최신 보안패치와 밴더 권고사항을 모두 적용

■ **Tibero**

Step 1) 시스템에서 제품 버전 현황 확인

```
tbboot -v
```

Step 2) Tibero 최신 패치 노트 확인

http://technet.tmaxsoft.com/

※ Tibero 패치 정책 (2015.02)

매 분기 초 픽스셋 발표 (년간 총 4회 배포 / fixset: hot fix 모음)

조치 시 영향	일반적인 경우 영향 없음

D-11 (상)	4. 패치관리 > 4.2 데이터베이스의 접근, 변경, 삭제 등의 감사기록이 기관의 감사기록 정책에 적합하도록 설정
취약점 개요	
점검내용	■ 감사기록 정책 설정이 기관 정책에 적합하게 설정되어 있는지 점검
점검목적	■ 데이터, 로그, 응용프로그램에 대한 감사 기록 정책을 수립하고 적용하여 데이터베이스에 문제 발생 시 원활하게 대응하고자 함
보안위협	■ 감사기록 정책이 설정되어 있지 않을 경우, 데이터베이스에 문제 발생 시 원인을 규명할 수 있는 자료가 존재하지 않아 이에 대한 대처 및 개선방안 수립이 어려움
참고	
점검대상 및 판단기준	
대상	■ Oracle, MSSQL, ALTIBASE, TIBERO 등
판단기준	**양호 :** DBMS의 감사 로그 저장 정책이 수립되어 있으며, 정책 설정이 적용되어 있는 경우
	취약 : DBMS에 대한 감사 로그 저장을 하지 않거나, 정책 설정이 적용되어 있지 않은 경우
조치방법	DBMS에 대한 감사 로그 저장 정책 수립, 적용
점검 및 조치 사례	

■ **Oracle**

Step 1) 데이터베이스 감사 기록 정책 및 백업 정책 수립

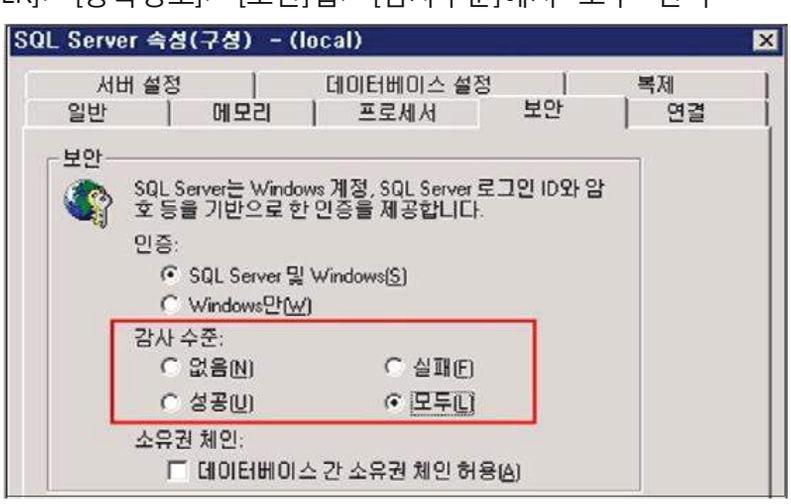
■ **MSSQL**

Step 1) 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

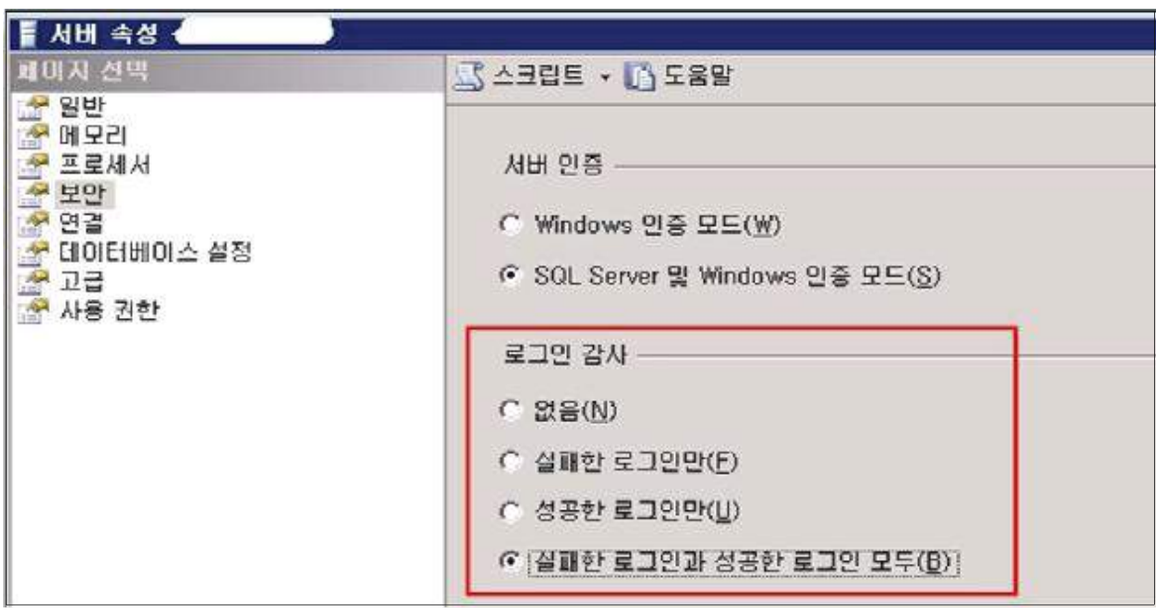


DBMS

D-11 (상)	4. 패치관리 > 4.2 데이터베이스의 접근, 변경, 삭제 등의 감사기록이 기관의 감사기록 정책에 적합하도록 설정

- **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

■ Altibase

Altibase HDB 서버 내에서 실행되고 있는 특정 구문 또는 모든 구문을 실시간으로 추적하고, 로그를 남기는 것을 감사(Audit)라고 함. SYS 사용자만이 이 구문을 사용해서 감사 조건을 설정할 수 있음

Step 1) AUDIT 구문으로 감사 정책을 설정

Step 2) 정책 설정 후 감사 조건 적용

```
ALTER SYSTEM STOP AUDIT;
ALTER SYSTEM START AUDIT;
ALTER SYSTEM RELOAD AUDIT;
```

■ Tibero

감사 기능은 감사의 대상에 따라 두 종류로 구분됨

1. 스키마 객체에 대한 감사
   지정된 스키마 객체에 수행되는 모든 동작을 기록할 수 있음
2. 시스템 특권에 대한 감사
   지정된 시스템 특권을 사용하는 모든 동작을 기록할 수 있음

D-11 (상)	4. 패치관리 > 4.2 데이터베이스의 접근, 변경, 삭제 등의 감사기록이 기관의 감사기록 정책에 적합하도록 설정

※ 감사를 설정하거나 해제하려면 다음 명령을 사용함
- audit (감사 설정)
- noaudit (감사 해제)

[감사 설정]

Step 1) 스키마 객체에 대한 감사

다른 사용자가 소유한 스키마의 객체 또는 디렉터리 객체를 감사하기 위해서는 AUDIT ANY 시스템 특권을 부여받아야함

< 감사 설정 예시 >

- AUDIT delete ON t BY SESSION WHENEVER SUCCESSFUL;
- 테이블에 수행되는 모든 delete 문이 성공하는 경우에만 감사 기록을 남김

Step 2) 시스템 특권에 대한 감사

시스템 특권을 감사하기 위해서는 AUDIT SYSTEM 시스템 특권을 부여받아야함

< 감사 설정 예시 >

- AUDIT create table BY Tibero;
- Tibero라는 사용자가 테이블을 생성하려고 할 때 그것이 성공하든 실패하든 관계없이 감사 기록을 남김

[감사 해제]

Step 1) 스키마 객체에 대한 감사 해제

다른 사용자가 소유한 스키마의 객체 또는 디렉터리 객체의 감사를 해제하기 위해서는 AUDIT ANY 시스템 특권을 부여받아야함

< 감사 해제 예시 >

- NOAUDIT delete ON t BY SESSION WHENEVER SUCCESSFUL;
- 테이블에 수행되는 모든 delete 문에 대해 더 이상 감사 기록을 남기지 않음

Step 2) 시스템 특권에 대한 감사 해제

시스템 특권의 감사를 해제하기 위해서는 AUDIT SYSTEM 시스템 특권을 부여받아야함

< 감사 해제 예시 >

- NOAUDIT create table BY Tibero;
- Tibero라는 사용자가 테이블을 생성할 때 더 이상 감사 기록을 남기지 않음

※ SYS 사용자 감사 설정 방법

Step 1) <$TB_SID.tip> 파일을 아래 내용처럼 입력 또는 수정

DBMS

D-11 (상)	4. 패치관리 > 4.2 데이터베이스의 접근, 변경, 삭제 등의 감사기록이 기관의 감사기록 정책에 적합하도록 설정
< SYS 사용자 감사 설정 예시 > - AUDIT_SYS_OPERATIONS=Y - AUDIT_FILE_DEST=/home/Tibero/audit/audit_trail.log - AUDIT_FILE_SIZE=10M SYS 사용자의 명령을 감사하도록 설정하면 수행한 모든 동작이 OS 파일에 기록되며 보안상의 이유로 데이터베이스에는 기록되지 않음	
조치 시 영향	일반적인 경우 영향 없음

D-12 (중)	1. 계정 관리 > 1.5 패스워드 재사용에 대한 제약의 설정
취약점 개요	
점검내용	■ 패스워드 변경 시 이전 패스워드를 재사용 할 수 없도록 패스워드 제약 설정이 되어 있는지 점검
점검목적	■ 패스워드 재사용 제약 설정 적용 여부를 점검하여 패스워드 변경 시 이전 패스워드 재사용을 제약하여 형식적인 패스워드 변경을 원천적으로 차단하기 위함
보안위협	■ 패스워드 재사용 제약 설정이 적용되어 있지 않을 경우 패스워드 변경 전 사용했던 패스워드를 재사용함으로써 비인가자의 계정 패스워드 추측 공격에 대한 시간을 더 많이 허용하여 패스워드 유출 위험이 증가함
참고	※ **패스워드 제약 설정:** 패스워드 변경 시 이전에 사용했던 패스워드를 재사용 할 수 없게 하는 설정으로써 이전 암호 재사용 가능 기간(PASSWORD_REUSE_TIME), 이전 암호 재사용 가능 횟수(PASSWORD_REUSE_MAX) 등이 있음
점검대상 및 판단기준	
대상	■ Oracle, ALTIBASE, TIBERO 등
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
점검 및 조치 사례	

■ **Oracle**

Step 1) (SQL*Plus) 설정확인

```
-- Check for both reuse max and reuse time not set:
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');
-- Check for reuse max with value that is less than allowed minimum
select profile from DBA_PROFILES where resource_name='PASSWORD_REUSE_MAX' and
limit not in ('UNLIMITED','NULL') and limit < '10';
-- Check for reuse time that is less than allowed minimum
select profile from DBA_PROFILES where resource_name='PASSWORD_REUSE_TIME' and
limit not in ('UNLIMITED','NULL')and limit < '365';
```

DBMS

D-12 (중)	1. 계정 관리 > 1.5 패스워드 재사용에 대한 제약의 설정

Step 2) PASSWORD_REUSE_TIME 및 프로파일 파라미터 수정

```
SQL> alter profile default limit password_reuse_time 365 password_reuse_max 10;
SQL> alter profile [profile name] limit password_reuse_time default
password_reuse_max default;
```

■ **Altibase**

조치방법 1. 사용자별 패스워드 정책 변경

Step 1) 다음 명령어를 통해 패스워드 정책 설정 여부 확인

```
select * from system_.sys_users_;
```

Step 2) 아래 프로퍼티에 대해 패스워드 정책 설정

```
CASE_SENSITIVE_PASSWORD
FAILED_LOGIN_ATTEMPTS
PASSWORD_LOCK_TIME
PASSWORD_LIFE_TIME
PASSWORD_GRACE_TIME
PASSWORD_REUSE_TIME
PASSWORD_REUSE_MAX
PASSWORD_VERIFY_FUNCTION
```

※ 정책 적용 시 다음 명령어를 사용

ALTER USER 유저명 LIMIT (프러퍼티 숫자);

적용 예) ALTER USER TESTUSER LIMIT (FAILED_LOGIN_ATTEMPTS 7, PASSWORD_LOCK_TIME 7);

조치방법 2. ALTIBASE HDB 프러퍼티 파일 $ALTIBASE_HOME/conf/altibase.properties를 변경

※ ALTIBASE HDB 서버가 실행되지 않은 상태에서 할 수 있는 정적인 환경 설정 방법

※ 프로퍼티 파일에서 해당 구성 요소를 특정 값으로 설정한 후 ALTIBASE HDB 서버를 재구동해야 수정된 값이 ALTIBASE HDB 서버에 반영

D-12 (중)	1. 계정 관리 > 1.5 패스워드 재사용에 대한 제약의 설정

■ **Tibero**

Step 1) 사용자별 패스워드 프로파일 적용 여부 확인

```
select * from dba_users;
```

#	USERNAME	USER_ID	PASS...	A	L...	E...	DEFAULT_TA...	CREATED	PROFILE	DEFAULT_T
1	SYS	0	VI9t1I...	C	<...	<..	SYSTEM	2015/11/23	<NULL>	TEMP
2	SYSCAT	13	VI9t1I...	C	<...	<..	SYSTEM	2015/11/23	<NULL>	TEMP
3	SYSGIS	14	VI9t1I...	C	<...	<..	SYSTEM	2015/11/23	<NULL>	TEMP
4	OUTLN	15	VI9t1I...	C	<...	<..	USR	2015/11/23	<NULL>	TEMP
5	TIBERO	18	+N2T...	C	<...	<..	USR	2015/11/23	<NULL>	TEMP
6	TIBERO1	19	+N2T...	C	<...	<..	USR	2015/11/23	<NULL>	TEMP
7	TESTUSER	20	hLb0j...	C	<...	<..	USR	2015/11/23	<NULL>	TEMP
8	TEST1	21	hLb0j...	C	<...	<..	USR	2015/11/23	DEFAULT	TEMP

Step 2) 설정되어 있을 경우 프로파일 설정 내용 확인

```
select * from dba_profiles;
```

#	PROFILE	RESOURCE_NAME	RESOURCE_TYPE	LIMIT
1	DEFAULT	FAILED_LOGIN_ATTEMPTS	PASSWORD	UNLIMITED
2	DEFAULT	PASSWORD_LIFE_TIME	PASSWORD	UNLIMITED
3	DEFAULT	PASSWORD_REUSE_TIME	PASSWORD	UNLIMITED
4	DEFAULT	PASSWORD_REUSE_MAX	PASSWORD	UNLIMITED
5	DEFAULT	PASSWORD_VERIFY_FUNC...	PASSWORD	NULL_VERIFY_FUNCTION
6	DEFAULT	PASSWORD_LOCK_TIME	PASSWORD	1
7	DEFAULT	PASSWORD_GRACE_TIME	PASSWORD	UNLIMITED
8	DEFAULT	LOGIN_PERIOD	PASSWORD	UNLIMITED

STEP 3) 설정되어 있지 않을 경우 프로파일 생성 시(또는 수정 시 alter profile) 패스워드 정책 설정 정책 적용 시 다음 명령어를 사용

```
CREATE PROFILE prof LIMIT
```

적용 예)

```
CREATE PROFILE prof LIMIT
        failed_login_attempts 3
        password_lock_time 1/1440
        password_life_time 90
        password_reuse_time unlimited
        password_reuse_max 10
        password_grace_time 10
        password_verify_function verify_function;
```

조치 시 영향	일반적으로 영향 없음

DBMS

D-13 (중)	1. 계정 관리 > 1.6 DB 사용자 계정의 개별적 부여 및 사용
취약점 개요	
점검내용	■ DB 접근 시 사용자 별로 서로 다른 계정을 사용하여 접근하는지 점검
점검목적	■ 사용자별 별도 DBMS 계정을 사용하여 DB에 접근하는지 점검하여 DB 계정 공유 사용으로 발생할 수 있는 로그 감사 추적 문제를 대비하고자 함
보안위협	■ DB 계정을 공유하여 사용할 경우 비인가자의 DB 접근 발생 시 계정 공유 사용으로 인해 로그 감사 추적의 어려움이 발생할 위험이 존재함
참고	-
점검대상 및 판단기준	
대상	■ Oracle, MSSQL, MySQL, ALTIBASE, TIBERO 등
판단기준	**양호 :** 사용자별 계정을 사용하고 있는 경우
	취약 : 공용 계정을 사용하고 있는 경우
조치방법	사용자별 계정 생성 및 권한 부여
점검 및 조치 사례	

■ **Oracle**

Step 1) 계정 확인(SQL*Plus)

```
SQL> select username from dba_users order by username;
```

(사용하지 않거나 모르는 계정 확인)

Step 2) 공통으로 사용하는 계정 삭제

```
SQL> DROP USER '삭제할 계정';
```

Step 3) 사용자별, 응용프로그램별 계정 생성

```
SQL> Create user username identified by passwd;
```

Step 4) 권한 부여

```
SQL> grant connect, resource to username;
```

■ **MSSQL**

Step 1) 불필요한 계정 삭제

```
Exec sp_droplogin '삭제할 계정'
```

Step 2). 사용자별, 응용프로그램별 계정 생성

```
CREATE login '생성 계정' WITH password = '패스워드'
CREATE user '생성 계정' FOR login '생성 계정' WITH default_schema ='생성 계정' ;
ALTER USER
EXEC sp_adduser '생성 계정', '생성 계정', 'db_owner'
EXEC sp_adduser '생성 계정', '생성 계정', '생성 계정'
EXEC sp_grantdbaccess '생성 계정','생성 계정'
```

D-13 (중)	1. 계정 관리 > 1.6 DB 사용자 계정의 개별적 부여 및 사용

■ **MySQL**

Step 1) 불필요한 계정 삭제

```
mysql> Delete from user where user='삭제할 계정';
```

Step 2) 사용자별, 응용프로그램별 계정 생성, 권한 설정

```
mysql> insert into user('localhost','user', 'password') values('localhost', '생성 계정', 'password('패스워드'));
mysql> insert into mysql.db values('%','DB name', 'username', 'Y', 'Y', 'Y', 'Y', 'Y', 'Y', 'Y', 'Y', 'Y', 'Y','Y', 'Y', 'Y', 'Y', 'Y', 'Y');
mysql> flush privileges
```

■ **Altibase**

Step 1) DB 에 생성된 계정 확인

```
select * from system_.sys_users_;
```

Step 2) Step 1) 결과에서 공용계정 확인하여 삭제

```
drop user testuesr cascade;
```

Step 3) 사용자별, 응용프로그램 별 등 목적에 맞게 계정 생성

```
create user testuser2 identified by testpassword;
```

■ **Tibero**

Step 1) DB 에 생성된 계정 확인

```
select * from dba_users;
```

Step 2) Step 1) 결과에서 공용계정 확인하여 삭제

```
drop user 사용자명 cascade;
```

Step 3) 사용자별, 응용프로그램 별 등 목적에 맞게 계정 생성

```
create user 사용자명 identified by 사용자 패스워드;
```

조치 시 영향	일반적으로 영향 없음

DBMS

D-14 (중)	2. 접근관리 > 2.4 불필요한 ODBC/OLE-DB 데이터 소스와 드라이브 제거 후 사용
취약점 개요	
점검내용	■ 사용하지 않는 불필요한 ODBC/OLE-DB가 설치되어 있는지 점검
점검목적	■ 불필요한 데이터 소스 및 드라이버를 제거함으로써 비인가자에 의한 데이터베이스 접속 및 자료 유출을 차단하기 위함
보안위협	■ 불필요한 ODBC/OLE-DB 데이터 소스를 통한 비인가자의 데이터베이스 접속 및 주요 정보 유출에 대한 위험이 발생할 수 있음
참고	※ 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
점검대상 및 판단기준	
대상	■ Windows OS
판단기준	**양호:** 불필요한 ODBC/OLE-DB가 설치되지 않은 경우
	취약: 불필요한 ODBC/OLE-DB가 설치된 경우
조치방법	불필요한 ODBC/OLE-DB 제거
점검 및 조치 사례	

■ Windows NT

Step 1) 사용하지 않는 불필요한 ODBC 데이터 소스 제거

시작> 설정> 제어판> 데이터 원본(ODBC)> 시스템 DSN

Step 2) 사용하지 않는 데이터 소스 제거

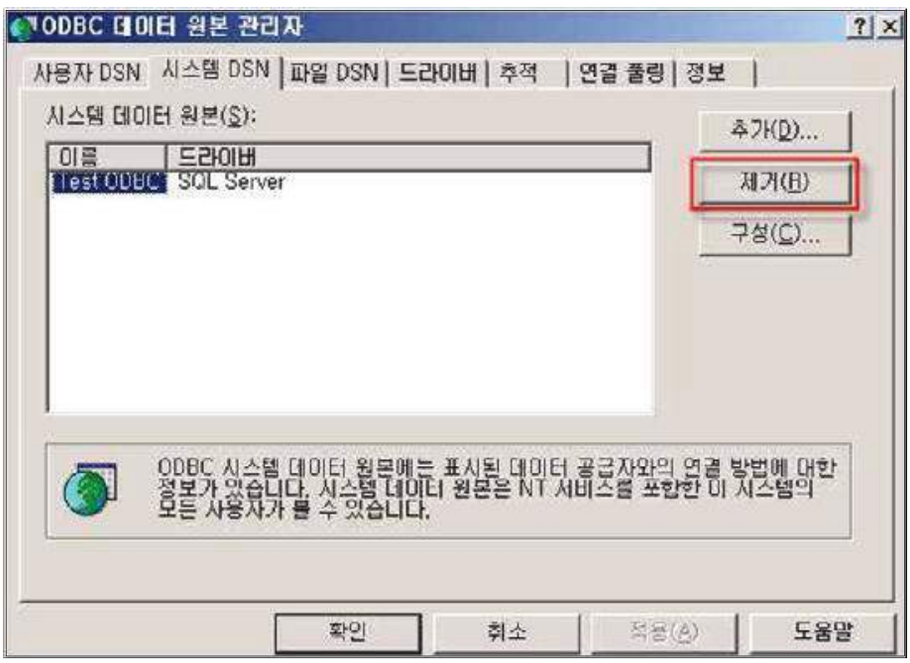
■ Windows 2000, 2003

Step 1) 사용하지 않는 불필요한 ODBC 데이터 소스 제거

시작> 설정> 제어판> 관리도구> 데이터 원본 (ODBC)> 시스템DSN> 해당 드라이브 클릭

Step 2) 사용하지 않는 데이터 소스 제거

D-14 (중)	2. 접근관리 > 2.4 불필요한 ODBC/OLE-DB 데이터 소스와 드라이브 제거 후 사용

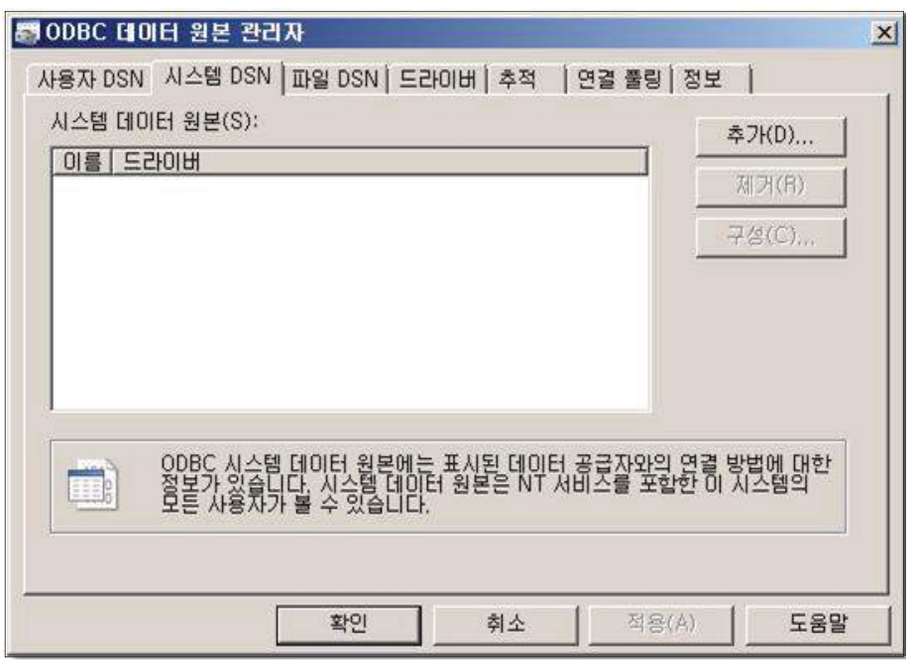


■ **Windows 2008**

Step 1) ODBC 사용하지 않는 불필요한 데이터 소스 제거

시작> 설정> 제어판> 관리도구> 데이터 원본 (ODBC)> 시스템DSN> 해당 드라이브 클릭

Step 2) 사용하지 않는 데이터 소스 제거



조치 시 영향	일반적인 경우 영향 없음

DBMS

D-15 (중)	2. 접근관리 > 2.5 일정 횟수의 로그인 실패 시 이에 대한 잠금정책 적용
취약점 개요	
점검내용	■ DBMS 설정 중 일정 횟수의 로그인 실패 시 계정 잠금 정책에 대한 설정이 되어 있는지 점검
점검목적	■ 일정 횟수의 로그인 실패 시 계정 잠금 정책을 설정하여 비인가자의 자동화된 무작위 대입 공격, 사전 대입 공격 등을 통한 사용자 계정 패스워드 유출을 방지하기 위함
보안위협	■ 일정한 횟수의 로그인 실패 횟수를 설정하여 제한하지 않으면 자동화된 방법으로 계정 및 패스워드를 획득하여 데이터베이스에 접근하여 정보를 유출할 수 있음
참고	-
점검대상 및 판단기준	
대상	■ Oracle, ALTIBASE, TIBERO 등
판단기준	**양호:** 로그인 시도 횟수를 제한하는 값을 설정한 경우
	취약: 로그인 시도 횟수를 제한하는 값을 설정하지 않은 경우
조치방법	로그인 시도 횟수 제한 값 설정
점검 및 조치 사례	

■ **Oracle**

Step 1) 접근 횟수 제한을 위해 파라미터 설정

`Failed_login_attempts` 프로파일 파라미터 수정

```
SQL> ALTER PROFILE LIMIT FAILED_LOGIN_ATTEMPTS XXX;
```

XXX회 이하로 설정

Step 2) 프로파일 적용

```
SQL> connect / as sysdba
SQL> @$Ora_Home/rdbms/admin/utlpwdmg.sql
```

또는, `default profile`에 `unlimited`로 설정하고 이 `default` 값을 적용하고자 하는 `profile`에 적용

```
SQL> Alter profile default limit password_lock_time unlimited;
SQL> Alter profile [profile name] limit password_lock_time default;
```

D-15 (중)	2. 접근관리 > 2.5 일정 횟수의 로그인 실패 시 이에 대한 잠금정책 적용

■ Altibase

조치방법 1. 사용자별 패스워드 정책 변경

Step 1) 다음 명령어를 통해 패스워드 정책 설정 여부 확인

```
select * from system_.sys_users_;
```

Step 2) 아래 프로퍼티에 대해 패스워드 정책 설정

```
CASE_SENSITIVE_PASSWORD
FAILED_LOGIN_ATTEMPTS
PASSWORD_LOCK_TIME
PASSWORD_LIFE_TIME
PASSWORD_GRACE_TIME
PASSWORD_REUSE_TIME
PASSWORD_REUSE_MAX
PASSWORD_VERIFY_FUNCTION
```

※ 정책 적용 시 다음 명령어를 사용

ALTER USER 유저명 LIMIT (프러퍼티 숫자);

적용 예) `ALTER USER TESTUSER LIMIT (FAILED_LOGIN_ATTEMPTS 7) ;`

조치방법 2. ALTIBASE HDB 프러퍼티 파일

$ALTIBASE_HOME/conf/altibase.properties를 변경

※ ALTIBASE HDB 서버가 실행되지 않은 상태에서 할 수 있는 정적인 환경 설정 방법

※ 프로퍼티 파일에서 해당 구성 요소를 특정 값으로 설정한 후 ALTIBASE HDB 서버를 재구동해야 수정된 값이 ALTIBASE HDB 서버에 반영

■ Tibero

Step 1) 사용자별 패스워드 프로파일 적용 여부 확인

```
select * from dba_users;
```

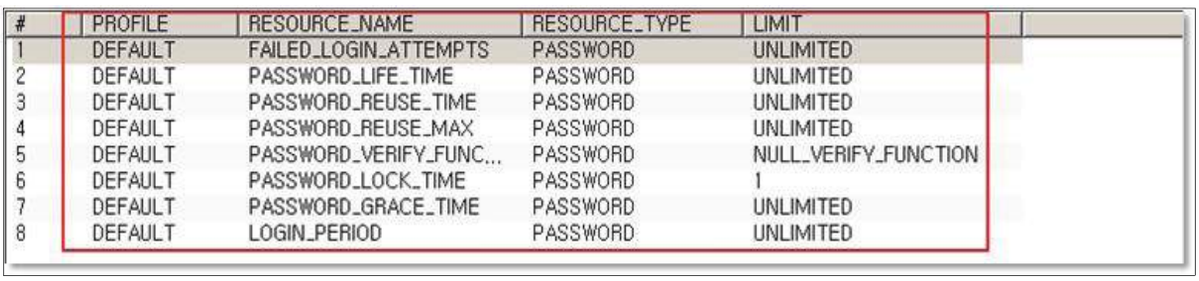
#	USERNAME	USER_ID	PASS...	A	L...	E..	DEFAULT_TA...	CREATED	PROFILE	DEFAULT_T
1	SYS	0	Vl9t1l...	C	<...	<..	SYSTEM	2015/11/23	<NULL>	TEMP
2	SYSCAT	13	Vl9t1l...	C	<...	<..	SYSTEM	2015/11/23	<NULL>	TEMP
3	SYSGIS	14	Vl9t1l...	C	<...	<..	SYSTEM	2015/11/23	<NULL>	TEMP
4	OUTLN	15	Vl9t1l...	C	<...	<..	USR	2015/11/23	<NULL>	TEMP
5	TIBERO	18	+N2T...	C	<...	<..	USR	2015/11/23	<NULL>	TEMP
6	TIBERO1	19	+N2T...	C	<...	<..	USR	2015/11/23	<NULL>	TEMP
7	TESTUSER	20	hLb0j...	C	<...	<..	USR	2015/11/23	<NULL>	TEMP
8	TEST1	21	hLb0j...	C	<...	<..	USR	2015/11/23	DEFAULT	TEMP

DBMS

D-15 (중)	2. 접근관리 > 2.5 일정 횟수의 로그인 실패 시 이에 대한 잠금정책 적용

Step 2) 설정되어 있을 경우 프로파일 설정 내용 확인

```
select * from dba_profiles;
```



#	PROFILE	RESOURCE_NAME	RESOURCE_TYPE	LIMIT
1	DEFAULT	FAILED_LOGIN_ATTEMPTS	PASSWORD	UNLIMITED
2	DEFAULT	PASSWORD_LIFE_TIME	PASSWORD	UNLIMITED
3	DEFAULT	PASSWORD_REUSE_TIME	PASSWORD	UNLIMITED
4	DEFAULT	PASSWORD_REUSE_MAX	PASSWORD	UNLIMITED
5	DEFAULT	PASSWORD_VERIFY_FUNC...	PASSWORD	NULL_VERIFY_FUNCTION
6	DEFAULT	PASSWORD_LOCK_TIME	PASSWORD	1
7	DEFAULT	PASSWORD_GRACE_TIME	PASSWORD	UNLIMITED
8	DEFAULT	LOGIN_PERIOD	PASSWORD	UNLIMITED

Step 3) 설정되어 있지 않을 경우 프로파일 생성 시(또는 수정 시 `alter profile`) 패스워드 정책 설정

※ 정책 적용 시 다음 명령어를 사용

```
CREATE PROFILE prof LIMIT
```

적용 예)

```
CREATE PROFILE prof LIMIT
        failed_login_attempts 3
        password_lock_time 1/1440
        password_life_time 90
        password_reuse_time unlimited
        password_reuse_max 10
        password_grace_time 10
        password_verify_function verify_function;
```

조치 시 영향	일반적인 경우 영향 없음

D-16 (하)	2. 접근관리 > 2.6 DB 계정의 umask를 022 이상으로 설정
취약점 개요	
점검내용	■ 사용자 계정의 umask 설정이 022 이상으로 설정되어 있는지 점검
점검목적	■ 소프트웨어 설치 때 생성되는 파일에 관리자를 제외한 일반 사용자의 파일 수정 권한을 제거함으로써 비인가자에 의한 DBMS 주요 파일 변경이나 삭제로부터 보호하기 위함
보안위협	■ umask를 "022" 이상으로 설정하지 않을 경우, 비인가자에 의한 데이터베이스의 주요 파일 변경, 삭제 등으로 데이터베이스 시스템 장애가 발생할 수 있음
참고	※ **umask:** 파일 및 디렉터리 생성 시 기본 권한을 지정해 주는 명령어 ※ 관련 점검 항목 : U-57(중) UMASK 설정 관리 ← 항목코드 최종 확인
점검대상 및 판단기준	
대상	■ Unix OS
판단기준	**양호:** 계정의 umask가 022 이상으로 설정되어있는 경우
	취약: 계정의 umask가 022 이상으로 설정되어 있지 않은 경우
조치방법	계정의 umask를 022 이상으로 설정 변경
점검 및 조치 사례	
■ **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 `# vi <file_name>` `umask 022`	
조치 시 영향	일반적으로 영향 없음

DBMS

D-17 (중)	2. 접근관리 > 2.7 주요 파일(설정파일, 패스워드 파일 등)들의 접근 권한 설정
취약점 개요	
점검내용	■ 데이터베이스의 주요 파일들에 대해 관리자를 제외한 일반 사용자의 파일 수정 권한을 제거하였는지 점검
점검목적	■ 데이터베이스의 주요 파일에 관리자를 제외한 일반 사용자의 파일 수정권한을 제거함으로써 비인가자에 의한 DBMS 주요 파일 변경이나 삭제를 방지하고 주요 정보 유출을 방지할 수 있음
보안위협	■ 데이터베이스 주요파일에 비인가자가 접근하여 수정 및 삭제를 하면 데이터베이스 운영에 장애가 발생할 수 있으며 계정 패스워드 정보 등의 중요한 정보가 유출될 수 있음
참고	※ **데이터베이스의 주요 파일:** orapw.ora, listener.ora,init<SID>.ora, redo 파일, 데이터베이스 설정 파일, 네트워크 설정 파일 등
점검대상 및 판단기준	
대상	■ Unix OS, Windows OS
판단기준	**양호:** 주요 설정 파일 및 디렉터리의 퍼미션 설정 시 일반 사용자의 수정 권한을 제거한 경우
	취약: 주요 설정 파일 및 디렉터리의 퍼미션 설정 시 일반 사용자의 수정 권한을 제거하지 않은 경우
조치방법	주요 설정 파일 및 디렉터리의 퍼미션 설정 변경
점검 및 조치 사례	

■ **Oracle**

- **Unix OS**

Step 1) 디렉터리 또는 파일의 퍼미션 점검

$ORACLE_HOME/bin/oracle (퍼미션 755)

$ORACLE_HOME/bin/ 아래 (퍼미션 755)

.sqlplus,sqlldr,sqlload,proc,oraenv,oerr,exp,imp,tkprof,tnsping,wrap

$ORACLE_HOME/bin 아래 (퍼미션 750)

.svrmgrl, lsnrctl, dbsnmp

$ORACLE_HOME/network (퍼미션 755)

$ORACLE_HOME/network/admin (퍼미션 755)

.listener.ora, sqlnet.ora 등

D-17 (중)	2. 접근관리 > 2.7 주요 파일(설정파일, 패스워드 파일 등)들의 접근 권한 설정

$ORACLE_HOME/lib (퍼미션 755)
$ORACLE_HOME/network/admin 아래 환경파일 (퍼미션 644)
.tnsnames.ora, protocol.ora, sqlpnet.ora
$ORACLE_HOME/dbs/init.ora (퍼미션 640)
$ORACLE_HOME/dbs/init<SID>.ora (퍼미션 640)
- Find $ORACLE_HOME –name init*.ora –print
- 파일 및 디렉터리의 퍼미션 설정 변경
 # chmod <적용 퍼미션> <file_name>

Step 2) redo 파일, 데이터베이스 설정 파일, 데이터 파일 위치 확인(SQL*Plus)

```
SQL> Select value from v$parameter where name='spfile';
SQL> Select 'Control Files: '||value from v$parameter where
name='control_files';
SQL> select 'Control Files: '||value from v$parameter where
name='spfile';
SQL> select 'Logfile: '||member from v$logfile;
SQL> select 'Datafile: '||name from v$datafile;
```

- 파일 및 디렉터리의 퍼미션 설정 변경
 # chmod <적용 퍼미션> <file_name>

- **Windows OS**

Step 1) 패스워드 파일(orapw<SID>) 접근 권한은 administrators, system group, owner group, oracle service account, DBA에게 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 Adminisrators, SYSTEM, Owner에게 모든 권한 또는, 그 이하로 설정하고 다른 그룹은 제거함

조치 시 영향	일반적으로 영향 없음

DBMS

D-18 (하)	2. 접근관리 > 2.8 관리자 이외의 사용자가 리스너 로그 및 trace 파일에 대한 변경을 제한
취약점 개요	
점검내용	■ 리스너 관련 설정 파일의 접근 권한을 관리자만 가능하게 하고 리스너 파라미터의 변경 방지에 대한 옵션 설정 여부 점검
점검목적	■ 리스너 설정 파일 및 파라미터 변경 방지 옵션을 설정하여 비인가자의 리스너를 이용한 파라미터 변경을 방지하여 trace 파일 및 리스너 로그의 신뢰도를 유지하기 위함
보안위협	■ 비인가자가 Oracle의 LSNRCTL 유틸리티를 이용하여 listener에 직접 접근 시 set 명령어를 이용하여 listener의 모든 파라미터를 변경할 수 있어서 trace 파일이나 listener 로그 파일을 변경할 수 있음
참고	※ **trace 파일:** 데이터베이스에 문제가 발생했을 시 문제를 진단하고 디버깅 할 수 있도록 다양한 정보를 제공하는 파일
점검대상 및 판단기준	
대상	■ Oracle
판단기준	**양호:** 리스너 관련 설정 파일에 대한 퍼미션이 관리자로 설정되어 있으며, 리스너로 파라미터를 변경할 수 없게 옵션을 설정했을 경우
	취약: 리스너 관련 설정 파일에 대한 퍼미션이 일반 사용자로 설정되어 있고, 리스너로 파라미터를 변경할 수 없게 옵션 설정을 하지 않았을 경우
조치방법	주요 파일 및 로그 파일에 대한 퍼미션을 관리자로 제한
점검 및 조치 사례	

■ **Oracle**

Step 1) 파일 퍼미션 확인

$ORACLE_HOME/network/admin 디렉토리의 퍼미션을 ls-al(Unix 계열 시스템) 또는 파일 속성(Windows 계열)을 통해 확인

```
LSNRCTL> status ListenerName
```

LISTENER.ORA 파일 확인

```
ADMIN_RESTRICTIONS_ListenerName=ON
```

Step 2) listener.ora 파일에 ADMIN_RESTRICTIONS_LISTENER=ON 라인 추가

listener를 재실행하거나 lsnrctl reload 명령어를 실행하여 listener를 재로딩함

```
#vi /Oracle_HomeDirectory/network/admin/listener.ora
```

ADMIN_RESTRICTIONS_LISTENER=ON 추가

※ ListenerName은 DBA가 제공한 리스너 이름

```
#cd /Oracle_Homedirectory/bin/에서
#LSNRCTL> reload
```

조치 시 영향	일반적으로 영향 없음

D-19 (중)	3. 옵션관리 > 3.3 패스워드 확인함수의 설정 및 적용
취약점 개요	
점검내용	■ 패스워드 복잡도를 확인하는 PASSWORD_VERIFY_FUNCTION 값이 설정되어 있는지 점검
점검목적	■ PASSWORD_VERIFY_FUNCTION 값을 설정하여 기본적인 패스워드 정책을 적용하고 이를 통해 로그인에 대한 보안성을 강화하여 저장중인 데이터의 안전성을 높이고자 함
보안위협	■ PASSWORD_VERIFY_FUNCTION 값이 설정되어 있지 않을 경우, 비인가자가 각종 공격(무작위 대입 공격, 사전 대입 공격 등)을 통해 취약한 패스워드가 설정된 사용자 계정의 패스워드를 획득하여 획득한 사용자 계정 권한을 통해 저장되어 있는 데이터의 유출, 수정, 삭제 등의 위험이 발생할 수 있음
참고	※ **PASSWORD_VERIFY_FUNCTION 값:** 이 프로파일에 명시된 사용자가 데이터베이스에 로그인 할 때 패스워드 확인을 위해 PL/SQL 함수가 사용되도록 명시하는 프로파일
점검대상 및 판단기준	
대상	■ Oracle, ALTIBASE, TIBERO 등
판단기준	**양호 :** 패스워드 검증 함수로 검증이 진행되는 경우
	취약 : 패스워드 검증 함수가 설정되지 않은 경우
조치방법	패스워드 검증 함수(PASSWORD_VERIFY_FUNCTION) 사용 설정
점검 및 조치 사례	

■ **Oracle**

Step 1) 설정 확인(SQL*Plus)

```
SQL> 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');
```

(반환 레코드가 존재하는 경우 취약)

Step 2) 패스워드 복잡도를 강제하는 패스워드 검증 함수를 생성, 사용하여야 함

<패스워드 확인 함수 적용 예시>

```
SQL> Alter profile default limit;
SQL> Password_verify_function verify_password_dod;
```

DBMS

D-19 (중)	3. 옵션관리 > 3.3 패스워드 확인함수의 설정 및 적용

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 잠김 날짜 기간
PASSWORD_GRACE_TIME	password가 만료된 후 password_life_time이 경과되어 비밀번호를 변경해야 할 경우, password를 변경할 수 있는 기간을 날수로 지정

■ **Altibase**

Step 1) 다음 명령어를 통해 PASSWORD_VERIFY_FUNCTION COLUMN 값을 확인 (값이 없을 경우 패스워드 유효성 검사 함수가 설정되어 있지 않음)

```
select * from system_.sys_users_;
```

Step 2) PASSWORD_VERIFY_FUNCTION 프로퍼티 설정

`ALTER USER` 유저명 `LIMIT (`프러퍼티 숫자`);`

적용 예) `ALTER USER TESTUSER LIMIT (PASSWORD_VERITY_FUNCTION default);`

```
1  select * from system_.sys_users_;
2  alter user testuser limit (password_verify_function defalut);
3
```

[패스워드 유효성 검사 함수 적용 확인]

	USER_ID	USER_NAME	PASSWORD_VERIFY_FUNCTION
1	0	PUBLIC	
2	1	SYSTEM_	
3	2	SYS	
4	105	TESTUSER	DEFALUT

[패스워드 유효성 검사 기본 함수로 설정됨을 확인]

■ **Tibero**

Step 1) 사용자별 패스워드 프로파일 적용 여부 확인

```
select * from dba_users;
```

Step 2) 설정되어 있을 경우 프로파일 설정 내용 확인

```
select * from dba_profiles;
```

D-19 (중)	3. 옵션관리 > 3.3 패스워드 확인함수의 설정 및 적용
Step 3) 설정되어 있지 않을 경우 프로파일 생성 시(또는 수정 시 alter profile) 패스워드 정책 설정 ※ 정책 적용 시 다음 명령어를 사용] CREATE PROFILE prof LIMIT 적용 예) CREATE PROFILE prof LIMIT failed_login_attempts 3 password_lock_time 1/1440 password_life_time 90 password_reuse_time unlimited password_reuse_max 10 password_grace_time 10 password_verify_function verify_function;	
조치 시 영향	일반적인 경우 영향 없음

DBMS

D-20 (하)	3. 옵션관리 > 3.4 인가되지 않은 Object Owner 의 제한
취약점 개요	
점검내용	■ Object Owner가 인가된 계정에게만 존재하는지 점검
점검목적	■ Object Owner가 비인가자에게 존재하고 있을 경우 이를 제거하기 위함
보안위협	■ 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
참고	※ **Object(객체):** ALTER, DELETE, EXECUTE, INDEX, INSERT, SELECT 등을 말함
점검대상 및 판단기준	
대상	■ Oracle, ALTIBASE, TIBERO 등
판단기준	**양호 :** Object Owner가 SYS, SYSTEM, 관리자 계정 등으로 제한된 경우
	취약 : Object Owner가 일반 사용자에게도 존재하는 경우
조치방법	Object Owner를 SYS, SYSTEM, 관리자 계정으로 제한 설정
점검 및 조치 사례	

■ **Oracle**

Step 1) 설정 확인(SQL*Plus)

```
SQL> 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');
```

Step 2) 권한 취소(SQL*Plus)

```
SQL> REVOKE 권한 on 객체 FROM User;
```

■ **Altibase**

Step 1) 사용자에게 부여된 객체 권한 정보를 확인

```
select * from system_.sys_grant_object_;
selcet * from system_.sys_privileges_;
```

D-20 (하)	3. 옵션관리 > 3.4 인가되지 않은 Object Owner 의 제한

Step 2) 부여된 권한 ID 를 확인하여 불필요 권한은 회수

`revoke` 권한 `on` 객체 `from` 유저

ALTIBASE HDB 는 다음과 같은 객체 접근 권한을 지원한다.

Priv ID	Object privileges	Table	Sequence	PSM/ External Procedure	View	directory	External Library
101	ALTER	O	O				
102	DELETE	O					
103	EXECUTE			O			O
104	INDEX	O					
105	INSERT	O					
106	REFERENCES	O					
107	SELECT	O	O		O		
108	UPDATE	O					
109	READ					O	
110	WRITE					O	

모든 사용자는 자동으로 메타 테이블에 대한 SELECT 권한을 가진다.

■ **Tibero**

Step 1) 데이터베이스 내 모든 스키마 객체 특권의 정보를 조회하여 인가받지 않은 객체 권한 소유자가 있는지 확인

```
select * from dba_tbl_privs;
```

Step 2) 잘못된 객체 권한 소유자 발견 시 해제

조치 시 영향	일반적인 경우 영향 없음

DBMS

D-21 (중)	3. 옵션관리 > 3.5 grant option 이 role 에 의해 부여되도록 설정
취약점 개요	
점검내용	■ 일반사용자에게 Grant Option이 Role 에 의해 부여되어 있는지 점검
점검목적	■ 일반사용자에게 Grant Option이 Role 에 의한 부여가 아닐 경우 권한을 취소함
보안위협	■ 일반 사용자에게 GRANT OPTION이 설정되어있는 경우, 일반 사용자가 객체소유자인 것과 같이 다른 일반 사용자에게 권한을 부여할 수 있어 WITH_GRANT_OPTION은 role에 의하여 설정되어야 함
참고	-
점검대상 및 판단기준	
대상	■ Oracle, MSSLQ, MySQL, ALTIBASE, TIBERO 등
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
점검 및 조치 사례	

■ **Oracle, Tibero**

Step 1) 설정 확인(SQL*Plus)

```
SQL> 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; (계정이 나오는 경우 취약)
```

Step 2) 권한 취소, 재부여(SQL*Plus)

```
SQL> REVOKE Role FROM User;
```

■ **MSSQL**

■ **MySQL**

D-21 (중)	3. 옵션관리 > 3.5 grant option 이 role 에 의해 부여되도록 설정

■ **Altibase**

Step 1) 사용자 계정을 조회하여 일반사용자에게 with grant option 이 부여되어 있을 경우 취약 (with grant option 1 일 경우)

```
select * from system_.sys_users_;
select * from system_.sys_grant_object_;
select * from system_.sys_privileges_;
```

	USER_ID	USER_NAME
1	0	PUBLIC
2	1	SYSTEM_
3	2	SYS
4	105	TESTUSER

[사용자 조회]

	GRANTOR_ID	GRANTEE_ID	PRIV_ID	USER_ID	OBJ_ID	OBJ_TYPE	WITH_GRANT_OPTION
1	2	105	102	2	105	T	0
2	2	105	107	2	105	T	0
3	2	105	105	2	105	T	1

[일반 사용자에 with grant option 설정 여부 확인]

Step 2) 권한 회수

`revoke` 권한 `on` 객체 `from` 유저

조치 시 영향	일반적인 경우 영향 없음

DBMS

D-22 (하)	3. 옵션관리 > 3.6 데이터베이스의 자원 제한 기능을 TRUE 로 설정
취약점 개요	
점검내용	■ RESOURCE_LIMIT 값이 TRUE로 설정되어 있는지 점검
점검목적	■ RESOURCE_LIMIT 값을 TRUE로 설정하도록 함
보안위협	■ 자원 제한 기능을 TRUE로 설정하지 않을 경우, 특정 사용자가 과도하게 많은 자원을 소비할 수 있으며 이로 인해 시스템에 과부하가 발생할 수 있음
참고	-
점검대상 및 판단기준	
대상	■ Oracle
판단기준	**양호 :** RESOURCE_LIMIT 설정이 TRUE로 되어있는 경우
	취약 : RESOURCE_LIMIT 설정이 FALSE로 되어있는 경우
조치방법	RESOURCE_LIMIT 설정을 TRUE로 설정 변경
점검 및 조치 사례	

■ **Oracle**

Step 1) init.ora 설정 파일에 RESOURCE_LIMIT = TRUE' 라인 추가

```
#vi /Oracle_HomeDirectory/admin/pfile/init.ora
```

Step 2) SQL*Plus에서

```
SQL> Alter System Set Resource_Limit=TRUE;
```

조치 시 영향	일반적인 경우 영향 없음

D-23 (중)	4. 패치관리 > 4.3 보안에 취약하지 않은 버전의 데이터베이스를 사용
취약점 개요	
점검내용	■ 안전한 버전의 데이터베이스를 사용하고 있는지 점검
점검목적	■ 안전한 버전의 데이터베이스를 사용하여 알려진 보안 취약점으로 인한 공격을 차단하기 위함
보안위협	■ 안전하지 않는 버전을 사용할 경우, 공격자가 시스템 권한 획득 등을할 수 있는 취약점이 존재함.
참고	-
점검대상 및 판단기준	
대상	■ Oracle, ALTIBASE, TIBERO 등
판단기준	**양호:** 보안 패치가 적용된 버전을 사용하는 경우
	취약: 보안 패치가 적용되지 않는 버전을 사용하는 경우
조치방법	보안패치가 적용된 버전으로 업데이트
점검 및 조치 사례	

■ **Oracle**

Step 1) Oracle 최신 버전 확인

http://www.oracle.com/technetwork/database/enterprise-edition/overview/index.html

Step 2) 버전 확인(SQL*Plus)

```
SQL> select * banner from v$version where banner like 'Oracle%';
```

■ **Altibase**

Step 1) 시스템에서 제품 버전 현황 확인

```
select * from v$database;
```

Step 2) Altibase 최신 패치 노트 확인

http://support.Altibase.com/kr/patch-note

STEP 3) 패키지 인스톨러를 이용한 제품 패치

Altibase HDB 는 제품 패치를 위한 설치 파일이 따로 존재하지 않음. 인스톨러를 시작할 때 설치 형태를 풀(full) 패키지 또는 패치로 선택할 수 있음

Altibase 고객지원서비스 포털 (http://support.Altibase.com/)을 방문하여 본인의 운영 체제에 적합한 인스톨러를 다운로드 받을 수 있음

DBMS

D-23 (중)	4. 패치관리 > 4.3 보안에 취약하지 않은 버전의 데이터베이스를 사용
■ **Tibero** Step 1) 시스템에서 제품 버전 현황 확인 `tbboot –v` Step 2) Tibero 최신 패치 노트 확인 http://technet.tmaxsoft.com/ ※ Tibero 패치 정책 (2015.02) 매 분기 초 픽스셋 발표(년간 총 4회 배포 / fixset: hot fix 모음)	
조치 시 영향	일반적으로 영향 없음

DBMS

D-24 (하)	5. 로그관리 > 5.1 Audit Table은 데이터베이스 관리자 계정으로만 접근하도록 제한
취약점 개요	
점검내용	■ Audit Table 접근 권한이 관리자 계정으로 제한되고 있는지 점검
점검목적	■ Audit Table 접근 권한을 관리자 계정으로 제한하고자 함
보안위협	■ Audit Table 이 데이터베이스 관리자 계정에 속하지 않을 경우, 비인가자가 감사 데이터의 수정, 삭제 등의 수행이 가능함
참고	-
점검대상 및 판단기준	
대상	■ Oracle, ALTIBASE, TIBERO 등
판단기준	**양호:** Audit Table 접근 권한이 관리자 계정으로 설정한 경우
	취약: Audit Table 접근 권한이 일반 계정으로 설정한 경우
조치방법	Audit Table 접근 권한을 관리자 계정으로 제한
점검 및 조치 사례	

■ Oralce, Tibero

Step 1) 설정 확인(SQL*Plus)

```
SQL> Select owner from dba_tables where table_name='AUD$';
```

SYS 또는 SYSTEM이 아닌 계정이 나올 경우 확인 후 권한 삭제

Step 2) Audit table에 접근할 권한이 없는 계정이 확인 될 경우 권한 삭제

■ Altibase

Step 1) 사용자 계정을 조회하여 SYSTEM_, SYS 의 USER_ID 를 확인

```
select * from system_.sys_users_;
```

Step 2) 시스템 테이블 조회 내용 중 AUDIT 관련 테이블 정보의 TABLE_ID 확인
(Step 1) 의 USER_ID 와 동일한)

```
select * from system_.sys_tables_;
```

STEP 3) AUDIT 테이블에 권한 없는 계정이 부여되어 있을 경우 권한 삭제

■ Tibero

감사 기록은 $TB_SID.tip 파일에 설정된 AUDIT_TRAIL 파라미터에 따라 데이터베이스 내부 또는 OS 파일에 저장할 수 있음. OS 파일에 감사 기록을 저장하는 경우 파일의 위치와 최대 크기를 각각 $TB_SID.tip파일의 AUDIT_FILE_DEST 파라미터와 AUDIT_FILE_SIZE 파라미터로 설정할 수 있음

DBMS

D-24 (하)	5. 로그관리 > 5.1 Audit Table은 데이터베이스 관리자 계정으로만 접근하도록 제한

조치방법 1. 데이터베이스 내부에 감사 기록 저장

Step 1) <$TB_SID.tip> 파일에 아래 내용 입력

```
AUDIT_TRAIL=DB_EXTENDED
```

감사 기록에 포함되는 기본 정보 및 사용자가 실행한 SQL 문장까지 저장

※ 다음 정적 뷰를 통해 감사 기록 조회가 가능

```
DBA_AUDIT_TRAIL (select * from dba_audit_trail;)
USER_AUDIT_TRAIL (select * from user_audit_trail;)
```

조치방법 2. OS 파일에 감사 기록 저장

Step 1) <$TB_SID.tip> 파일에 아래 내용 입력

```
AUDIT_TRAIL=OS
AUDIT_FILE_DEST=/home/Tibero/audit/audit_trail.log
AUDIT_FILE_SIZE=10M
```

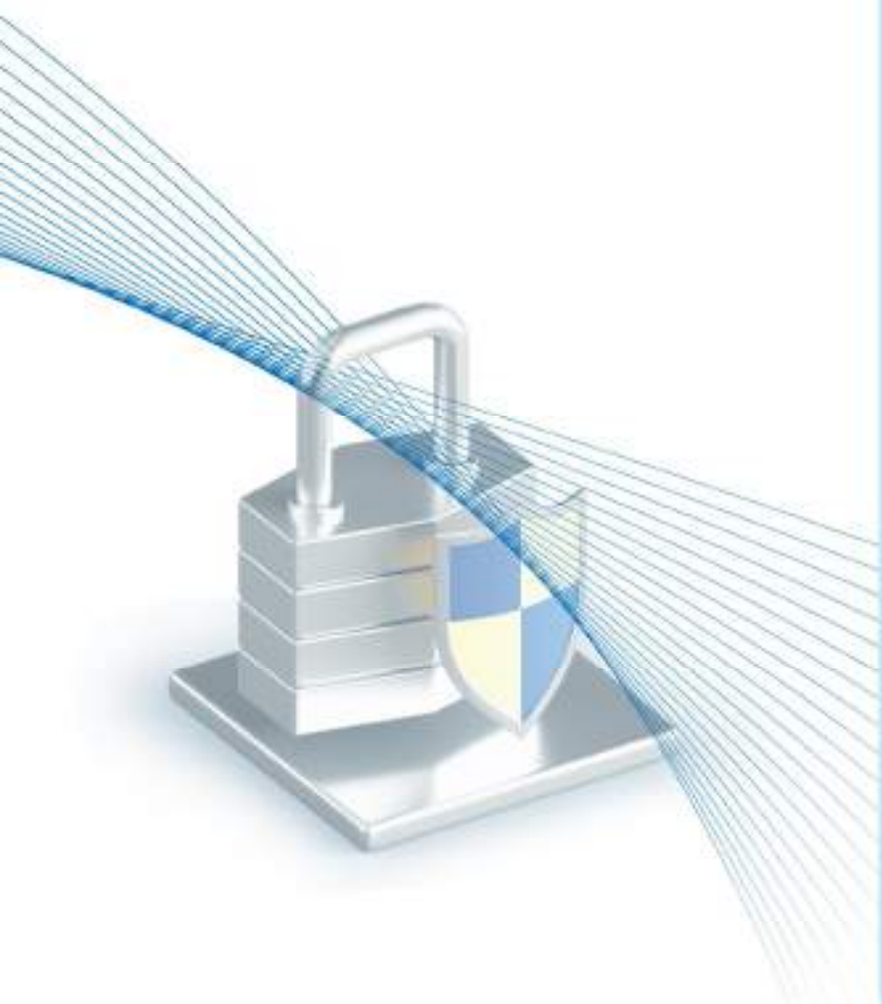
위와 같이 설정하면 "/home/Tibero/audit/audit_trail.log"에 최대 10MB의 크기로 감사 기록이 저장됨

※ 감사 파일이 있는 디렉터리에는 일반사용자는 접근할 수 없도록 설정

조치 시 영향	일반적으로 영향 없음

II

웹(WEB)



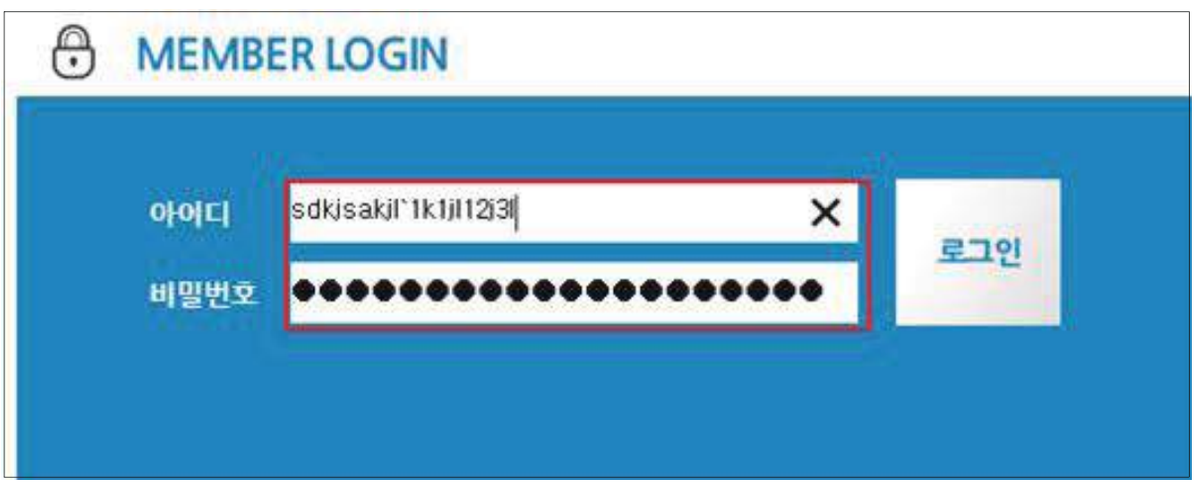
Web 취약점 분석·평가 항목

점검항목	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

BO (상)	1. 버퍼 오버플로우
취약점 개요	
점검내용	■ 파라미터 입력 값에 대한 적절성 점검 여부 진단
점검목적	■ 애플리케이션에서 파라미터 입력 값에 대한 적절성을 점검하여 비정상적 오류 발생을 차단하기 위함
보안위협	■ 애플리케이션 입력 값의 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 비 인가된 접근 및 사용 등이 발생할 수 있음
참고	※ 소스코드 및 취약점 점검 필요
점검대상 및 판단기준	
대상	■ 소스코드
판단기준	**양호 :** 파라미터 입력 값에 대량의 인수 값 전달 시 에러 페이지나 오류가 발생되지 않는 경우
	취약 : 파라미터 입력 값에 대한 검증이 이루어지지 않고 에러 페이지나 오류가 발생하는 경우
조치방법	외부 파라미터 입력 값을 할당하여 사용하는 경우 변수에 입력된 입력 값 범위를 검사하여 외부 파라미터 입력 값이 허용 범위를 벗어나는 경우 에러 페이지가 반환되지 않도록 조치
점검 및 조치 사례	

■ **점검방법**

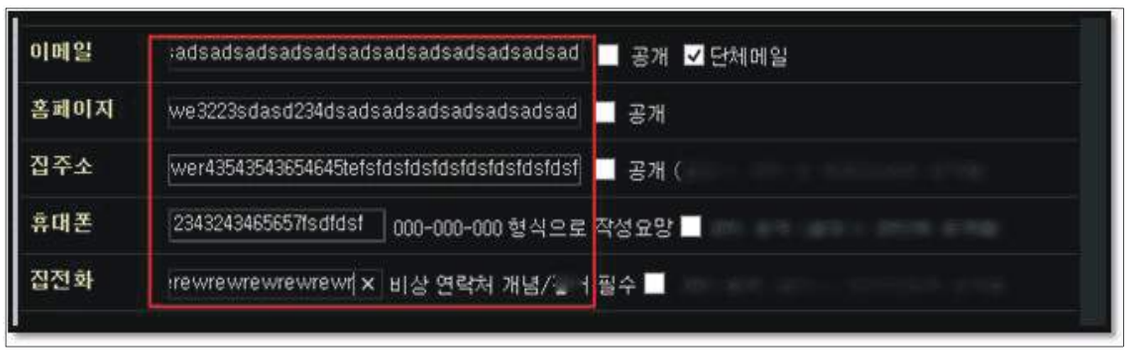
Step 1) 로그인 창에 많은 인수 값 전달 시 에러 페이지나 오류가 발생하는지 점검



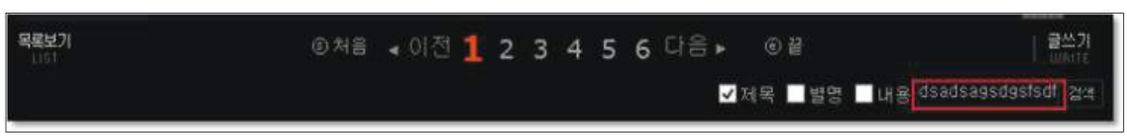
웹(Web)

BO (상)	1. 버퍼 오버플로우

Step 2) 회원정보 변경 창에 많은 인수 값 전달 시 에러 페이지나 오류가 발생하는지 점검



Step 3) 사이트 검색란에 많은 인수 값 전달 시 에러 페이지나 오류가 발생하는지 점검



Step 4) 게시물 작성 시 허용된 문자보다 많은 인수 값을 입력하여 에러 페이지나 오류가 발생하는지 점검

Step 5) 웹 애플리케이션에 많은 인수 값 전달 시 에러 페이지나 오류가 발생하는지 점검

■ 보안설정방법

Step 1) 웹 서버, WAS 서버 애플리케이션 버전을 안정성이 검증된 최신 버전으로 패치

Step 2) 웹 애플리케이션에 전달되는 인수 값을 필요한 크기만큼만 받을 수 있도록 변경하고 범위를 벗어난 인수 값이 전달될 경우 에러 페이지를 반환하지 않도록 설정

Step 3) 동적 메모리 할당을 위해 크기를 사용하는 경우 그 값이 음수가 아닌지 검사하여 버퍼 오버플로우를 예방하는 형태로 소스 코드 변경

Step 4) 버퍼 오버플로우를 점검하는 웹 스캐닝 툴을 이용하여 주기적으로 점검

조치 시 영향	일반적으로 영향 없음

FS (상)	2. 포맷스트링
취약점 개요	
점검내용	■ 웹페이지 내 포맷스트링 취약점 존재 여부 점검
점검목적	■ 포맷스트링 버그로 인한 위험으로부터 예방하기 위한 웹페이지 내 적절한 입력값 검증 로직을 탑재하기 위함
보안위협	■ C언어로 만드는 프로그램 중 변수의 값을 출력하거나 입력받을 때 입력받은 값을 조작하여 프로그램의 메모리 위치를 반환받아 메모리 주소를 변조하여 시스템의 관리자 권한을 획득할 수 있음
참고	※ **포맷 스트링 버그(format string bug):** printf 등의 함수에서 문자열 입력 포맷을 잘못된 형태로 입력하는 경우 나타나는 취약점으로 루트 권한을 획득하는 것도 가능함. 포맷 스트링의 종류에는 여러 가지가 있으며 그 중 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 ... %d : 정수형 10진수 상수 %f : 실수형 상수 %lf : 실수형 상수 %c : 문자값 %s : 문자 스트링 %u : 양의 정수(10진수) %o : 양의 정수(8진수) %x : 양의 정수(16진수) %n : 쓰인 총 바이트 수 ※ %n 은 이전까지 입력되었던 문자열의 길이(Byte)수 만큼 해당 변수에 저장시키기 때문에 메모리의 내용도 변조 가능하므로 Format String 취약점에서 핵심이기도 함. 문자열의 길이를 변조 시키고 싶은 값의 길이만큼 만든 후 %n을 써주게 되면 메모리상에 공격자가 원하는 값을 넣을 수 있게 됨 ※ 소스코드 및 취약점 점검 필요
점검대상 및 판단기준	
대상	■ Web Server, 소스코드
판단기준	**양호 :** 임의의 문자열 입력에 대한 검증이 이루어지는 경우
	취약 : 임의의 문자열 입력에 대한 검증이 이루어지지 않으며, 오류가 발생하는 경우
조치방법	웹 서버 응용프로그램(Apache, Tomcat, IIS 등) 을 최신 버전으로 패치하고 임의의 문자열 입력에 대한 검증 로직 구현

웹(Web)

FS (상)	2. 포맷스트링

점검 및 조치 사례

■ 점검방법

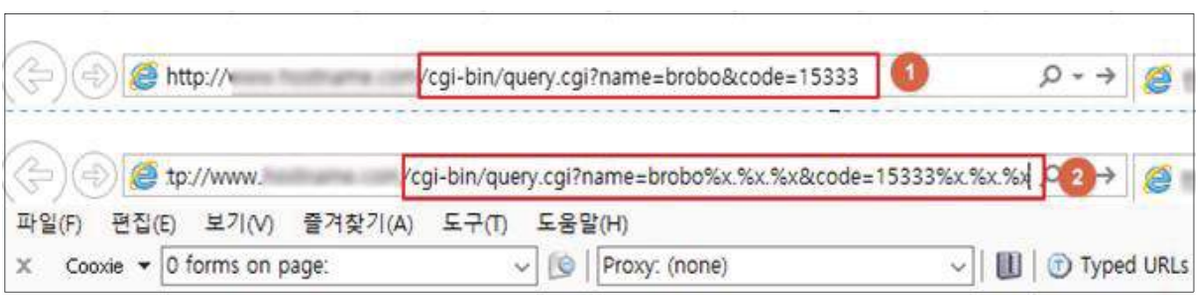
Step 1) 웹 사이트 인수 값에 아래와 같은 패턴 입력 후 전송하여 반환된 페이지가 다른 인수 값을 입력했을 때는 발생하지 않는 에러 반응이나 멈추는 등 이상반응을 보이는지 확인

패턴1 - %n%n%n%n%n%n%n%n%n,

패턴2 - %s%s%s%s%s%s%s%s%s%s,

패턴3 - %1!n!%2!n!%3!n!%4!n!%5!n!%6!n!%7!n!%8!n!%9!n!%10!n!

패턴4 - %1!s!%2!s!%3!s!%4!s!%5!s!%6!s!%7!s!%8!s!%9!s!%10!s!



■ 보안설정방법

Step 1) 컴파일러에서는 문자열 입력 포맷에 대한 자체적인 검사를 내장하고 있으므로 문자열 입력 포맷 검증 후 소스 코드에 적용

(예) GCC에서는 문자열 입력 포맷과 실제 입력이 맞지 않는 경우에 대해 경고 옵션 존재 하지만, 이 방식은 컴파일 시간에 문제를 발견할 수 있는 경우에 한해 검증 가능함
런타임 상황에서는 퍼지 테스트를 이용하여 프로그램의 입력 값으로 임의의 값을 넣어서 프로그램을 예외 상황으로 빠뜨리는 경우가 있으므로 이러한 경우에 버그가 없는지 확인이 필요함

Step 2) 웹 서버 응용프로그램(Apache, Tomcat, IIS 등)의 최신 보안패치 적용

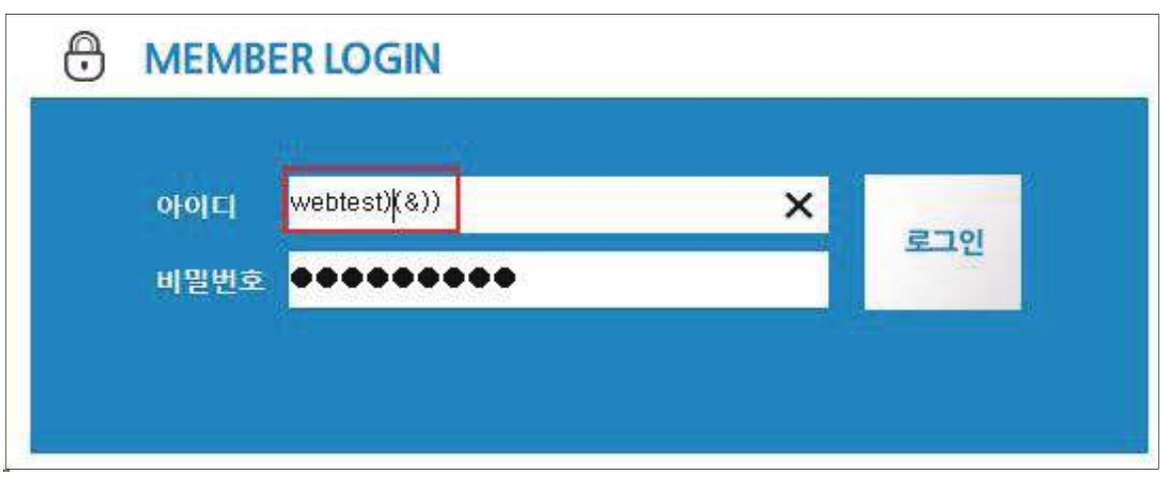
Step 3) 웹사이트 인수 값 처리 중에 발생할 경우 사용자가 입력하는 인수 값의 유효성에 대한 검증 로직을 구현

조치 시 영향	일반적으로 영향 없음

LI (상)	3. LDAP 인젝션
취약점 개요	
점검내용	■ 웹페이지 내 LDAP 인젝션 취약점 점검
점검목적	■ 취약한 시스템에 신뢰할 수 없는 LDAP 코드 삽입 공격을 통한 비인가자의 악의적인 행위를 차단하기 위함
보안위협	■ 응용 프로그램이 사용자 입력 값에 대한 적절한 필터링 및 유효성 검증을 하지 않아 공격자는 로컬 프록시를 사용함으로 LDAP 문의 변조가 가능함 ■ 공격 성공 시 승인되지 않은 쿼리에 권한을 부여하고, LDAP 트리 내의 내용 수정이나 임의의 명령 실행을 가능하게 하므로 적절한 필터링 로직을 구현하여야 함
참고	※ **LDAP 인젝션:** 사용자 입력을 기반으로 LDAP(Lightweight Directory Access Protocol)구문을 구축하여 웹 기반 응용 프로그램을 악용하는 데 사용되는 공격 ※ 소스코드 및 취약점 점검 필요
점검대상 및 판단기준	
대상	■ 소스코드, 웹 방화벽
판단기준	**양호 :** 임의의 LDAP 쿼리 입력에 대한 검증이 이루어져 변조된 쿼리가 실행되지 않는 경우
	취약 : 임의의 LDAP 쿼리 입력에 대한 검증이 이루어지지 않아 변조된 쿼리가 실행되는 경우
조치방법	지정된 문자열만 입력 허용하고, 임의의 LDAP 쿼리 입력에 대한 검증 로직 구현
점검 및 조치 사례	

■ 점검방법

Step 1) 웹사이트의 사용자 인수 값을 입력받는 애플리케이션(폼필드, URL 등)에 변조된 LDAP 쿼리 전송 후 실행되는지 확인



웹(Web)

LI (상)	3. LDAP 인젝션

■ 보안설정방법

Step 1) 사용자 입력 값을 White List로 지정하여 영문(a-z, A-Z)과 숫자(0-9)만을 허용

Step 2) DN과 필터에 사용되는 사용자 입력 값에는 특수문자가 포함되지 않도록 특수문자 제거

Step 3) 특수문자를 사용해야 하는 경우 특수문자(DN에 사용되는 특수문자는 '₩', 필터에 사용되는 특수문자는 =, +, <, >, #, ;, ₩ 등)에 대해서는 실행 명령이 아닌 일반문자로 인식되도록 처리

※ 필터링 대상

'	"	--	#	(	)
=	*/	/*	+	<	>
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_	sysobject	%
*	;	&	|		

Step 4) 웹 방화벽에 LDAP 관련 특수문자를 필터링하도록 룰셋 적용

조치 시 영향	일반적으로 영향 없음

OC (상)	4. 운영체제 명령 실행
취약점 개요	
점검내용	■ 웹사이트 내 운영체제 명령 실행 취약점 존재 여부 점검
점검목적	■ 적절한 검증절차를 거치지 않은 사용자 입력 값에 의해 의도하지 않은 시스템 명령어가 실행되는 것을 방지하기 위함
보안위협	■ 해당 취약점이 존재하는 경우 부적절하게 권한이 변경되거나 시스템 동작 및 운영에 악영향을 줄 가능성이 있으므로 "|", "&", ";", "`" 문자에 대한 필터링 구현이 필요함
참고	※ 소스코드 및 취약점 점검 필요
점검대상 및 판단기준	
대상	■ 소스코드, 웹 방화벽
판단기준	**양호 :** 임의의 명령어 입력에 대한 검증이 이루어지는 경우
	취약 : 임의의 명령어 입력에 대해 명령이 실행되는 경우
조치방법	애플리케이션은 운영체제로부터 명령어를 직접적으로 호출하지 않도록 구현하는 게 좋지만, 부득이하게 사용해야 할 경우 소스 코드나 웹 방화벽에서 특수문자, 특수 구문에 대한 검증을 할 수 있도록 조치해야 함

점검 및 조치 사례

■ 점검방법

Step 1) 웹 애플리케이션 인수값에 시스템 명령어 전달 시 명령이 실행되는지 확인

■ 보안설정방법

Step 1) 웹 방화벽에 모든 사용자 입력 값을 대상으로 악용될 수 있는 특수문자, 특수 구문 등을 필터링 할 수 있도록 규칙 적용

Step 2) 애플리케이션은 운영체제로부터 명령어를 직접적으로 호출하지 않도록 구현

Step 3) 명령어를 직접 호출하는 것이 필요한 경우에는, 데이터가 OS 의 명령어 해석기에 전달되기 전에 입력 값을 검증/확인 하도록 구현

Step 4) 입력 값에 대한 파라미터 데이터의 "&", "|", ";", "`" 문자에 대한 필터링 처리

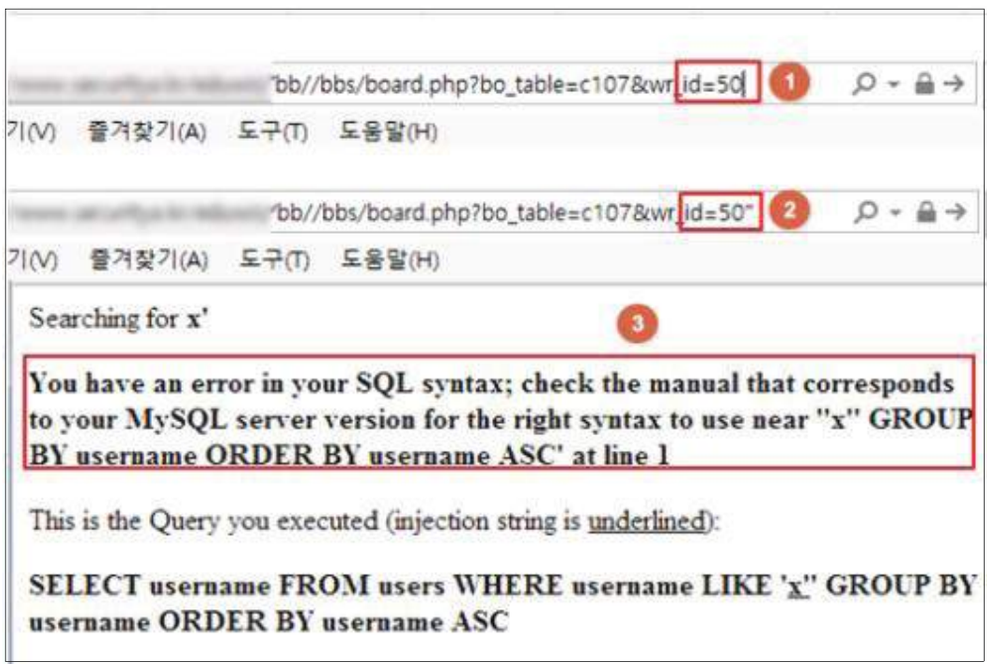
웹(Web)

OC (상)	4. 운영체제 명령 실행
※ 참고: “&”, “|”, “`” 문자 설명 • **&** : 윈도우 명령어 해석기에서 첫 번째 명령이 성공했을 경우만 두 번째 명령어를 실행 • **|** : 첫 번째 명령어가 성공하는지에 상관없이 두 번째 명령어를 실행 • ` : 쉘 해석기가 명령어를 해석하다 역 작은따옴표(`) 내에 포함된 명령어를 만나면 기존 명령어를 계속 실행하기 전에 역 작은따옴표로 둘러싸인 명령어를 먼저 실행 (예) `ls -al`	
조치 시 영향	일반적으로 영향 없음

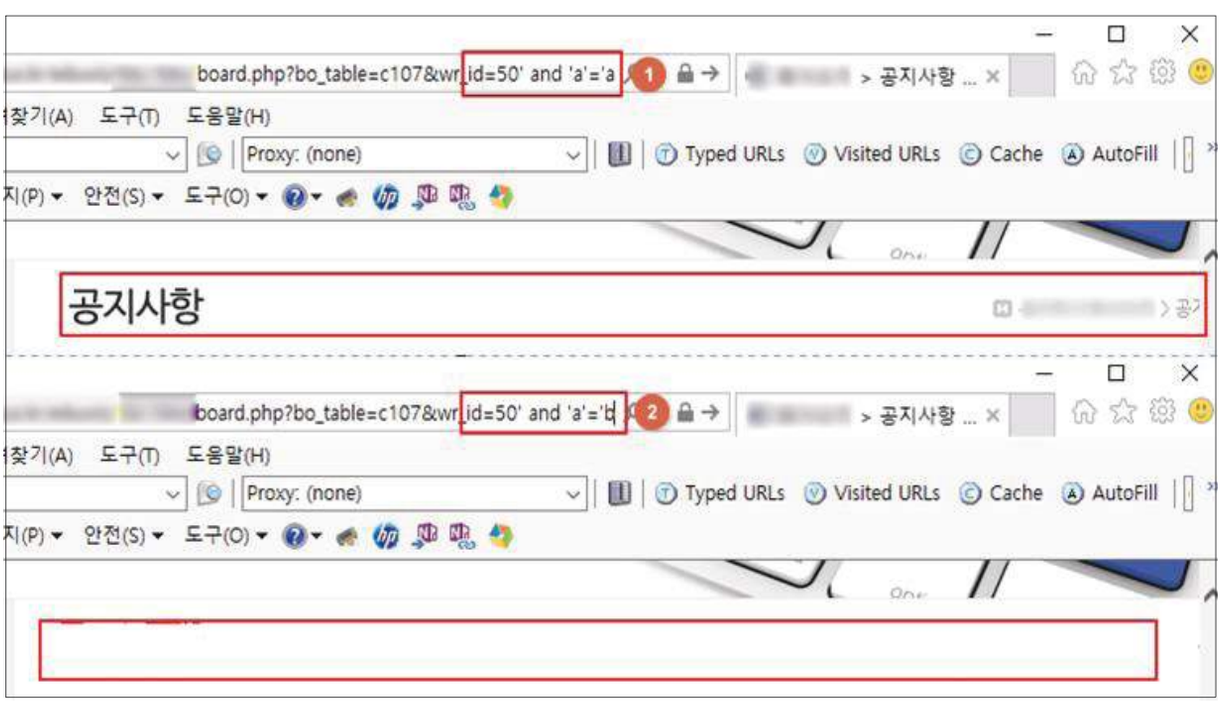
SI (상)	5. SQL 인젝션
취약점 개요	
점검내용	■ 웹페이지 내 SQL 인젝션 취약점 존재 여부 점검
점검목적	■ 대화형 웹 사이트에 비정상적인 사용자 입력 값 허용을 차단하여 악의적인 데이터베이스 접근 및 조작을 방지하기 위함
보안위협	■ 해당 취약점이 존재하는 경우 비정상적인 SQL 쿼리로 DBMS 및 데이터(Data)를 열람하거나 조작 가능하므로 사용자의 입력 값에 대한 필터링을 구현하여야 함
참고	※ **SQL인젝션:** 사용자의 입력 값으로 웹 사이트 SQL 쿼리가 완성되는 약점을 이용하며, 입력 값을 변조하여 비정상적인 SQL 쿼리를 조합하거나 실행하는 공격. 개발자가 생각지 못한 SQL문을 실행되게 함으로써 데이터베이스를 비정상적으로 조작 가능함 ※ SQL인젝션 공격 관련 코드 검토 필요 ※ 소스코드 및 취약점 점검 필요
점검대상 및 판단기준	
대상	■ 소스코드, 웹 방화벽
판단기준	**양호 :** 임의의 SQL Query 입력에 대한 검증이 이루어지는 경우
	취약 : 임의의 SQL Query 입력에 대한 검증이 이루어지지 않는 경우
조치방법	소스 코드에 SQL Query 입력값을 받는 함수나 코드를 써야 할 경우, 임의의 SQL Query 입력에 대한 검증 로직을 구현하여 검증되지 않는 SQL Query가 인수값으로 들어올 경우 에러 페이지가 아닌 정상 페이지가 반환되도록 필터링 처리하고 웹 방화벽을 운용할 경우 웹 방화벽에 SQL 인젝션 관련 룰셋을 적용하여 SQL 인젝션 공격 차단함
점검 및 조치 사례	
■ 점검방법 Step 1) 애플리케이션 인수 값에 특수문자나 임의의 SQL 쿼리를 전달하여 DB 에러 페이지가 반환되는지 확인	

웹(Web)

SI (상)	5. SQL 인젝션

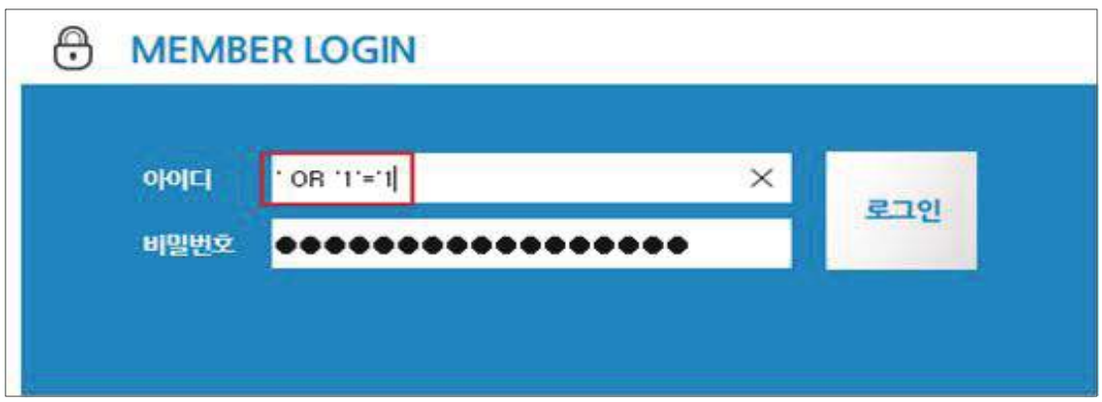


Step 2) 애플리케이션 인수 값에 임의의 SQL 참, 거짓 쿼리를 전달하여 참, 거짓 쿼리에 따라 반환되는 페이지가 다른지 확인



SI (상)	5. SQL 인젝션

Step 3) 로그인 창에 참이 되는 SQL 쿼리를 전달하여 로그인 되는 확인



■ 보안설정방법

Step 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)

문자	설명
'	문자 데이터 구분기호
;	쿼리 구분 기호
--, #	해당라인 주석 구분 기호
/* */	* 와 */ 사이 구문 주석

Step 2) Dynamic SQL 구문 사용 금지

Dynamic SQL 구문 사용을 지양하며 파라미터에 문자열 검사 필수적용

Step 3) 오류에 대한 예외처리

에러 메시지는 공격자에게 많은 정보를 제공하므로 오류처리로 정보 노출을 최소화

시스템에서 제공하는 에러 메시지 및 DBMS에서 제공하는 에러 코드가 노출되지 않도록 예외처리

Step 4) 웹 방화벽에 인젝션 공격 관련 차단 룰셋 적용

Step 5) 필터링 등 입력값 검증 프로세스는 Client side script가 아닌, Server 페이지로 구현

※ 애플리케이션 별 설정 방법

■ ASP

Step 1) 문자열 유효성 검증 로직 구현

(예) 특정 문자열 필터링 적용 (※ 예로 제시한 것으로, 구현 시 다를 수 있음)

웹(Web)

SI (상)	5. SQL 인젝션

```
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

Step 1) 문자열 유효성 검증 로직 구현

(예) 특정 문자열 필터링 적용 (※ 예로 제시한 것으로, 구현 시 다를 수 있음)

request로 입력 값을 가져올 경우 입력 값에서 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("\","");
Str = str. Replace("/","");
.....
return str;
}
```

SI (상)	5. SQL 인젝션

Step 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.";
}
}
}
```

■ JSP

Step 1) 문자열 유효성 검증 로직 구현

(예) 특정 문자열 필터링 적용 (※ 예로 제시한 것으로, 구현 시 다를 수 있음)

request로 입력 값을 가져올 경우 입력 값에서 특수문자를 제거하여 바인딩 하는 소스 삽입

replaceAll() 메소드를 사용하여 구현

웹(Web)

SI (상)	5. SQL 인젝션

```
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, "\", ""));
    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;
    }
```

Step 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 qury = "SELECT * FROM ? WHERE Name = ?";
  stmt = con.perpareStatement(query);
  stmt.setString(1, tableName);
  stmt.setString(2, name);
  rs = stmt.executeQuery();
  .....
}
catch (SQLException sqle){ }
finally { }
```

SI (상)	5. SQL 인젝션

(예2) JDO API 사용 시 외부 입력 값이 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)

SI (상)	5. SQL 인젝션

(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

Step 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|\"|\'|#|\/\*|\*\/|\\\|\;)","",
$get_Str);
}
```

SI (상)	5. SQL 인젝션

(예3) php.ini 설정 중 magic_quotes_gps 옵션을 이용하여 특정 문자열 필터링 적용

GPC(Get, Post, Cookie)를 통해 넘어오는 문자열 중 ', ", ₩, NULL 값의 앞에 자동으로 백슬래쉬 문자를 붙여주는 기능을 함 (PHP 6.0 이후 버전 사용 불능)

```
magic_quotes_gpc = on
```

STEP 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>
```

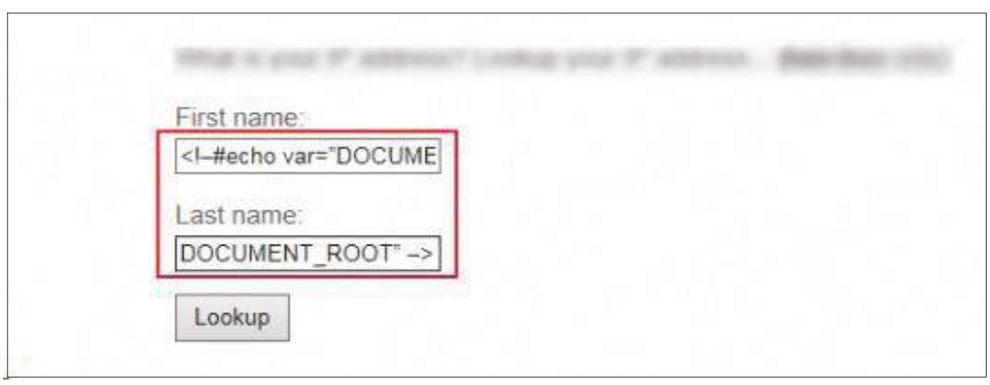
조치 시 영향	일반적으로 영향 없음

웹(Web)

SS (상)	6. SSI 인젝션
취약점 개요	
점검내용	■ 웹페이지 내 SSI 인젝션 공격 가능성 점검
점검목적	■ 적절한 입력값 검증 절차를 마련하여 악의적인 파일을 include 시키지 못하도록 하여 불법적인 데이터 접근을 차단하기 위함
보안위협	■ 해당 취약점이 존재할 경우 웹서버 상에 있는 파일을 include 시켜 명령문이 실행되게 함으로 불법적으로 데이터에 접근할 수 있음 ■ 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 입력 값에 대한 검증 로직을 추가로 구현하여야 함
참고	※ **SSI(Server-Side Includes):** CGI 프로그램을 작성하거나 혹은 서버사이드 스크립트를 사용하는 언어로, 웹 서버가 사용자에게 페이지를 제공하기 전에 구문을 해석하도록 지시하는 역할을 함 ※ **SSI(Server-Side Includes) 인젝션:** HTML 문서 내 입력받은 변수 값을 서버 측에서 처리할 때 부적절한 명령문이 포함 및 실행되어 서버의 데이터가 유출되는 취약점 ※ 소스코드 및 취약점 점검 필요
점검대상 및 판단기준	
대상	■ 소스코드, Web Server, 웹 방화벽
판단기준	**양호 :** 사용자 입력 값에 대한 검증이 이루어지는 경우
	취약 : 사용자 입력 값에 대한 검증이 이루어지지 않는 경우
조치방법	사용자 입력 값에 대한 검증 로직 추가 구현
점검 및 조치 사례	

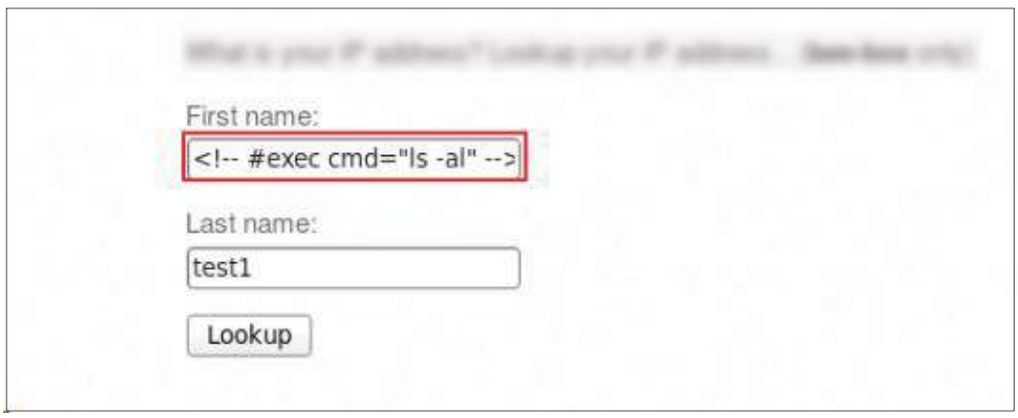
■ **점검방법**

Step 1) 인수 값에 <!--#echo var="DOCUMENT_ROOT" -->를 삽입하여 전송 후 반환되는 페이지에 사이트의 홈 디렉터리가 표시되는지 확인



SS (상)	6. SSI 인젝션

Step 2) 인수 값에 <!-- #exec cmd="ls -al" -->를 삽입하여 전송 후 반환되는 페이지에 디렉터리의 파일 리스트가 표시되는지 확인



■ 보안설정방법

Step 1) 사용자 입력으로 사용 가능한 문자들을 정해놓음

Step 2) 정해진 문자들을 제외한 나머지 모든 문자들을 필터링 함

Step 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	<	>	"	&#40	&#41	&#35	&amp

Step 4) 웹 서버의 SSI 기능을 사용하지 않거나, 웹 방화벽에 특수문자를 필터링하도록 룰셋 적용

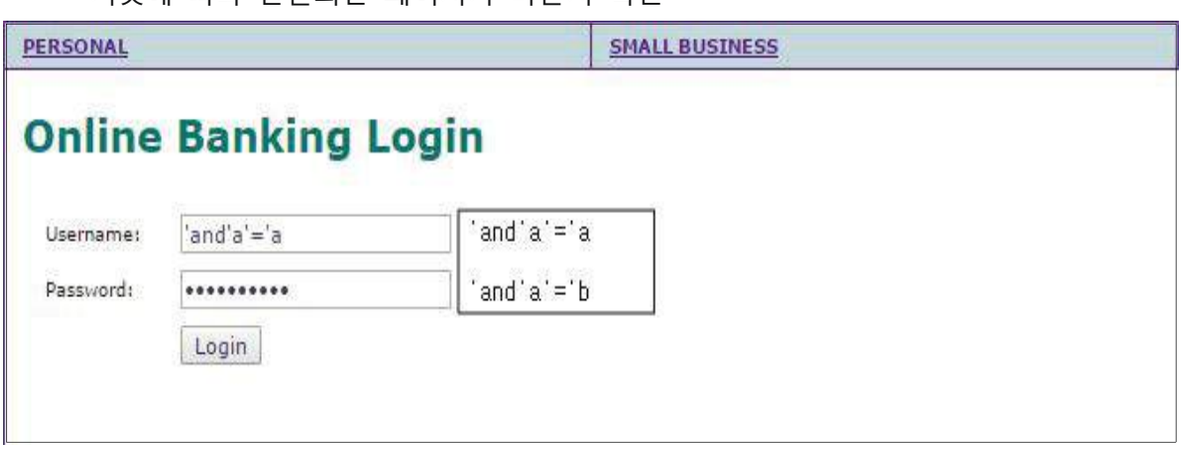
조치 시 영향	일반적으로 영향 없음

웹(Web)

XI (상)	7. XPath 인젝션
취약점 개요	
점검내용	■ 웹페이지 내 조작된 XPath 쿼리 공격 가능성 점검
점검목적	■ XPath 쿼리에 대한 적절한 필터링을 적용하여 웹사이트의 로직 손상 및 특정 데이터 추출을 차단하기 위함
보안위협	■ 해당 취약점이 존재할 경우 프로그래머가 의도하지 않았던 문자열을 전달하여 쿼리문의 의미를 왜곡시키거나 그 구조를 변경하고 임의의 쿼리를 실행하여 인가되지 않은 데이터를 열람할 수 있으므로 적절한 필터링 로직 구현이 필요함
참고	※ 소스코드 및 취약점 점검 필요
점검대상 및 판단기준	
대상	■ 소스코드, 웹 방화벽
판단기준	**양호 :** 쿼리 입력 값에 대해 검증이 이루어지는 경우
	취약 : 쿼리 입력 값에 대해 검증이 이루어지지 않는 경우
조치방법	쿼리 입력값에 대해 검증 로직 추가 구현
점검 및 조치 사례	

■ 점검방법

Step 1) ['and'a'='a, 'and'a'='b], [and 1=1, and 1=2]의 셋트의 값을 각각 삽입하여 쿼리의 참, 거짓에 따라 반환되는 페이지가 다른지 확인



Step 2) 다음 값을 입력해서 에러가 발생하지 않는지 확인

' or count(parent::*[position()=1])=0 or 'a'='b

' or count(parent::*[position()=1])>0 or 'a'='b

1 or count(parent::*[position()=1])=0

1 or count(parent::*[position()=1])>0

XI (상)	7. XPath 인젝션

■ 보안설정방법

XPath 쿼리에 입력 값이 입력되는 경우, 엄격한 입력 값 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

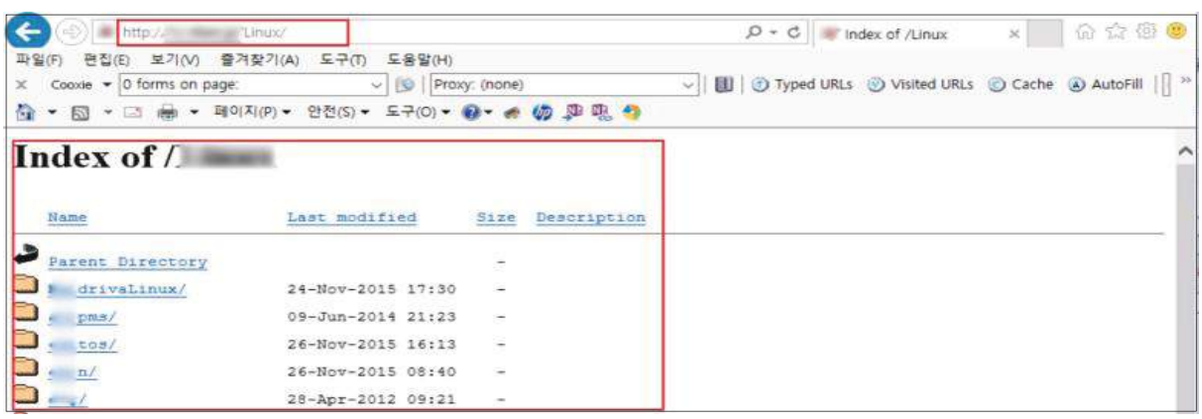
조치 시 영향	일반적으로 영향 없음

웹(Web)

DI (상)	8. 디렉터리 인덱싱
취약점 개요	
점검내용	■ 웹서버 내 디렉터리 인덱싱 취약점 존재 여부 점검
점검목적	■ 디렉터리 인덱싱 취약점을 제거하여 특정 디렉터리 내 불필요한 파일 정보의 노출을 차단
보안위협	■ 해당 취약점이 존재할 경우 브라우저를 통해 특정 디렉터리 내 파일 리스트를 노출하여 응용시스템의 구조를 외부에 허용할 수 있고, 민감한 정보가 포함된 설정 파일등이 노출될 경우 보안상 심각한 위험을 초래할 수 있음
참고	※ **디렉터리 인덱싱 취약점:** 특정 디렉터리에 초기 페이지 (index.html, home.html, default.asp 등)의 파일이 존재하지 않을 때 자동으로 디렉터리 리스트를 출력하는 취약점
점검대상 및 판단기준	
대상	■ Web Server
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
점검 및 조치 사례	

■ 점검방법

Step 1) URL 경로 중 확인 하고자 하는 디렉터리까지만 주소 창에 입력하여 인덱싱 여부를 확인



Step 2) 디렉터리 끝에 %3f.jsp 문자열을 붙여 디렉터리 인덱싱이 되는지 확인

DI (상)	8. 디렉터리 인덱싱

■ 보안설정방법

Step 1) 웹 서버 환경설정에서 디렉터리 인덱싱 기능 제거

※ 웹 서버 별 상세 설정

■ Apache

Httpd.conf 파일 내 DocumentRoot 항목의 Options에서 Indexes 제거
Indexes가 해당 디렉터리의 파일 목록을 보여주는 지시자임

설정 전

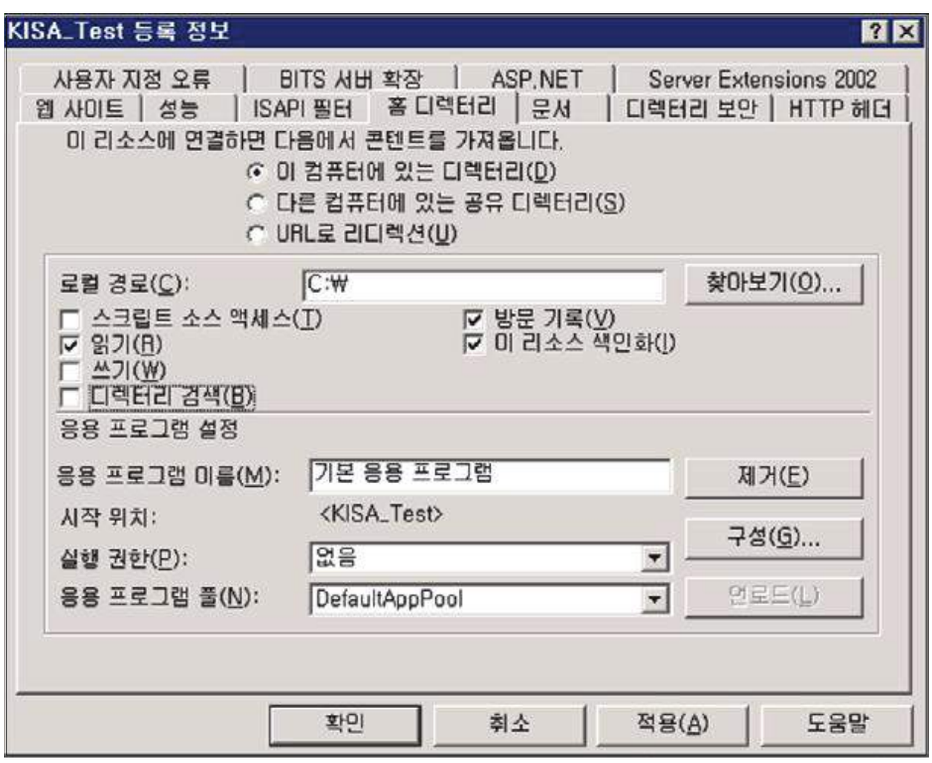
```
<Directory "/var/www/html">
Options Indexes
</Directory>
```

설정 후

```
<Directory "/var/www/html">
Options
</Directory>
```

■ 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



웹(Web)

DI (상)	8. 디렉터리 인덱싱

■ IIS 7.5/8.0

IIS(인터넷 정보 서비스) 관리자 > [해당 웹 사이트] > [IIS] > [디렉터리 검색] 선택
우측의 [사용 안 함] 버튼을 눌러 비활성화

■ WebtoB 설정

Step 1) ${WEBTOBDIR}/config/http.m 파일 Options 항목에서 index 옵션 삭제 또는, –index 옵션으로 설정 (default: -index)

Step 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"
```

Step 3) 확인 후 설정파일 컴파일 및 재구동

wscfl -i http.m (http.m 파일 컴파일)

wsdown

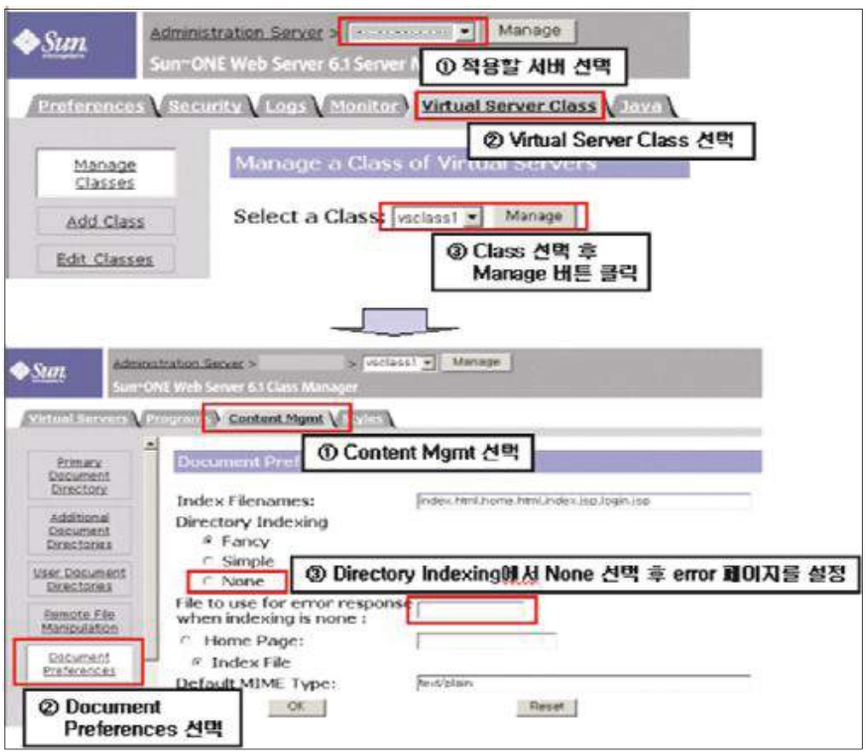
wsboot (재구동)

DI (상)	8. 디렉터리 인덱싱

■ iPlanet

Step 1) 관리자 콘솔에서 설정 (※ 1번 또는, 2번 방법 중 선택 적용)

관리자 콘솔 > Server Name > Virtual Server Class > Class Manage > Content Mgmt > Document Preferences > Directory Indexing 항목 "None" 설정



Step 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|HEA
Service method="TRACE" fn
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)

DI (상)	8. 디렉터리 인덱싱

■ %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|\?)\.jsp">
AllowOverride None
Deny from all
</LocationMatch>
```

Resin 2.1.x 에서는 최신 버전으로 업그레이드 하거나 아래와 같이 설정 할 수 있음
Step 1) Resin 환경 설정 파일 (resin.conf)에서 가상 디렉터리 설정 부분인 "web-app id"를 찾음
Step 2) 아래 내용 추가
<directory-servlet>none</directory-servlet>
※ 주의할 점: 모든 가상 디렉터리에 적용 필요

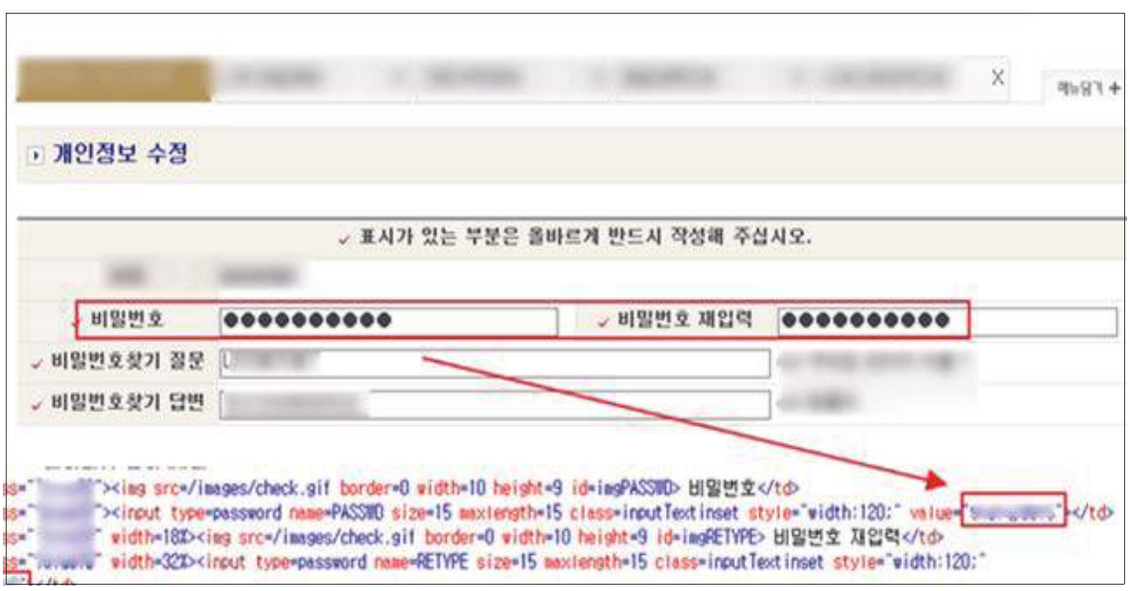
조치 시 영향	일반적으로 영향 없음

웹(Web)

IL (상)	9. 정보 누출
취약점 개요	
점검내용	■ 웹 서비스 시 에러 페이지 노출 여부 점검
점검목적	■ 에러 상황에서 적절한 에러 페이지가 노출되도록 하여 2차 공격에 활용될 수 있는 불필요한 정보 노출을 차단하기 위함
보안위협	■ 웹사이트 내 적절한 에러 페이지가 마련되지 않은 경우 오류 메시지에서 웹 사이트의 민감한 정보(소스 코드 내 계정 및 비밀번호, 애플리케이션정보, DB정보, 웹서버 구성 정보, 개발 과정의 코멘트 등)가 노출되어 공격자들의 2차 공격을 위한 정보로 활용 될 수 있음
참고	※ 소스코드 및 취약점 점검 필요
점검대상 및 판단기준	
대상	■ 소스코드, Web Server
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
점검 및 조치 사례	

■ 점검방법

Step 1) html 소스 내에 개인 정보(화면엔 마스킹 처리되지만 소스에는 그대로 표시), 인증정보, DB 접속 정보 등의 중요 정보가 노출되고 있는지 확인



웹(Web)

IL (상)	9. 정보 누출

Step 2) 에러 메시지에서 중요 정보(시스템 정보, 절대 경로 정보, 컴파일 소스 정보 등)가 노출되는지 확인

■ 보안설정방법

Step 1) 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

Step 2) 일반적으로 웹에서 발생하는 에러 메시지는 400, 500번대의 에러코드를 리턴하게 되는데 이러한 에러 코드에 대해 별도의 에러 페이지로 Redirect하거나 적절한 에러 처리 루틴을 설정하여 처리 되도록 함(전체적인 통합 에러 페이지를 작성한 후 모든 에러코드에 대해 통합 에러 페이지로 리다이렉트 되도록 설정)

※ 웹 서버 별 상세 설정

■ 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
```

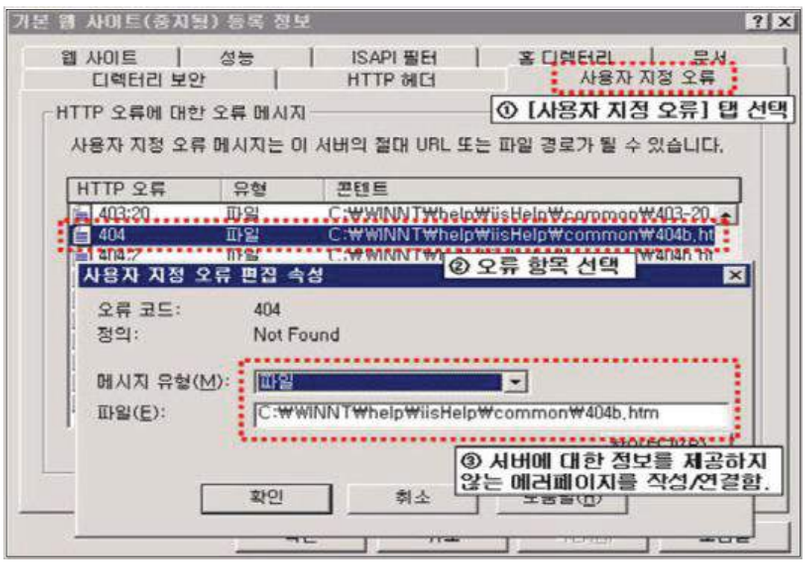
위와 같이 특정 에러코드에 대해 에러 메시지를 출력할 수도 있고 특정 웹 페이지로 Redirect 시킬 수 있으며, 이 설정은 httpd.conf 의 전역 설정에 추가 하거나 원하는 가상 호스트의 <VirtualHost> </VirtualHost> 사이에 추가하면 됨

■ 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

웹(Web)

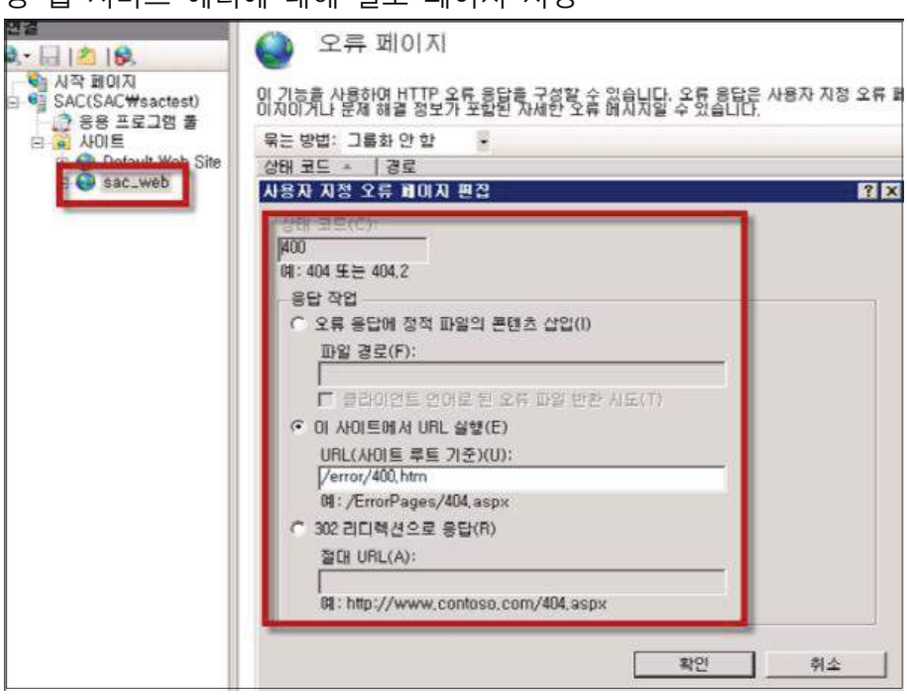
IL (상)	9. 정보 누출



■ IIS 7.0 설정

Step 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



Step 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

웹(Web)

CS (상)	10. 악성 콘텐츠
취약점 개요	
점검내용	■ 게시판 등에 악성 콘텐츠 삽입 및 실행 여부 점검
점검목적	■ 사이트 내 악의적인 콘텐츠 삽입 및 실행을 방지하기 위함
보안위협	■ 웹 사이트 게시판, 댓글, 자료실 등에 정상적인 콘텐츠 대신에 악성 콘텐츠를 주입하여 실행 될 경우 사용자가 원본 콘텐츠 대신 악성코드 감염 및 웹 페이지 변조 등 사용자에게 악의적인 영향을 미칠 수 있는 악성 콘텐츠를 열람할 수 있음
참고	※ 기반시설 특성상 원칙적으로 업로드 기능을 제한해야하나 꼭 사용하여야 할 경우에는 특정 사용자만이 허용된 특정 확장자의 콘텐츠 파일만 업로드 할 수 있게 제한하도록 권고함 ※ 관련 점검 항목 : XS(상), FU(상) ※ 소스코드 및 취약점 점검 필요
점검대상 및 판단기준	
대상	■ 소스코드, 웹 방화벽
판단기준	**양호 :** 악의적 콘텐츠가 실행되지 않는 경우
	취약 : 악의적 콘텐츠가 입력되며, 실행되는 경우
조치방법	사용자 입력 값에 대한 검증 로직 추가 및 실행 제한 설정
점검 및 조치 사례	
■ 점검방법 Step 1) 콘텐츠 삽입 및 파일 업로드 제한 필터링 적용 여부 점검 Step 2) 게시판 등의 페이지에서 강제적으로 이뤄지는 악의적인 프로그램 다운로드 및 콘텐츠 자동 실행이나 악의적인 사이트로의 이동이 발생하는지 확인 **■ 보안설정방법** Step 1) 악성 콘텐츠가 삽입되어 있는 페이지에 대하여 증거자료(화면, 소스 등)를 남기고, 삽입된 악성 콘텐츠를 삭제하거나 페이지의 삭제 등을 실시함 취득한 증거자료를 가지고 악성 콘텐츠의 삽입 원인에 대하여 분석하여 원인을 제거할 것을 권고함 Step 2) 게시판의 글 등록 및 파일 업로드 기능에 Flash 파일이나 avi 동영상 파일, exe 실행 파일 등 악성코드가 포함될 수 있는 콘텐츠를 삽입 또는 업로드 하지 못하게 필터링 적용 Step 3) 주기적으로 업로드 된 파일을 대상으로 바이러스 검사 실시	
조치 시 영향	일반적으로 영향 없음

XS (상)	11. 크로스사이트 스크립팅
취약점 개요	
점검내용	■ 웹 페이지 내 크로스사이트 스크립팅 취약점 존재 여부 점검
점검목적	■ 웹 페이지 내 크로스사이트 스크립팅 취약점을 제거하여 악성 스크립트의 실행을 차단
보안위협	■ 웹 애플리케이션에서 사용자 입력 인수 값에 대한 필터링이 제대로 이루어지지 않을 경우, 사용자 인수 값을 받는 웹 사이트 게시판, URL 등에 악의적인 스크립트(자바스크립트, VB 스크립트, ActiveX, 플래시 등)를 삽입하여 게시글이나 이메일을 읽는 사용자의 쿠키(세션)를 도용하거나 악성코드(URL 리다이렉트)를 유포할 수 있음
참고	※ **크로스사이트 스크립팅:** 악의적인 사용자가 공격하려는 사이트에 스크립트를 넣는 기법으로 공격 방식은 크게 stored 공격 방식과 reflected 공격 방식으로 나누어 짐 ※ OWASP - XSS 필터링 관련 참고사항 https://www.owasp.org/index.php/XSS_Filter_Evasion_Cheat_Sheet ※ 소스코드 및 취약점 점검 필요
점검대상 및 판단기준	
대상	■ 소스코드, 웹 방화벽
판단기준	**양호 :** 사용자 입력 인수 값에 대한 검증 및 필터링이 이루어지는 경우
	취약 : 사용자 입력 값에 대한 검증 및 필터링이 이루어지지 않으며, HTML 코드가 입력·실행되는 경우
조치방법	웹 사이트의 게시판, 자료실, URL 등에서 사용자로부터 입력받는 인수 값에 대해 검증 로직을 추가하거나 인수 값이 입력되더라도 실행되지 않게 하고, 부득이하게 게시판에서 HTML을 사용하는 경우 HTML 코드 중 필요한 코드에 대해서만 입력 가능하도록 설정
점검 및 조치 사례	

■ 점검방법

※ XSS 취약 유형

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

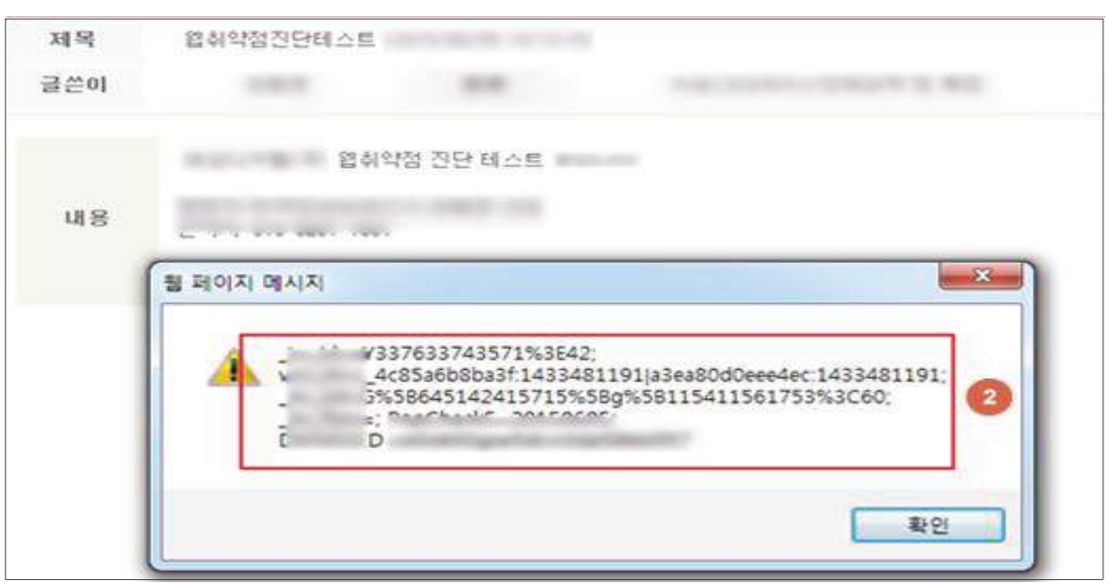
웹(Web)

XS (상)	11. 크로스사이트 스크립팅

XSS를 유발할 수 있는 스크립트	<script> … </script> <img src="javascript:…..">"> <embed>…</embed> <iframe></iframe> ※ Filtering을 우회하기 위해 다양한 표현 가능 ◆ %3Cscript%3E.....%3Cscript%3E ◆ Javascript; ◆ Java
script ◆ Java
script

Step 1) 사용자 인수 값을 입력받는 애플리케이션(회원정보 변경, 게시판, 댓글, 자료실 등)에 스크립트 입력 후 실행되는지 확인

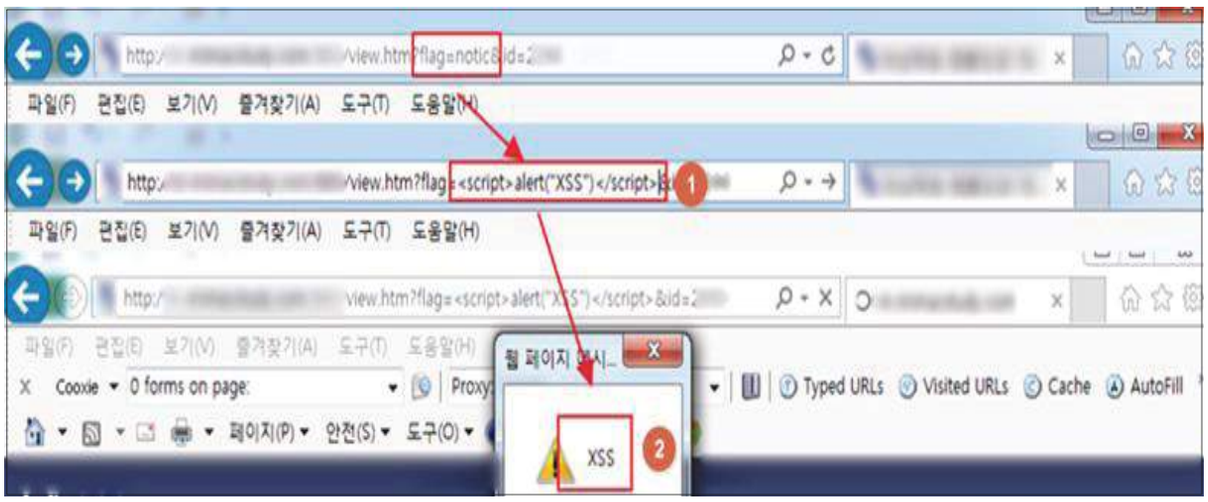
[게시글에 스크립트 삽입(stored)]



[스크립트 코드 동작]

XS (상)	11. 크로스사이트 스크립팅

Step 2) 사용자 인수 값을 입력받는 애플리케이션(검색, URL)에 스크립트 입력 후 실행되는지 확인



■ 보안설정방법

Step 1) 게시물에 HTML이나 자바 스크립트에 해당되는 태그 사용을 사전에 제한하고, 사용자가 입력한 인수 값에 대한 필터링 작업 필요

Step 2) 게시물의 본문뿐만 아니라 제목, 댓글, 검색어 입력 창, 그 외 사용자 측에서 넘어오는 값을 신뢰하는 모든 form과 인수 값에 대해서 필터링을 수행함

Step 3) 입력 값에 대한 필터링 로직 구현 시 공백 문자를 제거하는 trim, replace 함수를 사용하여 반드시 서버 측에서 구현되어야 함

※ 필터링 조치 대상 입력 값

- 스크립트 정의어 : <SCRIPT>, <OBJECT>, <APPLET>, <EMBED>, <FORM>, <IFRAME> 등
- 특수문자 : <, >, ", ', &, %, %00(null) 등

Step 4) URLDecoder 클래스에 존재하는 decode 메소드를 통해 URL 인코딩이 적용된 사용자 입력 값을 디코딩함으로써 우회 공격 차단

Step 5) 웹 방화벽에 모든 사용자 입력 폼(회원정보 변경, 게시판, 댓글, 자료실, 검색, URL 등)을 대상으로 특수문자, 특수 구문 필터링하도록 룰셋 적용

웹(Web)

XS (상)	11. 크로스사이트 스크립팅

※ 애플리케이션 별 보안 설정 방법

■ ASP

```
<%
... 중략 ...
If use_HTML Then
   content = Server.HTMLEncode(content)
... 중략 ...

ub ReplaceStr(content, byref str)
      content = replace(content, "'", " ₩'")
      content = replace(content, "&", "&amp;")
      content = replace(content, " ₩'", "&quot")
      content = replace(content, "<", "&lt")
      content = replace(content, ">", "&gt")

      str = content
End Sub
      ... 중략 ...
%>
```

■ PHP

```
... 중략 ...
   if($use_html == 1) // HTML tag를 사용하게 할 경우 부분 허용
      $memo = str_replace("<", "&lt", $memo);// HTML TAG 모두 제거
      $tag = explode(",", $use_tag);

      for($i=0; $i<count($tag); $i++) { // 허용할 TAG만 사용 가능하게 변경
            $memo = eregi_replace("&lt".$tag[$i]." ", "<".$tag[$i]." ", $memo);
            $memo = eregi_replace("&lt".$tag[$i].">", "<".$tag[$i].">", $memo);
            $memo = eregi_replace("&lt/".$tag[$i], "</".$tag[$i], $memo); }
      else // HTML tag를 사용하지 못하게 할 경우
      $memo = str_replace("<", "&lt", $memo);
      $memo = str_replace(">", "&gt", $memo);
      ... 중략 ...
```

XS (상)	11. 크로스사이트 스크립팅

■ JSP

```
<%
... 중략 ...
tring subject = request.getParameter("subject_BOX");
      subject = subject.replaceAll("<", "&lt");
      subject = subject.replaceAll(">", "&gt");
        ... 중략 ...
%>
```

※ 참고: 필터링 대상

<	>	<	>	innerHTML
javascript	eval	onmousewheel	onactive	onfocusout
expression	charset	ondataavailable	oncut	onkeyup
applet	document	onafteripudate	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	onbeforeuload	ondragover	onuload
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)

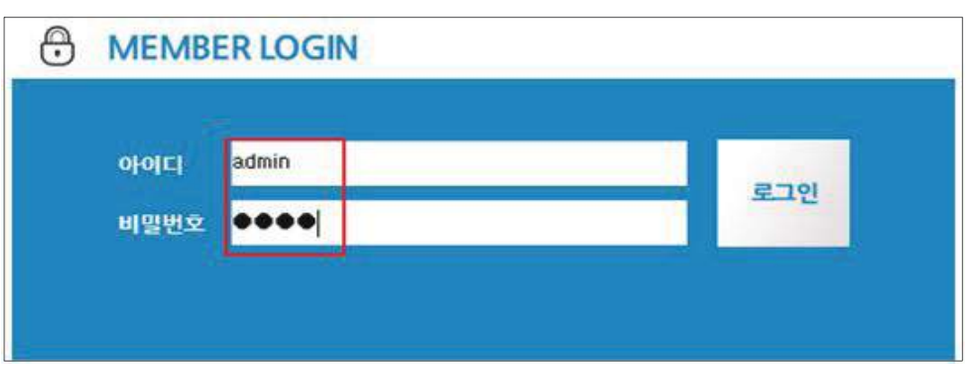
BF (상)	12. 약한 문자열 강도
취약점 개요	
점검내용	■ 웹페이지 내 로그인 폼 등에 약한 강도의 문자열 사용 여부 점검
점검목적	■ 유추 가능한 취약한 문자열 사용을 제한하여 계정 및 패스워드 추측 공격을 방지하기 위함
보안위협	■ 해당 취약점 존재 시 유추가 용이한 계정 및 패스워드의 사용으로 인한 사용자 권한 탈취 위험이 존재하며, 해당 위험을 방지하기 위해 값의 적절성 및 복잡성을 검증하는 체크 로직을 구현하여야 함
참고	※ **약한 문자열 강도 취약점:** 웹 애플리케이션에서 회원가입 시 안전한 패스워드 규칙이 적용되지 않아 취약한 패스워드로 회원가입이 가능할 경우 공격자가 추측을 통한 대입 및 주변 정보를 수집하여 작성한 사전파일 통한 대입을 시도하여 사용자의 패스워드를 추출할 수 있는 취약점 ※ 소스코드 및 취약점 점검 필요
점검대상 및 판단기준	
대상	■ 소스코드
판단기준	**양호 :** 관리자 계정(비밀번호 포함)이 유추하기 어려운 계정으로 설정되어 있는 경우
	취약 : 관리자 계정(비밀번호 포함)이 유추하기 쉬운 계정으로 설정되어 있는 경우
조치방법	계정 및 비밀번호의 체크 로직 추가 구현
점검 및 조치 사례	

■ 점검방법

Step 1) 웹 사이트 로그인 페이지의 로그인 창에 추측 가능한 계정이나 패스워드를 입력하여 정상적으로 로그인 되는지 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



웹(Web)

BF (상)	12. 약한 문자열 강도

■ 보안설정방법

Step 1) 취약한 계정 및 패스워드를 삭제하고, 사용자가 취약한 계정이나 패스워드를 등록하지 못하도록 패스워드 규정이 반영된 체크 로직을 구현하여야 함

※ 규정 예시

Step 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)

Step 2) 연속적인 숫자나 생일, 전화번호 등 추측하기 쉬운 개인정보 및 아이디와 비슷한 비밀번호는 사용하지 않는 것을 권고

Step 3) 비밀번호에 유효기간을 설정하여 반기별 1회 이상 변경

조치 시 영향	일반적으로 영향 없음

웹(Web)

IA (상)	13. 불충분한 인증
취약점 개요	
점검내용	■ 중요 페이지 접근 시 추가 인증 요구 여부 점검
점검목적	■ 중요 페이지에 추가 인증으로 접근을 강화하여 불필요한 정보의 노출 및 변조를 차단하기 위함
보안위협	■ 중요 정보(회원정보 등) 페이지에 대한 인증 절차가 불충분할 경우 발생하는 취약점으로 권한이 없는 사용자가 중요 정보 페이지에 접근하여 정보를 유출하거나 변조할 수 있으므로 중요 정보 페이지에는 추가적인 인증 절차를 구현하여야 함
참고	※ 소스코드 및 취약점 점검 필요
점검대상 및 판단기준	
대상	■ 소스코드
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
점검 및 조치 사례	

■ **점검방법**

Step 1) 중요 정보(회원정보 변경) 페이지 접근 전에 재인증 여부 확인

Step 2) 인증 후 페이지에 아이디만을 인증 값으로 하여 변수로 관리되고 있는지 확인

웹(Web)

IA (상)	13. 불충분한 인증

■ **보안설정방법**

Step 1) 중요 정보(회원정보 변경) 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

Step 2) 접근 통제 정책을 구현하고 있는 코드는 구조화, 모듈화가 되어 있어야 함

Step 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

Step 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

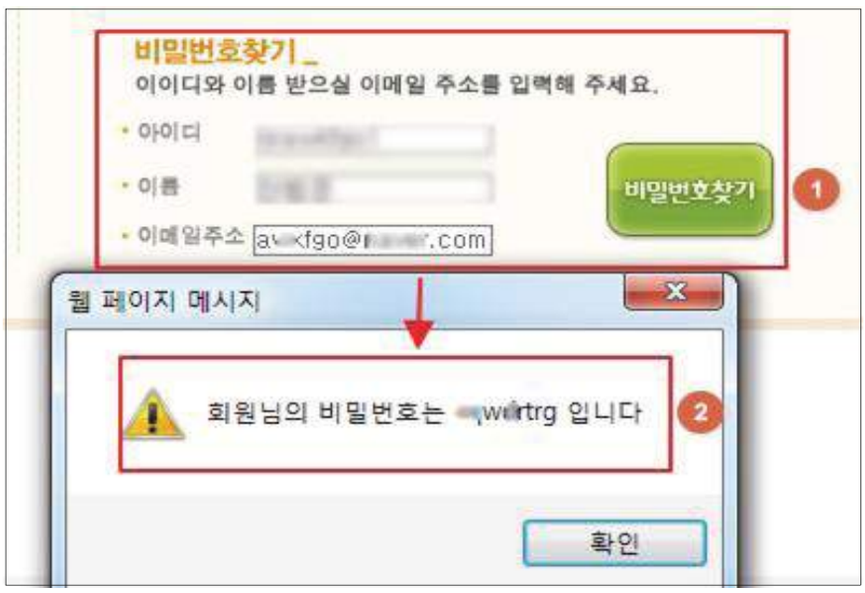
조치 시 영향	일반적으로 영향 없음

웹(Web)

PR (상)	14. 취약한 패스워드 복구
취약점 개요	
점검내용	■ 웹 사이트 내 패스워드 복구 절차의 적절성 점검
점검목적	■ 패스워드 복구 로직을 유추하기 어렵게 구현하고, 인증된 사용자 메일이나 SMS에서만 복구 패스워드를 확인할 수 있도록 하여 비인가자를 통한 사용자 패스워드 획득 및 변경을 방지하기 위함
보안위협	■ 취약한 패스워드 복구 로직(패스워드 찾기 등)으로 인하여 공격자가 불법적으로 다른 사용자의 패스워드를 획득, 변경할 수 있음
참고	※ 소스코드 및 취약점 점검 필요
점검대상 및 판단기준	
대상	■ 소스코드
판단기준	**양호 :** 패스워드 재설정 시 난수를 이용하여 재설정하고 인증된 사용자 메일이나 SMS로 재설정된 패스워드 전송 시
	취약 : 패스워드 재설정 시 일정 패턴으로 재설정되고 웹 사이트 화면에 바로 출력 시
조치방법	패스워드 복구 로직을 변경하고 인증된 사용자 메일이나 SMS에서만 재설정된 패스워드를 확인 가능하도록 조치
점검 및 조치 사례	
■ 점검방법 Step 1) 재설정(또는 패스워드 찾기)되는 패스워드 몇 개를 획득하여 사용자의 연락처, 주소, 메일 주소, 일정 패턴을 패스워드로 이용하고 있는지 확인하고 재설정된 패스워드를 인증된 사용자 메일이나 SMS로 전송하는지 확인	

웹(Web)

PR (상)	14. 취약한 패스워드 복구



■ 보안설정방법

Step 1) 사용자의 개인 정보(연락처, 주소, 메일 주소 등)로 패스워드를 생성하지 말아야 하며, 난수를 이용한 불규칙적이고 최소 길이(6자 이상 권고) 이상의 패턴이 없는 패스워드를 발급하여야 함

Step 2) 사용자 패스워드를 발급해주거나 확인해줄 때 웹 사이트 화면에 바로 출력해주는 것이 아니라 인증된 사용자 메일이나 SMS로 전송해주어야 함

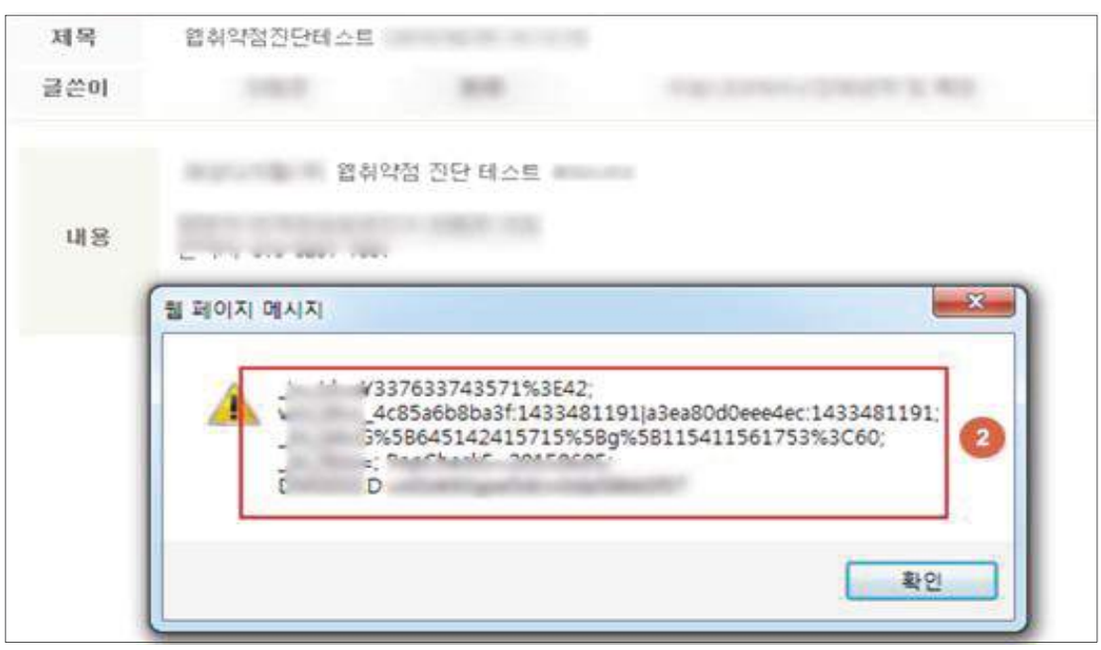
조치 시 영향	일반적으로 영향 없음

웹(Web)

CF (상)	15. 크로스사이트 리퀘스트 변조(CSRF)
취약점 개요	
점검내용	■ 사용자의 신뢰(인증) 정보의 변조 여부 점검
점검목적	■ 사용자 입력 값에 대한 적절한 필터링 및 인증에 대한 유효성을 검증하여 신뢰(인증) 정보 내의 요청(Request)에 대한 변조 방지
보안위협	■ 사용자의 신뢰(인증) 정보 내에서 사용자의 요청(Request)을 변조함으로써 해당 사용자의 권한으로 악의적인 공격을 수행할 수 있음
참고	※ **CSRF(Cross-site request forgery):** 사용자가 자신의 의지와는 무관하게 공격자가 의도한 행위(수정, 삭제, 등록 등)를 특정 웹사이트에 요청하게 하는 공격 유형 ※ 소스코드 및 취약점 점검 필요
점검대상 및 판단기준	
대상	■ 소스코드, 웹 방화벽
판단기준	**양호 :** 사용자 입력 값에 대한 검증 및 필터링이 이루어지는 경우
	취약 : 사용자 입력 값에 대한 필터링이 이루어지지 않으며, HTML 코드(또는 스크립트)를 입력하여 실행되는 경우
조치방법	사용자 입력 값에 대해 검증 로직 및 필터링 추가 적용
점검 및 조치 사례	

■ 점검방법

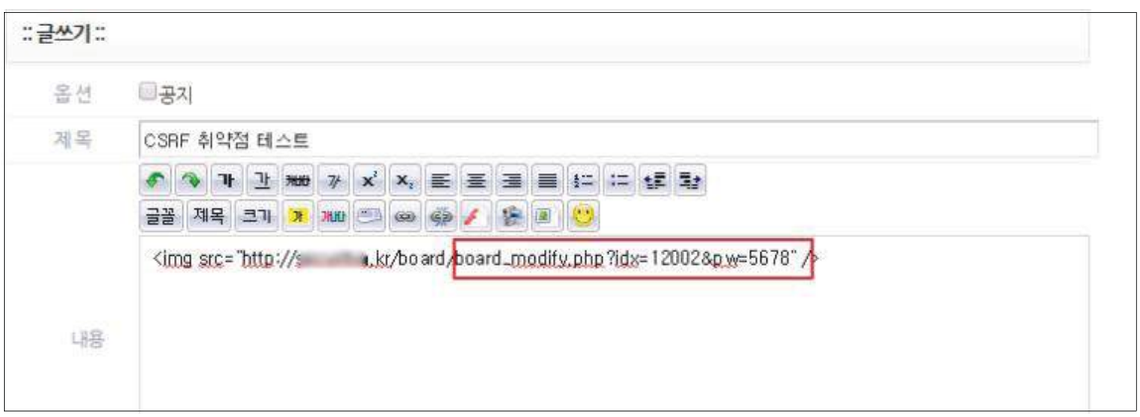
Step 1) XSS 취약점이 존재하는지 확인



CF (상)	15. 크로스사이트 리퀘스트 변조(CSRF)

Step 2) 등록 및 변경 등의 데이터 수정 기능의 페이지가 있는지 조사함

Step 3) 데이터 수정 페이지에서 전송되는 요청(Request)을 취득 후 인수 값을 변조하여 변조한 인수 값의 권한을 가진 사용자가 게시글(회원정보변경 등)을 열람하였을 경우 전송한 인수 값의 데이터가 정상적으로 수행되는지 점검



■ 보안설정방법

Step 1) 사용자가 입력하는 값에 대한 검증 로직 구현

Step 2) 정상적인 리퀘스트와 비정상적인 리퀘스트를 구분할 수 있도록 Form/URL 에서 임의의 토큰을 추가하고 이 토큰을 검증하도록 설계

Step 3) HTML 이나 자바스크립트에 해당되는 태그 사용을 사전에 제한하고, 서버 단에서 사용자 입력 값에 대한 필터링 구현

Step 4) HTML Editor 사용으로 인한 상기사항 조치 불가 시, 서버 사이드/서블릿/DAO(Data Access Object) 영역에서 조치하도록 설계

Step 5) XSS 조치 방안 참조

조치 시 영향	일반적인 경우 영향 없음

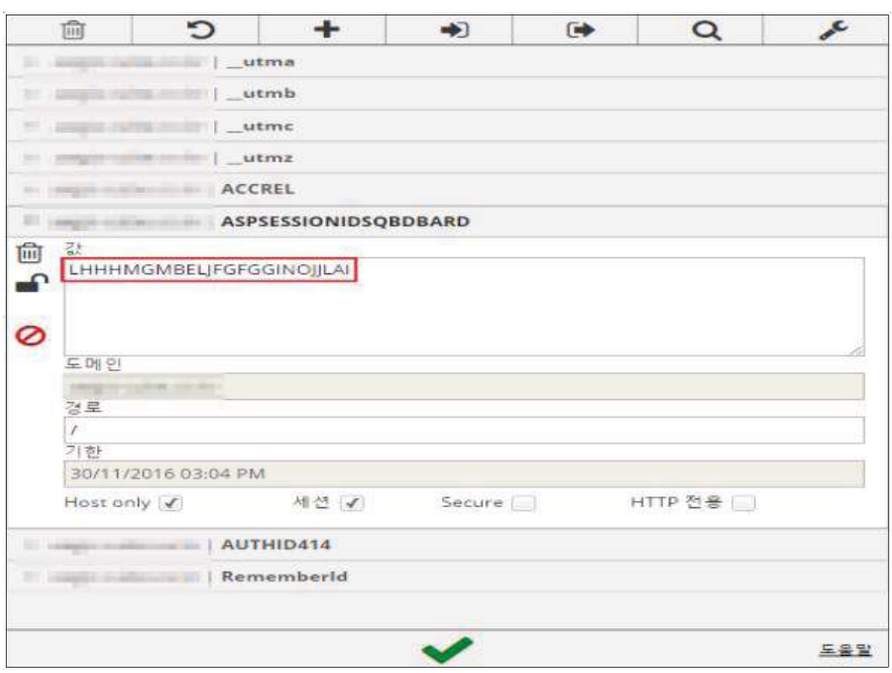
웹(Web)

SE (상)	16. 세션 예측
취약점 개요	
점검내용	■ 단순한 방법(연속된 숫자 할당 등)으로 생성되는 세션 ID를 예측하여 세션 탈취 여부 점검
점검목적	■ 사용자의 세션ID를 추측 불가능하도록 난수로 생성하여 공격자의 불법적인 접근을 차단하기 위함
보안위협	■ 사용자에게 전달하는 세션 ID가 일정한 패턴을 가지고 있는 경우 공격자가 세션 ID를 추측하여 불법적인 접근을 시도할 수 있음
참고	※ **세션(Session):** 일정 시간동안 같은 사용자(브라우저)로 부터 들어오는 일련의 요구를 하나의 상태로 보고 그 상태를 일정하게 유지시키는 기술 ※ 소스코드 및 취약점 점검 필요
점검대상 및 판단기준	
대상	■ 소스코드
판단기준	**양호 :** 추측 불가능한 세션 ID가 발급되는 경우
	취약 : 세션 ID가 일정한 패턴으로 발급되는 경우
조치방법	추측 불가능한 세션 ID가 발급되도록 로직 구현
점검 및 조치 사례	

■ 점검방법

Step 1) 각기 다른 IP 주소와 다른 사용자명, 시간적 차이로 세션 ID를 발급받음

Step 2) 발급받은 세션 ID에 일정한 패턴이 있는지 조사



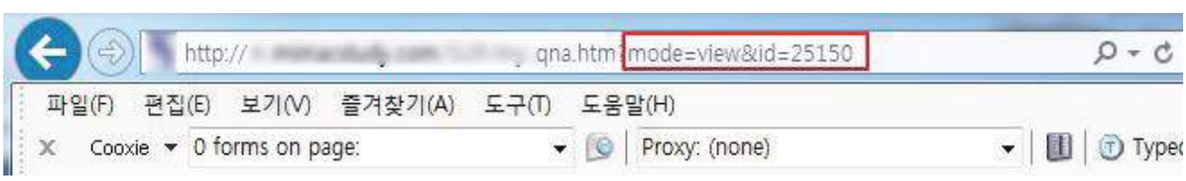
SE (상)	16. 세션 예측
Step 3) 일정한 패턴이 확인되고, 패턴에 의해 사용 가능한 세션 ID의 예측이 가능한지 확인 **■ 보안 설정 방법** 아무리 길이가 길고 복잡한 항목으로 세션 ID가 만들어져도 공격자가 충분한 시간과 자원이 있다면 뚫는 것은 불가능하지 않으므로 강력한 세션 ID를 생성하여야 함 주된 목적은 수많은 대역폭과 처리 자원을 가지고 있는 공격자가 하나의 유효한 세션 ID를 추측하는데 최대한 오랜 시간이 걸리게 하여 쉽게 추측하지 못하게 하는 것에 있음 단순 조합 보다는 상용 웹 서버나 웹 애플리케이션 플랫폼에서 제공하는 세션 ID를 사용하고, 가능하다면 맞춤형 세션 관리 체계를 권고함 세션 ID는 로그인 시마다 추측할 수 없는 새로운 세션 ID로 발급하여야 함	
조치 시 영향	일반적인 경우 영향 없음

웹(Web)

IN (상)	17. 불충분한 인가
취약점 개요	
점검내용	■ 민감한 데이터 또는 기능에 접근 및 수정 시 추가 인증 절차 여부 점검
점검목적	■ 접근 권한에 대한 검증 로직을 구현하여 다른 사용자가 민감한 정보나 인증이 필요한 페이지의 접근을 차단하기 위함
보안위협	■ 중요 정보 페이지 접근을 위한 인증 로직이 구현되지 않을 경우, 비인가 사용자의 페이지에 접근 및 중요 정보의 열람 및 변조가 가능함
참고	※ 소스코드 및 취약점 점검 필요
점검대상 및 판단기준	
대상	■ 소스코드
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
점검 및 조치 사례	

■ **점검방법**

Step 1) 비밀 게시글(또는 개인 정보 수정, 패스워드 변경 등) 페이지에서 다른 사용자와의 구분을 ID, 일련번호 등의 단순한 값을 사용하는지 조사



Step 2) 게시글을 구분하는 인수 값을 변경하는 것만으로 다른 사용자의 비밀 게시글(또는 개인 정보 변경, 패스워드 변경 등)에 접근 가능한지 확인

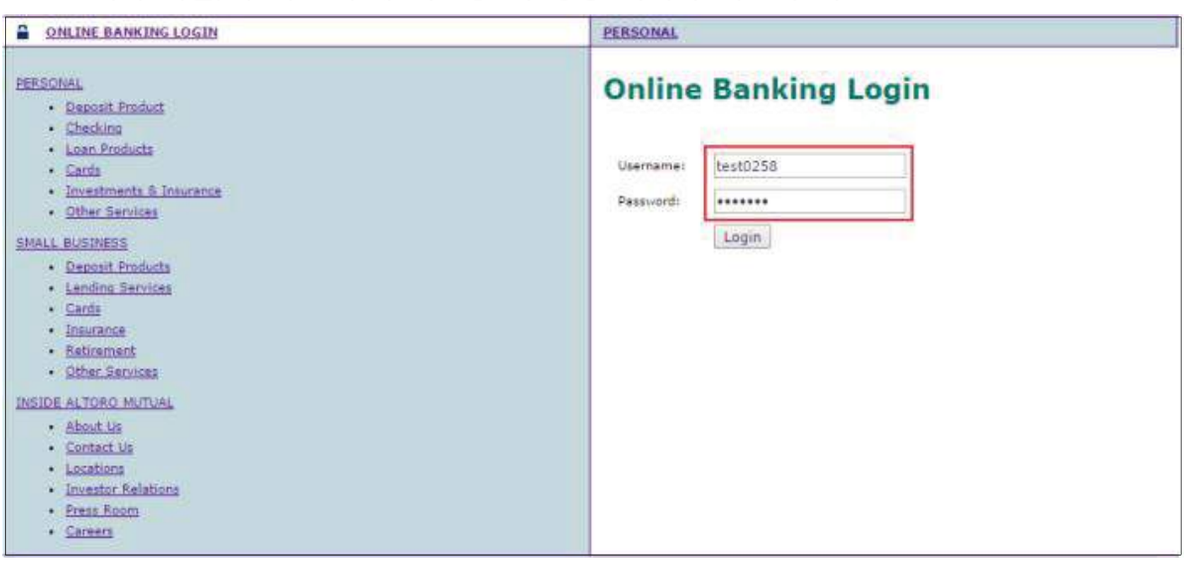
IN (상)	17. 불충분한 인가
■ 보안설정방법 Step 1) 민감한 중요 데이터에 대한 접근 페이지에서 인증을 위한 로직이 구현되지 않았다면, 세션을 통한 인증 및 사용자에게 확인을 위한 인증 값 입력을 통한 인증 절차를 구현하여 정상적인 로그인 사용자인지 또는 권한이 허용된 사용자인지 여부를 확인 후 해당 페이지에 접근할 수 있도록 함 Step 2) 페이지별 권한 매트릭스를 작성하여, 페이지에 부여된 권한의 타당성을 체크 후에 권한 매트릭스를 기준으로 하여 전 페이지에서 권한 체크가 이뤄지도록 구현하여야 함	
조치 시 영향	일반적인 경우 영향 없음

웹(Web)

SC (상)	18. 불충분한 세션 만료
취약점 개요	
점검내용	■ 세션의 만료 기간 설정 여부 점검
점검목적	■ 세션 타임아웃 기능을 구현하여 공격자가 만료되지 않은 세션 활용을 방지하기 위함
보안위협	■ 세션의 만료 기간을 정하지 않거나, 만료기한을 너무 길게 설정된 경우 악의적인 사용자가 만료되지 않은 세션을 활용하여 불법적인 접근이 가능할 수 있음
참고	※ 소스코드 및 취약점 점검 필요
점검대상 및 판단기준	
대상	■ 소스코드, Web Server
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(세션 종료 시간은 사이트의 특성에 따라 달라질 수 있으므로 사이트의 특성에 맞게 적정 시간 설정)
점검 및 조치 사례	

■ 점검방법

Step 1) 인증 후 정상적으로 세션이 발행된 페이지의 리퀘스트를 취득하여 일정 시간(사이트에 따라 다름)이 지난 후에 재전송 시 정상 처리가 되는지 확인



[로그인 후 세션 발급]

SC (상)	18. 불충분한 세션 만료

[일정 시간 경과 후 세션 유지 여부 확인]

■ 보안설정방법

Step 1) 세션 타임아웃 기능이 구현되어 있지 않을 경우 장시간 부재중인 사용자에 대한 보호 장치가 없는 것이며, 세션 타임아웃 구현 시 타임아웃 시간은 10분으로 설정할 것을 권고함

※ 애플리케이션 별 설정 방법

■ 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 ...
```

구분		설 명
Property	SessionID	사용자마다 갖게 되는 고유한 세션 값
	Timeout	세션이 유지되는 기간
Method	Abandon	강제로 세션을 소멸시키는 함수
Event	Onstart	각각의 사용자가 처음 방문할 때 발생
	Onend	사용자의 세션이 끝나는 시점에 발생

웹(Web)

SC (상)	18. 불충분한 세션 만료

■ 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

Step 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>
```

Step 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 …
```

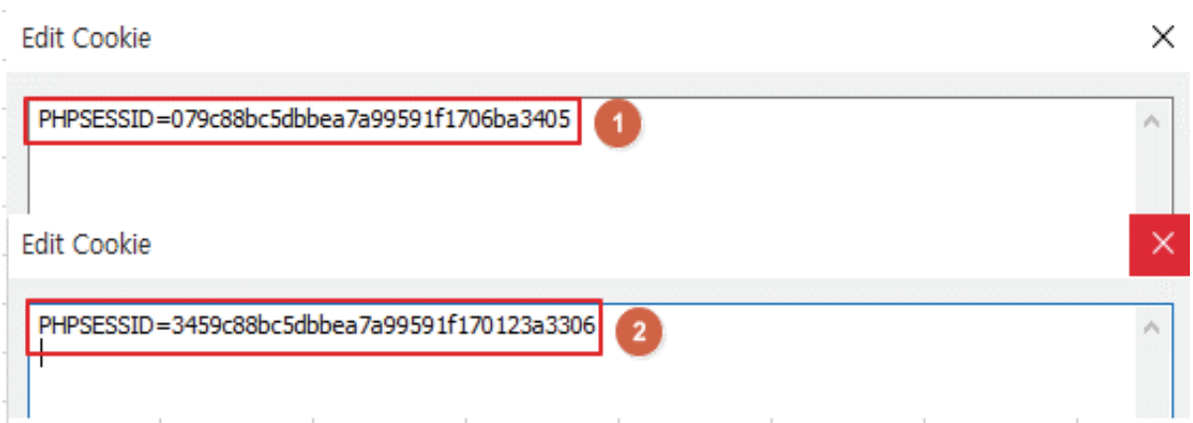
조치 시 영향	일반적으로 영향 없음

웹(Web)

SF (상)	19. 세션 고정
취약점 개요	
점검내용	■ 사용자 로그인 시 항상 일정하게 고정된 세션 ID값을 발행하는지 여부 확인
점검목적	■ 로그인 할 때마다 예측 불가능한 새로운 세션 ID를 발행하여 세션 ID의 고정 사용을 방지하기 위함
보안위협	■ 사용자 로그인 시 항상 일정하게 고정된 세션ID가 발행되는 경우 세션 ID를 도용한 비인가자의 접근 및 권한 우회가 가능
참고	※ 소스코드 및 취약점 점검 필요
점검대상 및 판단기준	
대상	■ 소스코드
판단기준	**양호 :** 로그인 할 때마다 예측 불가능한 새로운 세션 ID가 발행되고, 기존 세션 ID는 파기될 경우
	취약 : 로그인 세션 ID가 고정 사용되거나 새로운 세션 ID가 발행되지만 예측 가능한 패턴으로 발행될 경우
조치방법	사용자가 로그인 할 때마다 예측 불가능한 새로운 세션 ID 생성 로직 구현하고 기존 세션 ID는 파기함
점검 및 조치 사례	

■ 점검방법

Step 1) 로그인 시(1) 세션 ID가 발행되는지 확인하고 로그아웃 후 다시 로그인(2) 할 때 예측 불가능한 새로운 세션 ID가 발급되는지 확인



■ 보안설정방법

로그인 할 때마다 예측 불가능한 새로운 세션 ID를 발급받도록 해야 하고 기존 세션 ID는 파기해야 함

조치 시 영향	일반적인 경우 영향 없음

웹(Web)

AU (상)	20. 자동화 공격
취약점 개요	
점검내용	■ 자동화된 공격으로 인한 다수 수의 프로세스 실행 여부 점검
점검목적	■ 웹 애플리케이션에 구현된 기능의 적절성에 대한 검증 로직을 구현하여 자동화 공격 및 무차별 대입 공격 방지
보안위협	■ 웹 애플리케이션의 특정 프로세스에 대한 접근 시도 횟수 제한을 설정하지 않고 자동화 공격을 방치하면, 웹사이트를 다운시키거나 무차별 대입 공격으로 인해 사용자 계정을 탈취할 수 있고, 데이터 등록 또는 메일 발송 기능 등을 이용하여 악의적인 활용이 가능
참고	※ 소스코드 및 취약점 점검 필요
점검대상 및 판단기준	
대상	■ 소스코드, 웹 방화벽
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 및 웹 방화벽 룰셋 설정을 통해 대량의 불특정 프로세스 요청 차단
점검 및 조치 사례	

■ 점검방법

Step 1) 데이터 등록 및 메일 발송의 기능에서 반복적인 기능을 이용하여 대량의 데이터 등록이나 메일 발송이 가능한지 확인

■ 보안설정방법

Step 1) 데이터 등록 및 메일 발송 기능에서 사용자 등록이 일회성이 될 수 있도록, 캡차(이미지를 이용하여 확인 값을 표시하고 사용자가 값을 등록하여 인증함) 등 일회성 확인 로직을 구현하여야 함

※ **캡차(CAPTCHA)**: 자동화된 컴퓨터와 사람을 판별하기 위한 기술의 일종

AU (상)	20. 자동화 공격

Step 2) 자동화 공격을 시도하면 짧은 시간에 다량의 패킷(양)이 전송되므로 이를 공격으로 감지하고 방어할 수 있는 IDS/IPS의 시스템을 구축하여야 함

Step 3) 서버에 요청되는 패킷(양)을 모니터링 할 수 있는 시스템 구축이 없이는 적시 적절한 방어가 어려움

조치 시 영향	일반적인 경우 영향 없음

웹(Web)

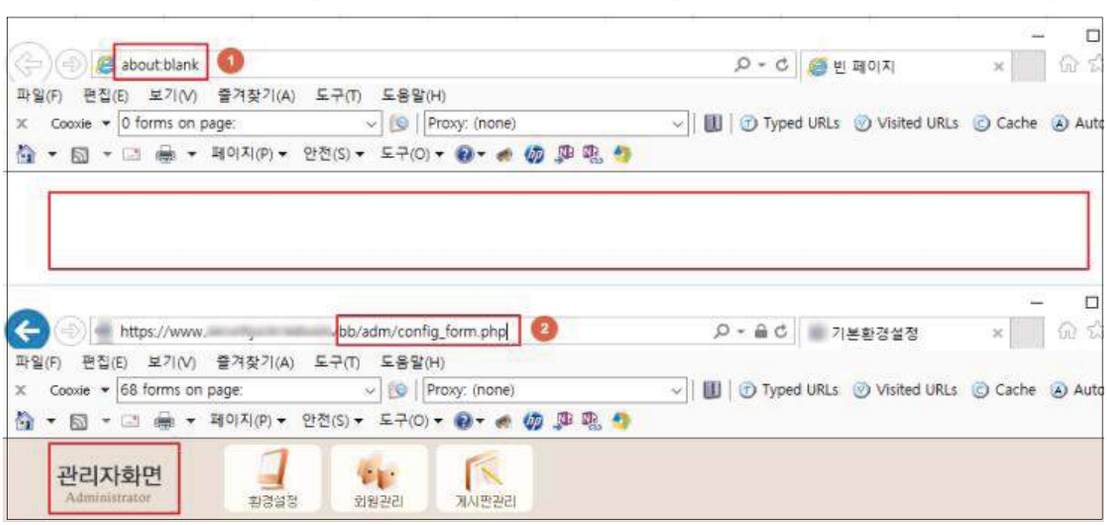
PV (상)	21. 프로세스 검증 누락
취약점 개요	
점검내용	■ 인증이 필요한 웹 사이트의 중요(관리자 페이지, 회원변경 페이지 등) 페이지에 대한 접근 제어 설정 여부 확인
점검목적	■ 인증이 필요한 모든 페이지에 대해 유효 세션임을 확인하는 프로세스 및 주요 정보 페이지에 접근 요청자의 권한 검증 로직을 적용하여, 비인가자가 하위 URL 직접 접근, 스크립트 조작 등의 방법으로 중요한 페이지에 접근 시도 하는 것을 차단하기 위함
보안위협	■ 인증이 필요한 웹 사이트의 중요(관리자 페이지, 회원변경 페이지 등) 페이지에 대한 접근 제어가 미흡할 경우 하위 URL 직접 접근, 스크립트 조작 등의 방법으로 중요한 페이지에 대한 접근이 가능함
참고	※ 소스코드 및 취약점 점검 필요
점검대상 및 판단기준	
대상	■ 소스코드
판단기준	**양호 :** 인증 후에 접근해야 하는 웹 사이트의 하위 URL을 로그인 하지 않고 직접 접근할 때 접근이 불가능 한 경우
	취약 : 웹 사이트의 하위 URL을 로그인 하지 않고 직접 접근할 때 접근이 가능한 경우
조치방법	인증이 필요한 페이지의 경우 페이지별 권한 체크 로직 구현
점검 및 조치 사례	

■ 점검방법

Step 1) 업무프로세스 파악

Step 2) 권한의 종류 및 범위 파악

Step 3) 페이지의 모든 기능을 수집하여 프로세스 상에 통제된 페이지에 접근이 가능한지 확인



PV (상)	21. 프로세스 검증 누락

■ **보안설정방법**

Step 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

Step 2) 인증이 필요한 모든 페이지에 대해 유효 세션임을 확인하는 프로세스 및 주요 정보 페이지에 접근 요청자의 권한 검증 로직을 적용함

Step 3) 유효 세션의 검증 및 페이지에 대한 접근 권한은 스크립트에 의존하지 말아야 하며, Server Side Script로 구현된 프로세스를 사용

※ **애플리케이션 별 설정 유형**

■ ASP

(예) 인증이 필요한 페이지 소스 코드

```
<% - 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)
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 … %>
```

웹(Web)

PV (상)	21. 프로세스 검증 누락

■ JSP

(예) 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	일반적인 경우 영향 없음

FU (상)	22. 파일 업로드
취약점 개요	
점검내용	■ 웹 사이트의 게시판, 자료실 등에 조작된 Server Side Script 파일 업로드 및 실행 가능 여부 점검
점검목적	■ 업로드 되는 파일의 확장자에 대한 적절성 여부를 검증하는 로직을 통해 공격자가 조작된 Server Side Script 파일 업로드 방지 및 서버 상에 저장된 경로를 유추하여 해당 Server Side Script 파일 실행을 불가능하게 하기 위함
보안위협	■ 해당 취약점 존재 시 공격자가 조작된 Server Side Script 파일을 업로드 하고 실행하여, 쉘 권한 획득 후 홈페이지를 통해 시스템 명령어를 실행하고, 웹 브라우저를 통해 그 결과 값을 보며, 시스템 관리자 권한 획득 또는 인접 서버에 대한 침입을 시도할 수 있음
참고	※ **Server Side Script:** 웹에서 사용되는 스크립트 언어 중 서버 사이드에서 실행되는 스크립트 ※ 소스코드 및 취약점 점검 필요
점검대상 및 판단기준	
대상	■ 소스코드, Web Server, 웹 방화벽
판단기준	**양호 :** 업로드 되는 파일에 대한 확장자 검증이 이루어지는 경우
	취약 : 업로드 되는 파일에 대한 확장자 검증이 이루어지지 않는 경우
조치방법	업로드 되는 파일에 대한 확장자 검증 및 실행 권한 제거
점검 및 조치 사례	

■ 점검방법

Step 1) 사용자 게시판의 파일 첨부 기능 존재 유무 확인

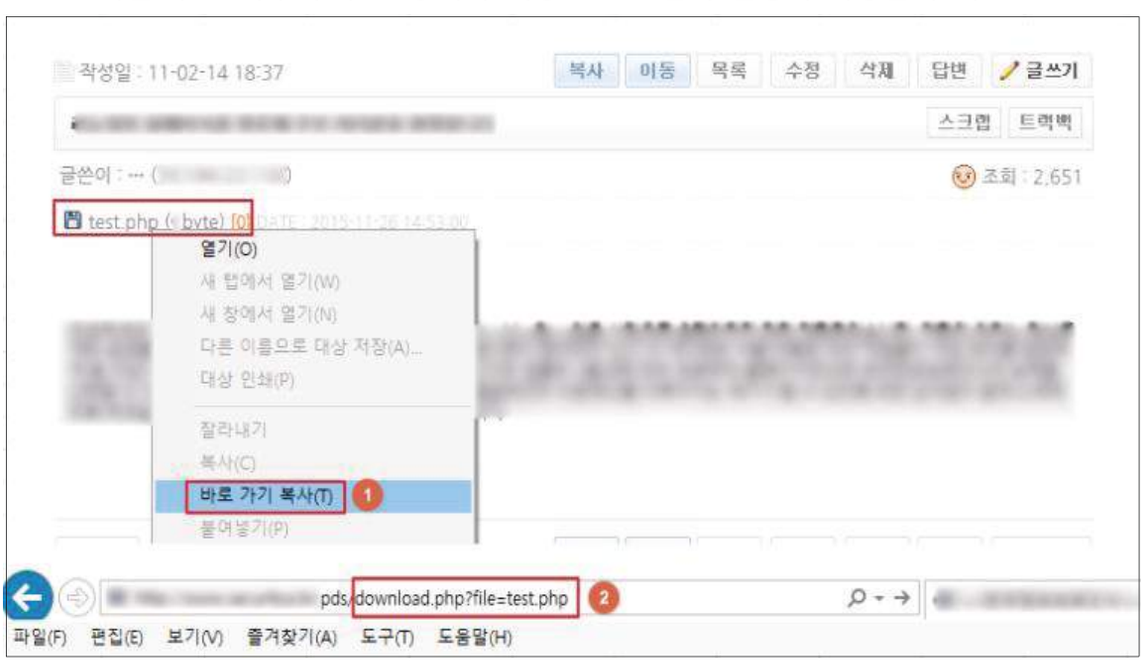
웹(Web)

FU (상)	22. 파일 업로드

Step 2) 첨부 기능이 존재하는 경우, 확장자가 jsp, php, asp, cgi 등 Server Side Script 프로그램들의 파일들이 업로드 가능한지 확인

※ 클라이언트 프로그램에서 JavaScript, VBScript 등의 스크립트로 파일첨부를 차단하는 경우 차단 기능을 수정하여 파일을 첨부함

Step 3) 홈페이지에 있는 디렉터리 정보를 이용하여 첨부한 Server Side Script 프로그램의 위치를 조사한 후 브라우저 주소 창에서 해당 프로그램의 실행이 가능한지 확인



FU (상)	22. 파일 업로드

■ **보안설정방법**

※ 사용자가 파일을 업로드 할 수 있는 모든 모듈에 적용 필요

Step 1) 화이트 리스트 방식으로 허용된 확장자만 업로드 허용

Step 2) 업로드 되는 파일을 디렉터리에 저장할 때 파일명과 확장자를 외부 사용자가 추측할 수 없는 문자열로 변경하여 저장(파일 이름은 DB에 저장)

Step 3) 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

Step 4) 파일 업로드 필드를 대상으로 특수문자 필터링하도록 웹 방화벽 룰셋 적용

※ **유형 별 상세 설정**

- 웹 애플리케이션
  - ASP

Step 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
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
IsAllowExtention = ReturnValue
End Function
.....
If Not IsAllowExtention("파일명.txt", "doc,hwp,pdf,jpg") Then
response.write "허용되지 않은 확장자 입니다."
End if
```

웹(Web)

FU (상)	22. 파일 업로드

Step 2) MIME TYPE 확인을 통한 실행 파일 업로드 차단
(예) MIME TYPE을 통한 악성 파일 업로드 차단

```
if UploadForm("UPFILE").MineType<> "image" then
Response.write "Permit only Image files"
Response.end
end if
```

Step 3) 파일 확장자에 특수문자가 포함되지 않도록 검증하는 로직 구현
Step 4) 파일 검증 시 대소문자 구분 없이 문자열 비교

■ ASP.net

Step 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

```
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;
}
```

FU (상)	22. 파일 업로드

Step 2) MIME TYPE 확인을 통한 실행 파일 업로드 차단

(예) MIME TYPE을 통한 악성 파일 업로드 차단

```
public void validateFileToUpload(FileUpload objFile)
{
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

Step 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

```
.....
publievoidupload(HttpServletRequestrequest)throwsServletException
{
MultipartHttpRequest multi = (MultipartHttpRequest) request;
String next = (String) multi.getFileNames().next();
MultipartFile file = multi.getFile(next);
If (file == null ) return;
// 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
.....
```

웹(Web)

FU (상)	22. 파일 업로드

Step 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.getFilesystemName("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;
}
}
%>
```

■ PHP

Step 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 (eregi("[^a-z0-9 \._ \-]",$_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;
.....
```

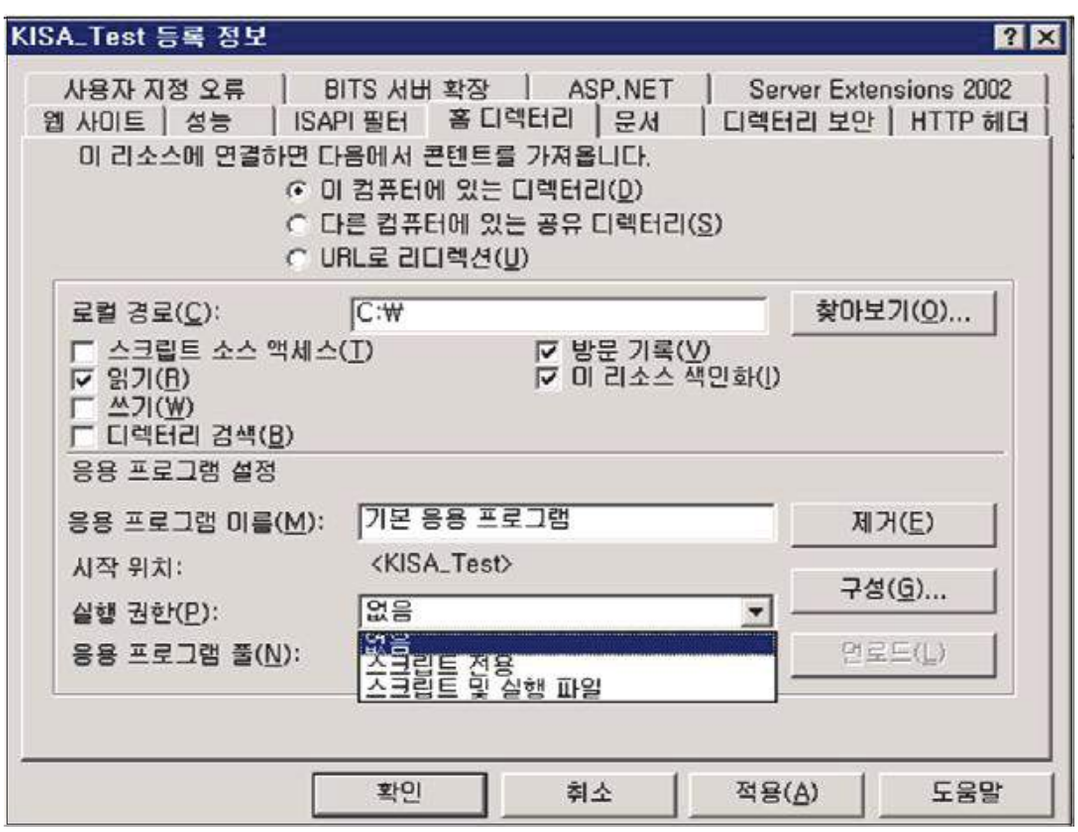
FU (상)	22. 파일 업로드

Step 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."
}
?>
```

- 웹 서버
  - IIS

설정 > 제어판 > 관리도구 > 인터넷 서비스(IIS) 관리자 선택
해당 업로드 폴더에서 우클릭 > 등록 정보 > 디렉터리> 실행 권한 "없음" 설정



웹(Web)

FU (상)	22. 파일 업로드

■ 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
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 다운로드는 거부됨

Step 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

Step 2) 시스템 보안설정 시 웹 서버 구동은 반드시 관리자 권한이 아닌 일반 사용자 권한으로 구동함

Step 3) 외부사용자가 첨부 파일을 이용하여 권한을 획득할지라도 최소한의 권한만을 사용할 수 있도록 함

Step 4) 업로드 된 디렉터리에서 실행 권한을 제거하는 방법은 임시적이기는 하지만 소스코드의 수정 없이 간단히 수행될 수 있음

● 웹 방화벽

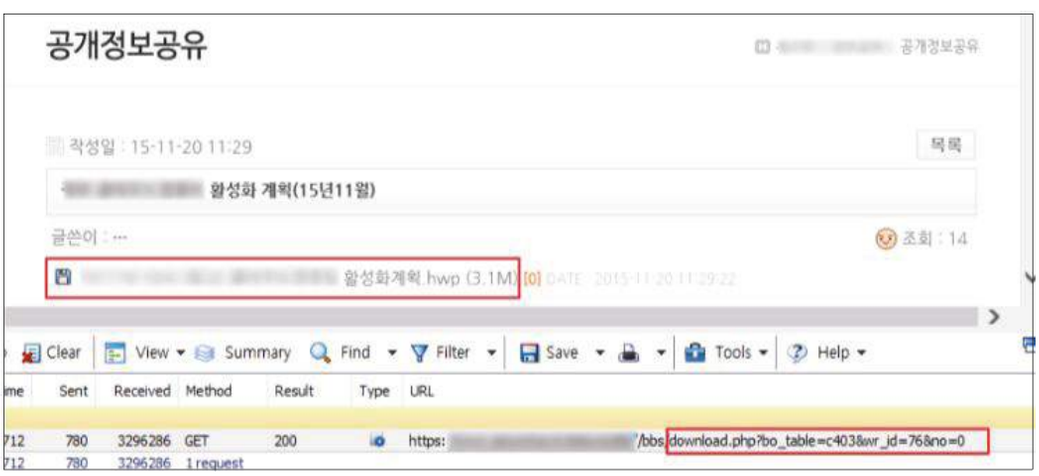
Step 1) 다운로드 인수 값을 대상으로 특수문자(../ ./ ..₩ .₩ %) 필터링 규칙 적용

조치 시 영향	일반적인 경우 영향 없음

FD (상)	23. 파일 다운로드
취약점 개요	
점검내용	■ 다운로드 파일이 저장이 허용된 디렉터리 외 다른 디렉터리의 접근이 가능한지 여부 점검
점검목적	■ 공격자가 웹 사이트의 다운로드 파일이 저장된 디렉터리 이외의 접근을 방지하여, 해당 디렉터리를 벗어나서 임의의 위치에 있는 파일을 열람하거나 다운받는 것을 불가능하게 하고자 함
보안위협	■ 해당 취약점이 존재하는 경우, 공격자가 웹 사이트의 파일 다운로드 관련 애플리케이션의 인수 값을 조작하여 웹 사이트의 중요한 파일(DB 커넥션 파일, 애플리케이션파일 등)이나 웹 사이트를 운용 중인 웹서버 루트에 있는 중요한 설정 파일(passwd, shadow 등)을 다운로드할 수 있음 ■ 웹사이트 상에서 파일을 다운받게 해주는 cgi, jsp, php, php3 등의 애플리케이션에서 입력되는 인수 값의 유효성을 검증하지 않는 경우 임의의 문자(../.. 등)나 주요 파일명의 입력을 통해 웹 서버의 홈 디렉터리를 벗어나서 임의의 위치에 있는 파일을 열람하거나 다운받는 것이 가능함
참고	※ 소스코드 및 취약점 점검 필요
점검대상 및 판단기준	
대상	■ 소스코드, 웹 방화벽
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
점검 및 조치 사례	

■ 점검방법

Step 1) 웹 사이트의 게시판(공지사항, 자유게시판), 자료실 등에서 cgi, jsp, php 등의 애플리케이션을 이용하여 파일을 다운받는 페이지가 있는지 조사

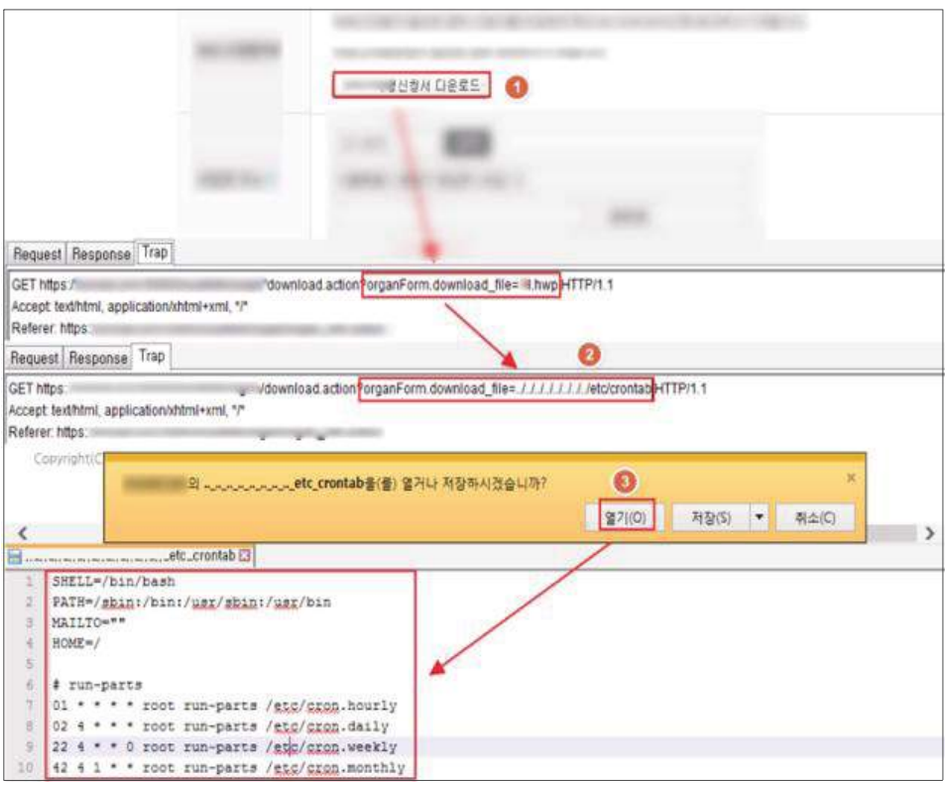


웹(Web)

FD (상)	23. 파일 다운로드

Step 2) 웹 사이트의 파일 다운로드 애플리케이션의 인수 값을 웹 서버(웹 사이트 포함) 중요한 파일(winnt₩win.ini, /etc/passwd 등)의 상대 경로(../)로 치환한 후 전송했을 때 해당 경로 파일들을 다운로드 가능한지 확인

```
../../../../../../../../../../../../etc/passwd
../../../../../../../../../../../../winnt/win.ini
../../../../../../../../../../../boot.ini
```



Step 3) "Step 2"에서변조하여 전송한 애플리케이션 인수 값을 아래의 인코딩(또는 치환, 종단문자 추가)을 적용하고 전송하여 인수 값으로 전송한 해당 경로 파일의 내용이 웹 브라우저에 표시되거나 파일로 다운로드 되는지 확인

URL 인코딩 - .(%2e), /(%2f), ₩(%5c)

16bit 유니코드 인코딩 - .(%u002e), /(%u2215), ₩(%u2216)

더블URL 인코딩 - .(%252e), /(%252f), ₩(%255c)

경로 치환 - ...///, ...₩₩, ...₩/, .../₩

종단 문자 추가- [파일명]%00.jpg, [파일명]%0a.jpg

FD (상)	23. 파일 다운로드

■ **보안설정방법**

Step 1) 파일 다운로드의 취약성은 주로 파일의 이름을 조작하는 데서 비롯되므로 다운로드 파일 이름을 데이터베이스에 저장하고 다운로드 수행 시 요청 파일 이름과 비교하여 적절한지 확인하여 사용자가 조작할 수 있는 변수를 제거함

Step 2) 다운로드 애플리케이션 소스 파일을 수정하여 파일을 다운받을 수 있는 디렉터리를 특정 디렉터리로 한정하고 이 외의 다른 디렉터리에서는 파일을 다운받을 수 없도록 ..₩ 등의 상위 경로 접근이 제한 되도록 설정해야 함

Step 3) PHP를 사용하는 경우 php.ini 에서 magic_quotes_gpc를 On으로 설정하여 .₩./ 와 같은 역 슬러시 문자 입력 시 치환되도록 설정

Step 4) 파일 다운로드의 절대 경로 설정 및 DocBase의 상위경로 또는, 타 드라이브로 설정을 변경함

Step 5) 다운로드 경로 정보를 자바스크립트나 js 소스에서 확인 가능하지 않게 제한하며, 웹 서버 서블릿 내부 또는 별도의 설정 파일에서 관리

Step 6) 다운로드를 제공하는 페이지의 유효 세션 체크 로직 필수 적용

Step 7) 다운로드 인수 값을 대상으로 특수문자 필터링하도록 웹 방화벽 룰셋 적용

문자	설명
.	Path Traversal 가능성의 확인
/	특정 Path의 접근 가능성을 확인
₩	운영환경에 따른 Path 접근 확인
%	UTF 인코딩 파라미터

[참고 : 필터링문자]

※ 애플리케이션 별 보안 설정

■ **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)
if strFile = strFPath Then
.....
```

웹(Web)

FD (상)	23. 파일 다운로드

■ 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;
```

FD (상)	23. 파일 다운로드

■ 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
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]
}
```

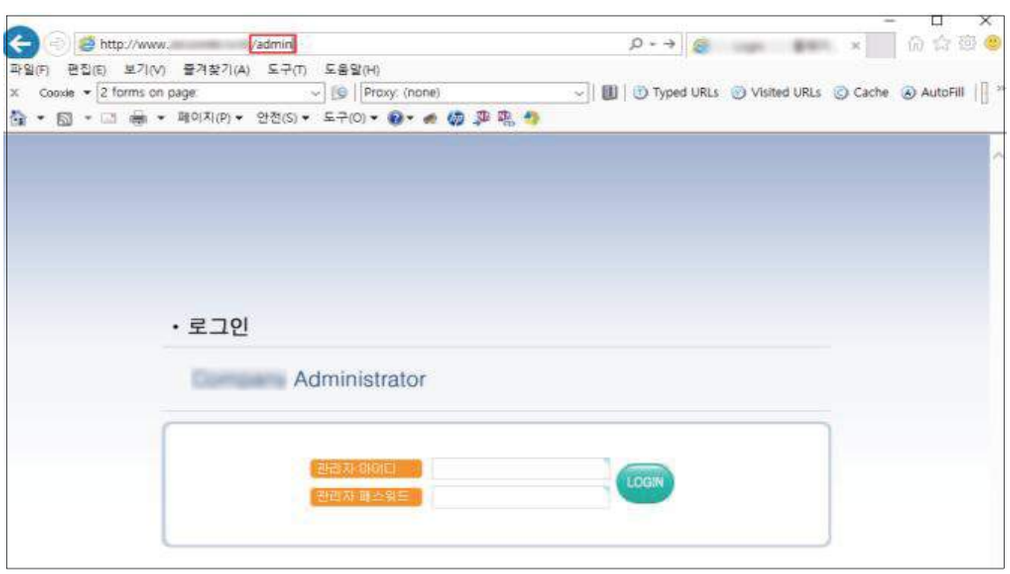
조치 시 영향	일반적으로 영향 없음

웹(Web)

AE (상)	24. 관리자 페이지 노출
취약점 개요	
점검내용	■ 유추하기 쉬운 URL로 관리자 페이지 및 메뉴 접근의 가능 여부 점검
점검목적	■ 관리자 페이지 URL이 유추하기 쉬운 이름(admin, manager 등)이나 설정 프로그램 설계 오류를 수정하여 비 인가자의 관리자 메뉴 접근을 방지하고자 함
보안위협	■ 웹 관리자의 권한이 노출될 경우 홈페이지의 변조뿐만 아니라 취약성 정도에 따라서 웹 서버의 권한까지도 노출될 수 있음
참고	※ 소스코드 및 취약점 점검 필요
점검대상 및 판단기준	
대상	■ 소스코드, Web Server, 웹 방화벽
판단기준	**양호 :** 유추하기 쉬운 URL로 관리자 페이지 접근이 불가능한 경우
	취약 : 유추하기 쉬운 URL로 관리자 페이지 접근이 가능한 경우
조치방법	유추하기 어려운 이름(포트 번호 변경 포함)으로 관리자 페이지를 변경하여 쉽게 추측하여 관리자 페이지에 접근할 수 없도록 하고 근본적인 해결을 위해 지정된 IP 만 관리자 페이지에 접근 가능하도록 제한하여야 함 단, 부득이하게 관리자 페이지를 외부에 노출을 하여야 할 경우 관리자 페이지 로그인 시 2차 인증(otp, vpn, 인증서 등)을 해야만 로그인 가능하도록 적용하는 것이 좋음
점검 및 조치 사례	

■ **점검방법**

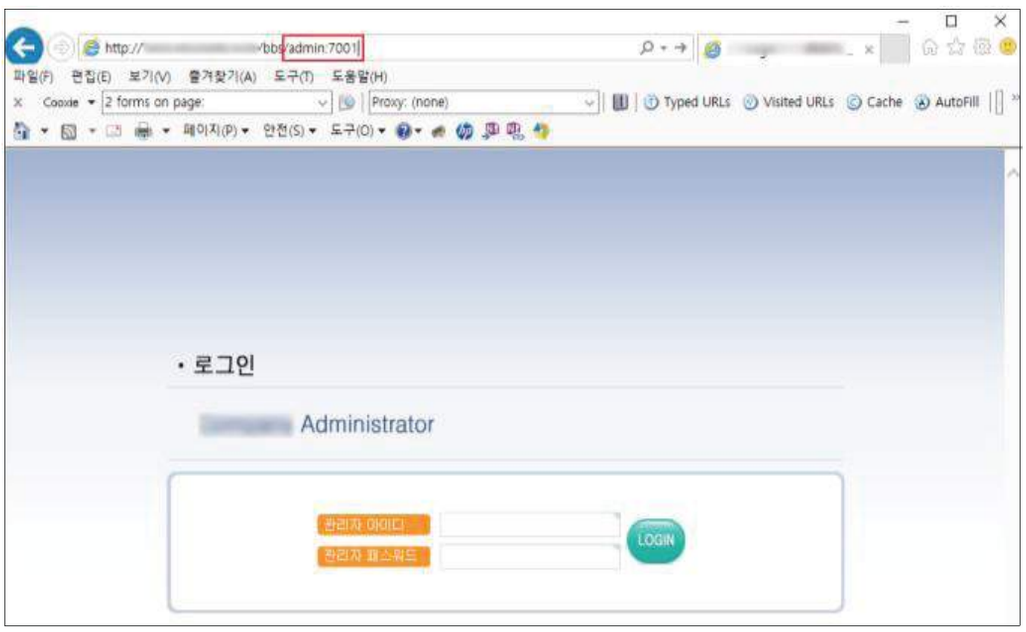
Step 1) 추측하기 쉬운(/admin, /manager, /master, /system, /administrator 등)의 명칭을 사용하는 디렉터리 및 파일 관리자 페이지 존재 여부 확인



웹(Web)

AE (상)	24. 관리자 페이지 노출

Step 2) 추측하기 쉬운(7001, 8080, 8443, 8888 등) 포트의 접속으로 관리자 페이지가 노출되는지 확인

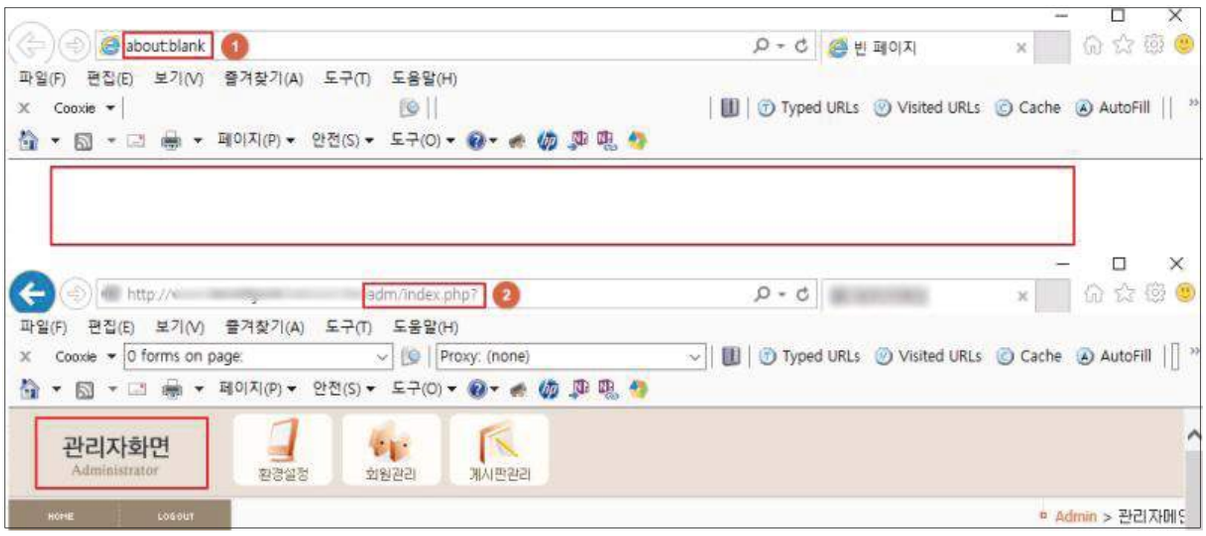


Step 3) 관리자 페이지의 로그인 창에 기본 관리자 계정(admin, administrator, manager) 및 패스워드를 입력하여 로그인 되는지 확인

Step 4) 사용자 인증 후 접근한 관리자 페이지 메인 페이지나 하위 메뉴 페이지 등 중간 페이지(/admin/main.asp, /admin/menu.html 등) URL으로 인증 과정 없이 직접 접근 가능한지 확인

웹(Web)

AE (상)	24. 관리자 페이지 노출



■ 보안설정방법

Step 1) 일반 사용자의 접근이 불필요한 관리자 로그인 페이지 주소를 유추하기 어려운 이름으로 변경하고 관리자 페이지 접근 포트도 변경함

Step 2) 관리자 페이지 주소를 직접 입력하여 접근하지 못하도록 관리자 페이지 각각에 대하여 관리자 인증을 위한 세션 관리

Step 3) 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

Step 4) 웹 방화벽을 이용하여 특정 IP만 접근 가능하도록 제한

조치 시 영향	일반적으로 영향 없음

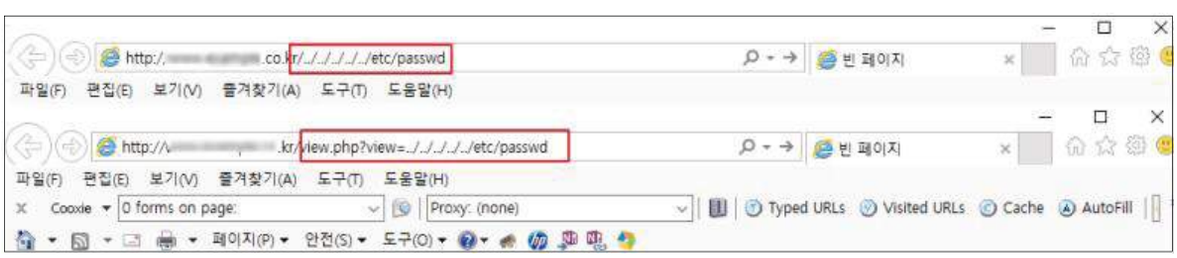
웹(Web)

PT (상)	25. 경로 추적
취약점 개요	
점검내용	■ 웹 서버와 웹 애플리케이션의 파일 또는 디렉터리의 접근 통제 여부 점검
점검목적	■ 웹 서버 또는 웹 애플리케이션의 중요한 파일과 데이터의 접근 및 실행을 방지하고자 함
보안위협	■ 웹 서버와 웹 애플리케이션의 파일 또는 디렉터리 접근이 통제되지 않아 웹 서버 또는 웹 애플리케이션의 중요한 파일과 데이터에 접근을 허용하는 취약점으로 웹 루트 디렉터리에서 외부의 파일까지 접근하여 이를 실행할 수 있음
참고	※ 소스코드 및 취약점 점검 필요
점검대상 및 판단기준	
대상	■ 소스코드, Web Server, 웹 방화벽
판단기준	**양호 :** 웹사이트 루트 디렉터리 상위 디렉터리(예. /root) 접근이 불가능한 경우
	취약 : 웹사이트 루트 디렉터리 상위 디렉터리로 접근이 가능한 경우
조치방법	웹 사이트의 최상위 디렉터리를 웹 사이트 Root 디렉터리로 제한하여 웹사이트를 통해 웹서버의 시스템 루트 디렉터리로 접근 못하게 제한
점검 및 조치 사례	

■ 점검방법

Step 1) 웹 브라우저에 표시할 페이지를 지정하는 애플리케이션 인수 값을 임의의 경로가 포함된 인수 값으로 변조 후 전송하여 인수 값으로 전송한 해당 경로의 파일 내용이 웹 브라우저에 표시되는지 확인

```
../../../../../../../../../../../../etc/passwd
../../../../../../../../../../../../winnt/win.ini
../../../../../../../../../../../../boot.ini
```



Step 2) "Step 1)"에서 변조하여 전송한 애플리케이션 인수 값을 아래의 인코딩(또는 치환, 종단문자추가)을 적용하고 전송하여 인수 값으로 전송한 해당경로 파일의 내용이 웹 브라우저에 표시되는지 확인

웹(Web)

PT (상)	25. 경로 추적

URL 인코딩 - .(%2e), /(%2f), ₩(%5c)
16bit 유니코드 인코딩 - .(%u002e), /(%u2215), ₩(%u2216)
더블URL 인코딩 - .(%252e), /(%252f), ₩(%255c)
경로 치환 - .../, ...₩₩, ...₩/, .../₩
종단 문자 추가- [파일명]%00.jpg, [파일명]%0a.jpg

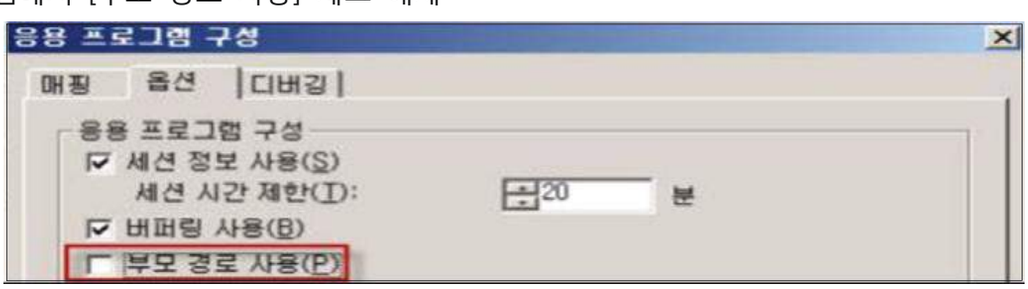
■ 보안설정방법

Step 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
예) 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



Step 2) 애플리케이션 소스 파일을 수정하여 파일 내용을 웹 브라우저에 표시 할 수 있는 디렉터리를 특정 디렉터리로 한정하고 이 외의 다른 디렉터리에서는 파일 내용을 표시할 수 없도록 ../ 등의 상위 경로 접근이 제한 되도록 설정해야 함
Step 3) PHP를 사용하는 경우 php.ini 에서 magic_quotes_gpc를 On으로 설정하여 .₩./ 와 같은 역 슬러시 문자 입력 시 치환되도록 설정
Step 4) 인수 값을 대상으로 특수문자를 필터링하도록 웹 방화벽 룰셋 적용

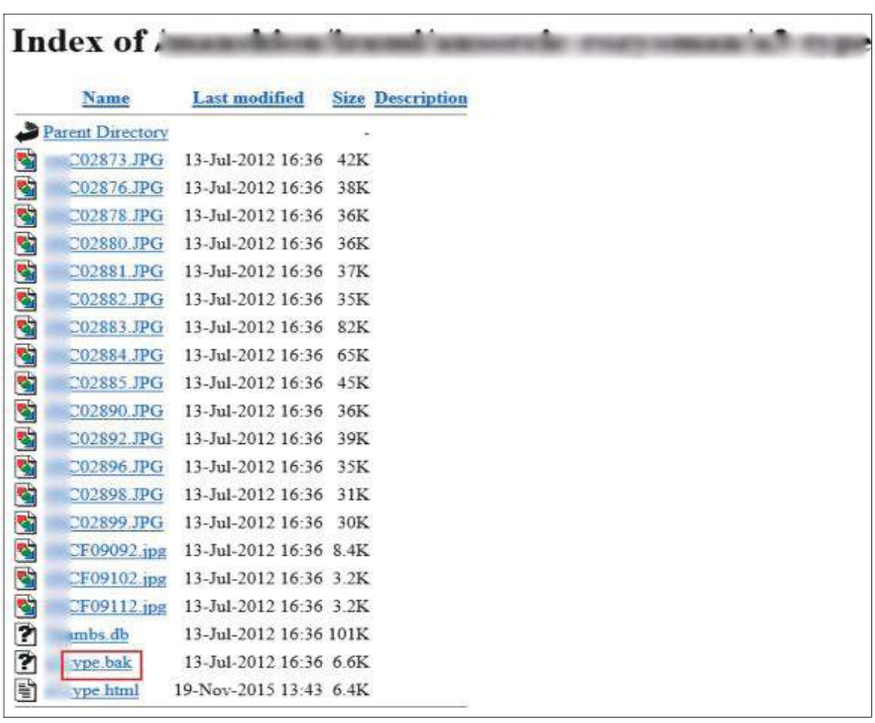
조치 시 영향	일반적으로 영향 없음

웹(Web)

PL (상)	26. 위치 공개
취약점 개요	
점검내용	■ 예측 가능한 폴더의 위치 사용 여부 및 불필요한 파일의 존재 여부 점검
점검목적	■ 공격자가 폴더의 위치를 예측하여 파일 및 정보 회득을 방지하고자 함
보안위협	■ 폴더나 파일명의 위치가 예측 가능하고 쉽게 노출되어 공격자가 이를 악용하여 대상에 대한 정보를 획득하고 민감한 데이터에 접근 가능
참고	-
점검대상 및 판단기준	
대상	■ Web Server
판단기준	**양호 :** 불필요한 파일이 존재하지 않고, 샘플 페이지가 존재하지 않을 경우
	취약 : 불필요한 파일이 존재하거나, 샘플 페이지가 존재하는 경우
조치방법	웹사이트 루트 폴더 내의 파일 중 사이트에서 쓰지 않는 불필요한 파일 삭제 및 샘플 페이지 삭제
점검 및 조치 사례	

■ 점검방법

Step 1) 웹 루트 디렉터리 내 웹 서비스에 불필요한 확장자(.bak, .backup, .org, .old, .zip, .log, .sql, .new, .txt, .tmp, .temp) 파일이 존재 하는지 확인



웹(Web)

PL (상)	26. 위치 공개

Step 2) 각종 샘플페이지(cgi-bin, manual, usage, iissamples, scripts, iisHelp, IISAdmin, _vit_bin, Printers, phpinfo.php, examples, jsp, servlets)의 디렉터리 및 파일 존재여부 확인

■ 보안설정방법

※ 삭제해야 할 파일 확장자 예시

삭제해야 할 파일 확장자			
*.bak	*.backup	*.org	*.old
*.zip	*.log	*.!	*.sql
*.new	*.txt	*.tmp	*.temp

Step 1) 웹 디렉터리를 조사하여 [표. 삭제해야 할 파일 확장자] 에 포함된 백업 파일을 모두 삭제하고, *.txt 같이 작업 중 생성된 일반 텍스트 파일이나 이미지 파일 등도 제거함

Step 2) 백업 파일은 백업 계획을 수립하여 안전한 곳에 정기적으로 백업해야 하며 웹 서버 상에는 운영에 필요한 최소한의 파일만을 생성하여야 함

Step 3) 웹 서버 설정 후 디폴트 페이지와 디폴트 디렉터리 및 Banner를 삭제하여 Banner Grab에 의한 시스템 정보 유출을 차단함

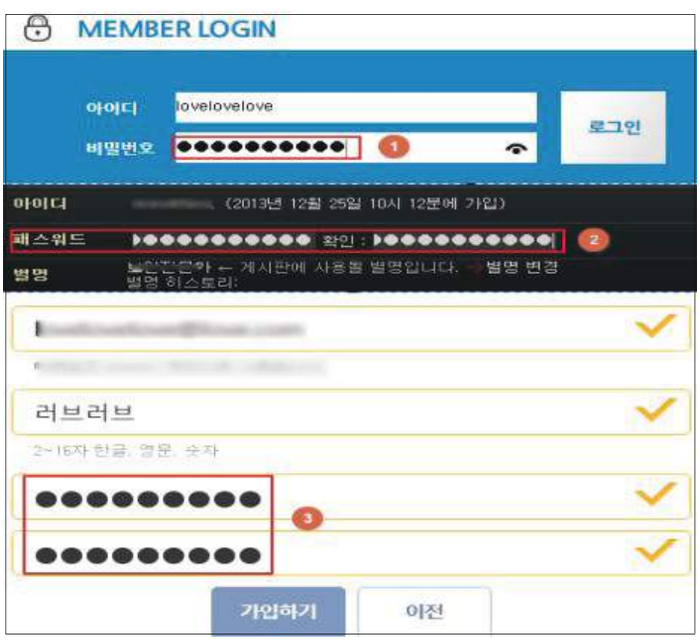
Step 4) Apache, IIS, Tomcat 등 각 웹 서버 설정 시 함께 제공되는 샘플 디렉터리 및 매뉴얼 디렉터리, 샘플 애플리케이션을 삭제하여 보안 위험을 최소화 함

조치 시 영향	일반적으로 영향 없음

SN (상)	27. 데이터 평문 전송
취약점 개요	
점검내용	■ 서버와 클라이언트 간 통신 시 데이터의 암호화 여부 점검
점검목적	■ 서버와 클라이언트 간 통신 시 데이터가 평문으로 전송되어 정보 유출의 위험을 방지하고자 함
보안위협	■ 웹상의 데이터 통신은 대부분 텍스트 기반으로 이루어지기 때문에 서버와 클라이언트 간에 암호화 프로세스를 구현하지 않으면 간단한 도청(Sniffing)을 통해 정보를 탈취 및 도용할 수 있음
참고	※ **Sniffing:** 스니퍼(sniff: 냄새를 맡다, 코를 킁킁거리다)를 이용하여 네트워크상의 데이터를 도청하는 행위 ※ 소스코드 및 취약점 점검 필요
점검대상 및 판단기준	
대상	■ 소스코드, Web Server
판단기준	**양호 :** 중요 정보 전송 구간에 암호화 통신이 적용된 경우
	취약 : 중요 정보 전송 구간에 암호화 통신이 이루어지지 않는 경우
조치방법	사이트의 중요 정보 전송 구간(로그인, 회원가입, 회원정보관리, 게시판 등) 암호화 통신(https, 애플리케이션방식) 적용
점검 및 조치 사례	

■ **점검방법**

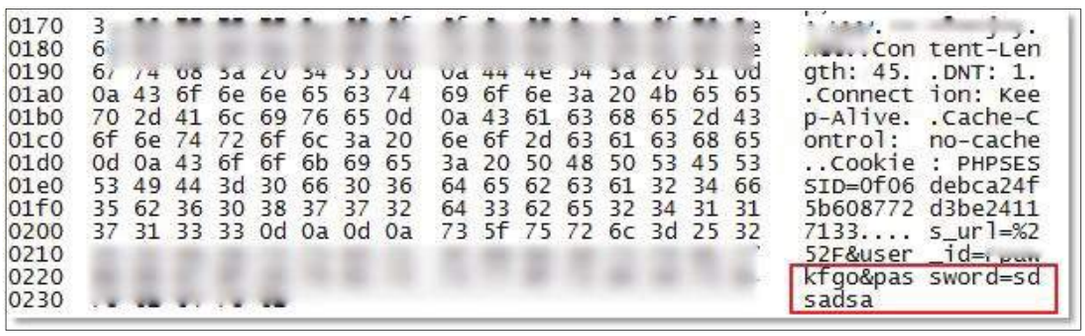
Step 1) 중요 정보(인증정보, 개인정보 등)를 송수신하는 페이지 존재여부 확인



웹(Web)

SN (상)	27. 데이터 평문 전송

Step 2) 중요 정보 송수신 페이지가 암호화 통신(https, 데이터 암호화 등)을 하는지 확인



■ 보안설정방법

Step 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

Step 2) 쿠키와 같이 클라이언트 측에서 노출되는 곳에 비밀번호, 인증인식 값, 개인정보 등의 정보를 기록하지 않음

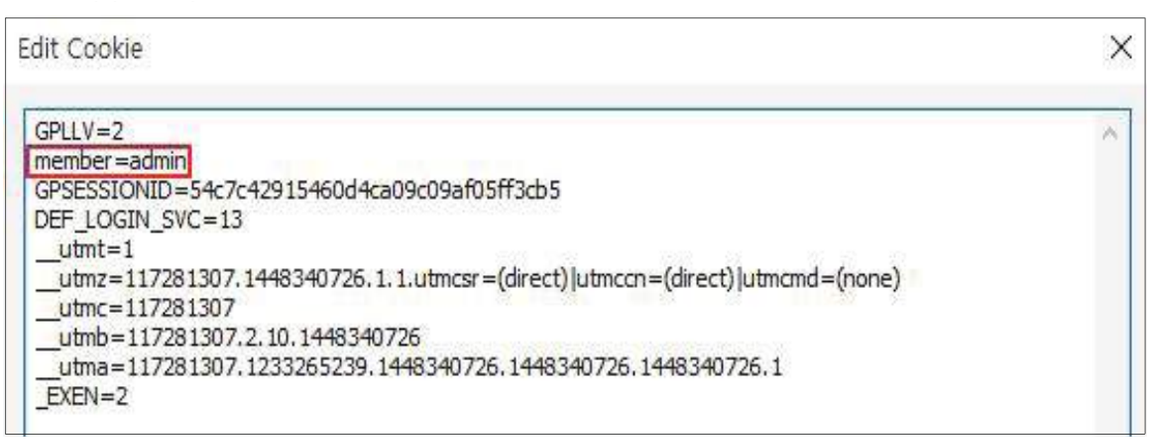
조치 시 영향	일반적으로 영향 없음

웹(Web)

CC (상)	28. 쿠키 변조
취약점 개요	
점검내용	■ 쿠키 사용 여부 및 사용하는 경우 안전한 알고리즘으로 암호화 여부 점검
점검목적	■ 쿠키를 사용하는 경우 안전한 알고리즘으로 암호화하여 공격자가 쿠키 인젝션 등과 같은 쿠키 값 변조를 통한 다른 사용자로의 위장 및 권한 변경을 방지하고자 함
보안위협	쿠키(Cookie)는 클라이언트에 전달되는 값으로 중요 정보로 구성되므로 이 정보의 조작을 통해 다른 사용자의 유효한 세션을 취득할 수 있으며, 기타 중요 정보의 유출 및 변조가 발생할 위험이 존재
참고	※ **쿠키(Cookie):** 인터넷 사용자가 어떠한 웹사이트를 방문할 경우 그 사이트가 사용하고 있는 서버에서 인터넷 사용자의 컴퓨터에 설치하는 작은 기록 정보 파일 ※ 소스코드 및 취약점 점검 필요
점검대상 및 판단기준	
대상	■ 소스코드
판단기준	**양호 :** 쿠키를 사용하지 않고 Server Side Session을 사용하고 있거나, 쿠키(또는 Session)를 사용하는 경우 안전한 알고리즘(SEED, 3DES, AES)이 적용되어 있는 경우
	취약 : 안전한 알고리즘이 적용되어 있지 않는 쿠키(Session)를 사용하거나, Client Side Session을 사용하는 경우
조치방법	쿠키 대신 Server Side Session 방식을 사용하거나, 쿠키를 통해 인증 등 중요한 기능을 구현해야 할 경우엔 안전한 알고리즘(SEED, 3DES, AES 등) 적용
점검 및 조치 사례	

■ 점검방법

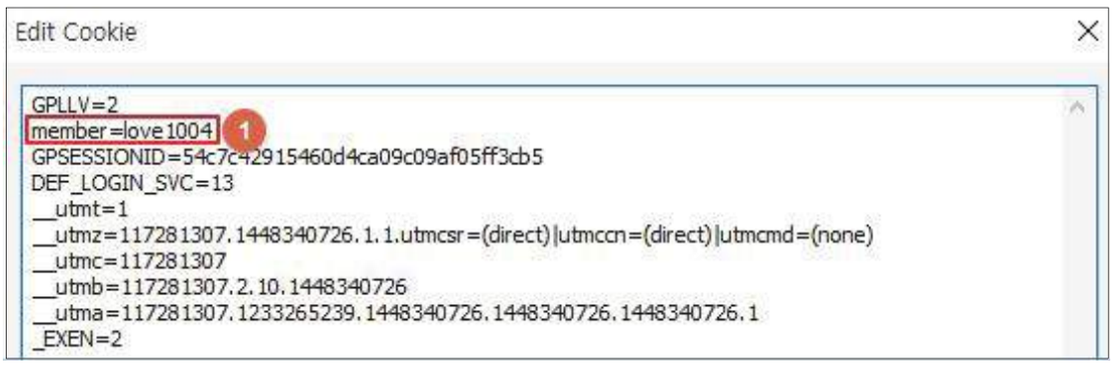
Step 1) 쿠키 내용 및 발행되는 쿠키에 중요 정보(인증을 위한 ID, 권한을 위한 구분자 등)의 노출 여부 조사

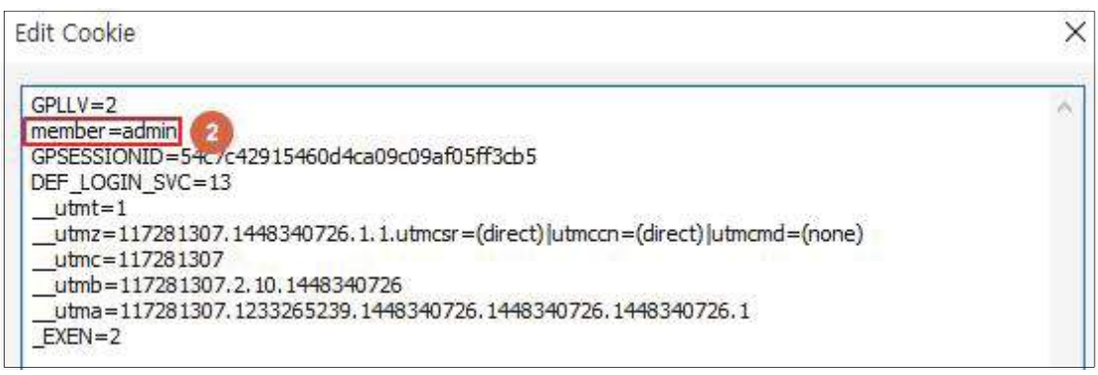


웹(Web)

CC (상)	28. 쿠키 변조

Step 2) 쿠키의 중요 정보를 변경하여 다른 사용자 및 권한으로 정상 이용이 가능한지 확인





■ 보안설정방법

Step 1) 쿠키 대신 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

Step 2) 쿠키(또는 Session)를 사용해서 중요 정보나 인증을 구현해야 할 경우 안전한 알고리즘 (SEED, 3DES, AES 등) 적용

조치 시 영향	일반적으로 영향 없음