클라우드 취약점 점검 가이드

2024. 6

KISA 한국인터넷진흥원
KOREA INTERNET & SECURITY AGENCY

클라우드 취약점 점검 가이드

2024. 6

KISA 한국인터넷진흥원
KOREA INTERNET & SECURITY AGENCY

CONTENTS

클라우드 취약점 점검 가이드

1

개요

1.1. 개요

클라우드컴퓨팅서비스 보안인증제도는「클라우드컴퓨팅 발전 및 이용자 보호에 관한 법률」제23조 제2항에 따라 클라우드컴퓨팅서비스의 정보보호 수준 향상 및 보장을 위하여 보안인증을 수행하는 제도입니다.

클라우드 보안인증은 클라우드컴퓨팅서비스의 보안인증기준 적합 유무를 평가하기 위하여, 서면/현장평가, CCE*, CVE**, 시큐어코딩, 모의침투테스트를 진행합니다. CCE 취약점 점검은 클라우드 서비스를 구성하고 있는 시스템을 대상으로 보안과 관련된 설정을 확인하며, 시스템 담당자의 서비스 이해도 및 기술 숙련도에 따라 인증평가 대응 및 보완조치가 가능하기에, 인증신청기업이 인증평가를 수행하는 과정에서 CCE 취약점 점검에 대해 어려움을 겪고 있습니다.

이에, 본 가이드를 통해 CCE 취약점 점검 및 조치 방법을 공개함으로써, 인증신청기업 및 클라우드 시스템 담당자들에게 인증평가 사전준비와 자발적 보안활동 수행을 돕기 위한 참고자료로 활용 될 수 있도록 클라우드취약점 점검 가이드를 발간하게 되었습니다.

* CCE(Common Configuration Enumeration) : 보안에 취약한 설정에 대한 점검
** CVE(Common Vulnerabilities and Exposures) : OS, Application 고유의 취약점

1.2. 목적 및 활용

본 가이드는 클라우드 보안인증(CSAP) 담당자 및 클라우드 담당자의 역량강화를 위한 CCE 취약점에 대한 39종에 대한 기술적 가이드를 제공합니다.

가이드 39종은 각 항목별 진단항목, 항목설명, 진단기준, 진단방법, 조치방법으로 구성되어 있습니다.

본 가이드를 활용할 수 있는 대상으로는 클라우드 보안 인증을 위한 담당자와 클라우드 서비스의 보안수준 향상을 위한 클라우드 정보보호 담당자 등 클라우드 서비스의 보안활동 수행 시 참고자료로 활용할 수 있습니다.

1.3. 유의 사항

본 가이드는 클라우드 인증(CSAP) 평가 시 취약점 점검(CCE) 항목별 진단 기준 및 조치 방법에 대한 이해를 돕기 위해 발간된 것으로 수록된 진단 방법은 클라우드인증(CSAP) 평가기준을 의미합니다. 또한, 해당 시스템의 기능, 버전 등 시스템 운영상황에 따라 진단방법과 판단기준은 변경될 수 있으며, 시스템의 전반적인 운영현황을 인증평가원이 확인 후에 진단항목의 양호 유무를 최종적으로 판단합니다.

클라우드 취약점 점검 가이드

2

보안가이드

2.1.

KVM

2.1. KVM

보안 설정(6개 항목) 총 1개 영역에서 6개 항목으로 구성된다.

[표 1] KVM 진단 체크리스트

구분	진단 항목
가. 보안 설정	불필요한 계정 제거
	Session Timeout 설정
	IP 접근 제한 설정
	Default Bridge 제거
	로그의 정기적 관리 및 백업
	최신 보안 패치 적용

불필요한 계정 제거

항목설명

로그인이 가능한 사용하지 않는 불필요한 계정(퇴직, 전직 등의 이유로 사용하지 않는 계정 및 장기간 미사용 계정, 테스트, default 계정)은 사용 중인 계정보다 상대적으로 관리가 잘 이루어지지 않아 공격자의 목표가 되어 계정이 탈취될 수 있으므로 시스템 계정 중 불필요한 계정 및 default 계정은 제거해야 한다. 또한 default 계정의 경우 비인가자가 접근할 수 있으므로 제거 또는 변경이 필요하다.

진단 기준

양호
불필요한 계정이 존재하지 않는 경우

취약
불필요한 계정이 존재하는 경우

진단 방법

■ 불필요한 계정 및 의심스러운 계정 존재 여부 확인

```
# grep /bin/bash /etc/passwd | cut –f1 –d:
```

■ 사용하지 않는 default 계정 확인

1) 담당자가 해당 계정의 용도를 명확하게 알지 못하는 경우
2) 테스트 계정
3) 퇴직자 계정
4) 인가되지 않은 계정

조치 방법

■ 계정 삭제

1) 계정 목록 확인 후, 불필요한 계정(인가되지 않은 계정, 퇴직자 계정, 테스트 계정 등 담당자가 실제 업무에 필요 없다고 판단하는 계정)은 삭제 또는 잠금/만료 설정

비고

※ 담당자와의 인터뷰를 통해 담당자가 업무에 필요 없다고 판단하는 계정을 파악하여 불필요한 계정 및 의심스러운 계정을 제거

Session Timeout 설정

항목설명

관리자가 실수로 로그 아웃을 하지 않고 자리를 비우는 경우 비인가자가 해당 장비에 접근하여 침해 사고를 일으킬 위험이 존재한다. 따라서 관리자가 장비에 접속하고 무의식적으로 장기간 접속 터미널을 사용하지 않을 때 자동으로 접속을 종료하거나 로그 아웃이 되도록 설정해야 한다.

진단 기준

양호

Session Timeout이 10분(600초) 이내로 설정되어 있는 경우

취약

Session Timeout이 10분(600초) 이내로 설정되어 있지 않은 경우

진단 방법

■ Session Timeout 설정 정보 확인

$ cat /etc/profile | grep TMOUT

```
root@ubuntu:/# cat /etc/profile | grep TMOUT
readonly TMOUT=600;
export TMOUT
root@ubuntu:/#
```

조치 방법

■ Sesstion Timeout 설정

1) $ vi /etc/profile

2) readonly TMOUT=600;
   export TMOUT

■ 설정 적용

1) source /etc/profile

IP 접근 제한 설정

항목설명

취약한 네트워크 서비스(Telnet, FTP)를 통한 외부 비인가자의 불법적인 시스템 침해 사고를 방지하기 위해 iptables을 이용하여 허용 호스트만 서비스를 사용할 수 있도록 IP 주소 및 포트 번호를 제한해야 한다.

진단 기준

양호

접속을 허용할 특정 호스트에 대한 IP 주소 및 포트 번호를 제한하고 있는 경우

취약

접속을 허용할 특정 호스트에 대한 IP 주소 및 포트 번호를 제한하고 있지 않은 경우

진단 방법

■ iptables 설정 확인(Ubuntu)

```
# iptables –L –n –v
```

■ iptables 설정 확인(CentOS)

```
# iptables –t –nat –L
```

■ ssh telnet 등 포트 포워딩 설정 확인

```
# iptables –L FORWARD
```

조치 방법

■ iptables 기본 정책을 DROP 설정 후, 접근 허용 IP 등록

1) iptables –P 명령어를 입력하여 기본 정책 변경(DROP)
```
# iptables –P INPUT DROP
```

2) iptables –A 명령어를 입력하여 특정 서비스에 대한 접근 허용 IP 등록
```
# iptables –A INPUT –p tcp –s [접근 허용 IP] --dport [포트 번호] –j ACCEPT
```

3) 설정 내용 저장
```
# service iptables save
```

Default Bridge 제거

항목설명

Default 네트워크 Bridge의 동일한 호스트에서 네트워크 통신 제한이 되지 않으므로 네트워크 공격에 취약하다.

진단 기준

양호

Default Bridge를 사용하고 있지 않고
별도의 네트워크 bridge를 사용하는 경우

취약

Default Bridge를 사용하고 있는 경우

진단 방법

■ 명령어를 입력하여 Default Bridge 사용 확인

1) # virsh net-list

```
root@ubuntu:/# virsh net-list
 Name      State    Autostart   Persistent
----------------------------------------------
 br0       active   yes         yes
 default   active   yes         yes
```

조치 방법

■ Default Bridge 제거 후, 별도 네트워크 브릿지 생성하여 사용

1) virsh net-destroy default
2) virsh net-undefine default
3) service libvirtd restart

비고

※ KVM 설치 시, Default Bridge 자동 생성
※ Default Bridge가 출력되지 않는다면 Default Bridge '사용 안함' 설정

로그의 정기적 관리 및 백업

항목설명

로그 정보는 침해 사고 발생 시 해킹의 흔적 및 공격기법을 확인할 수 있는 중요 자료로 이용될 수 있으며 정기적인 로그 분석을 통하여 시스템 침입 흔적과 취약점을 확인할 수 있다. 정기적인 로그 점검을 통해 안정적인 시스템 상태를 유지하고 침해 사고 시 외부 공격 여부를 파악하고 대처해야 한다.

진단 기준

양호

로그를 기록하고 있으며 로그 파일 백업이 정기적으로 이루어지고 있는 경우

취약

로그를 기록하고 있으며 로그 파일 백업이 정기적으로 이루어지고 있지 않은 경우

진단 방법

■ 인터뷰를 통해 로그 기록 정책 확인

1) 로그 기록 방식
2) 로그 파일 기록 주기
3) 로그 파일 백업 방식 및 주기

조치 방법

■ 로그 기록 및 백업

1) 로그를 기록하고 있지 않을 경우
로그 기록 및 백업 정책을 세워 로그를 주기적으로 남겨야 하며 로그 파일 또한 주기적으로 백업을 진행해야 함

비고

※ su 시도에 관한 로그: /var/log/sulog, /var/log/secure
반복적인 로그인 실패에 관한 로그: /var/log/btmp
로그인 거부 메시지에 관한 로그: /var/log/messages

최신 보안 패치 적용

항목설명

주기적인 패치 적용을 통하여 보안성 및 시스템 안전성을 확보하는 것이 시스템 운용의 중요한 요소이다. 서비스 중인 시스템의 경우 패치 적용에 따르는 문제점(현재 운용 중인 응용프로그램의 예기치 않은 중지, 패치 자체의 버그 등)과 재부팅의 어려움 등으로 많은 패치를 적용하는 것이 매우 어렵기 때문에 패치 적용시 많은 부분을 고려해야 한다.

진단 기준

양호

최신 보안 패치 적용 정책을 수립하여 주기적으로 패치를 관리하고 있는 경우

취약

최신 보안 패치 적용 정책을 수립하지 않고 주기적으로 패치 관리를 하지 않는 경우

진단 방법

■ KVM 커널 버전 확인

1) # libvirtd —version

```
root@ubuntu:/#
root@ubuntu:/# libvirtd --version
libvirtd (libvirt) 6.0.0
```

2) # virsh version

```
root@ubuntu:/# virsh version
Compiled against library: libvirt 6.0.0
Using library: libvirt 6.0.0
Using API: QEMU 6.0.0
Running hypervisor: QEMU 4.2.1
```

3) virsh version —daemon

```
root@ubuntu:/# virsh version --daemon
Compiled against library: libvirt 6.0.0
Using library: libvirt 6.0.0
Using API: QEMU 6.0.0
Running hypervisor: QEMU 4.2.1
Running against daemon: 6.0.0
```

■ QEMU 애뮬레이션 버전 확인

1) # kvm —version

조치 방법

■ 최신 보안 패치 적용

■ 인터뷰를 통해 주기적으로 최신 보안 패치 적용 여부 확인

비고

※ 최신 보안 패치 적용 시 시스템 영향도를 파악하여 충분한 테스트 후 적용 권고

2.2.

Xenserver

2.2. Xenserver

계정 관리(7개 항목), 파일 시스템(12개 항목), 네트워크 서비스 및 주요 응용 설정(5개 항목), 하이퍼바이저 정책 설정(3개 항목), 패치 및 로그 관리(6개 항목) 총 5개 영역에서 33개 항목으로 구성된다.

[표 2] Xenserver 진단 체크리스트

구분	진단 항목
가. 계정 관리	Default 계정 관리
	일반계정 root 권한 관리
	passwd 파일 권한 설정
	group 파일 권한 설정
	패스워드 사용규칙 적용
	로그인이 불필요한 계정 shell 제한
	SU(Select User) 사용 제한
나. 파일 시스템	사용자 UMASK(User Mask) 설정
	SUID(Set User-Id), SGID(Set Group-Id)
	xsconsole 파일 권한 설정
	Crontab 파일 권한 설정 및 관리
	/etc/profile 파일 권한 설정
	/etc/hosts 파일 권한 설정
	/etc/issue 파일 권한 설정
	사용자 홈 디렉터리 및 파일 관리
	주요 디렉터리 파일 권한 설정
	PATH 환경변수 설정
	/etc/service 파일 권한 설정
	부팅스크립트 파일 권한 설정
다. 네트워크 서비스 및 주요 응용설정	서비스 Banner 관리
	session timeout 설정
	root 계정의 ssh 및 sftp 접근 제한
	SSH(Secure Shell)버전 취약
	불필요한 서비스 제거
라. 하이퍼바이저 정책 설정	관리용 원격 접근 제어
	Remote Shell 접근 제어
	Guest VM 네트워크 분리
마. 패치 및 로그 관리	SU 로그 설정
	syslog 설정
	syslog 전송 포트 차단
	로깅 수준 설정
	로그 파일 권한 설정
	보안패치 적용

Default 계정 관리

항목설명

시스템에서 이용하지 않는 Default 계정 및 의심스러운 특이한 계정의 존재 여부를 검사하여 삭제한다. 대부분 시스템에서 사용하지 않는 것이 확실한 아래의 계정들과 의심스러운 계정을 삭제하여 일반적으로 로그인이 필요치 않은 시스템 계정은 로그인을 금지한다. OS나 Package 설치 시 Default로 생성되는 계정은 대부분 Default 패스워드를 사용하는 경우가 많으며 패스워드 추측 공격에 악용될 수 있다.

진단 기준

양호

OS 나 Package 설치 시 기본으로 생성되는 불필요한 계정이 존재하지 않을 경우

취약

OS 나 Package 설치 시 기본으로 생성되는 불필요한 계정이 존재할 경우

진단 방법

■ lp, uucp, nuucp 의심스러운 특이한 계정(예. guest, test) 및 미사용 계정의 존재 여부 확인

cat /etc/passwd | egrep "lp:|uucp:|nuucp:“

```
[root@46409ceded40 /]# cat /etc/passwd | egrep "lp:|uucp:|nuucp:"
lp:x:4:7:lp:/var/spool/lpd:/sbin/nologin
```

※ 퇴직, 휴직, 계약 해지자 등 해당 계정 존재 시 삭제
※ lp, uucp, nuucp, 의심스러운 특이한 계정(예. guest, test) 및 미사용 계정 삭제

조치 방법

■ 불필요한 계정 삭제

userdel lp
userdel uucp
userdel nuucp

※ 로그인 쉘을 /bin/false로 수정하는 것은 보안상 문제가 발생할 수 있으므로 삭제를 권고함
※ /nologin 설정은 양호로 처리함

일반계정 root 권한 관리

항목설명

시스템 관리자는 root 계정을 포함해, 모든 계정의 의심되는 디렉터리 및 파일을 정기적으로 조사하여 삭제하며, 주기적으로 불필요한 사용자 계정을 조사하여 제거하는 것이 보안상 필요하다.

진단 기준

양호

root 및 시스템 계정(daemon, bin, adm, uucp, nuucp, lp, hpdb 등)을 제외하고 UID가 0이 존재하지 않는 경우

취약

root 및 시스템 계정(daemon, bin, adm, uucp, nuucp, lp, hpdb 등)을 제외하고 UID가 0이 존재하는 경우

진단 방법

■ /etc/passwd 파일의 필드 3번째 값 확인(UID가 0인지 확인)

cat /etc/passwd

(예시) test:x:0:0:test:/home/test:/bin/bash

※ UID가 0일 경우 취약함

조치 방법

■ root 및 시스템 계정 외 UID가 0인 계정의 UID 값 변경

(예시) test 계정의 UID 를 2002로 바꿀 경우

usermod -u 2002 test

passwd 파일 권한 설정

항목설명

"/etc/passwd" 파일의 접근 권한을 제한하고 있는지 점검하며, 파일 설정의 문제점이나 파일 permission 등을 진단하여 관리자의 실수나, 오류로 발생할 수 있는 침해사고(일반 사용자 권한 /root 권한 획득)의 위험성을 진단한다.

진단 기준

양호

패스워드 파일의 소유자가 root이고, 권한이 644(rw-r--r--)인 경우

취약

패스워드 파일의 소유자가 root가 아니거나 타 사용자에게 쓰기 권한 및 접근 권한이 존재할 경우

진단 방법

■ /etc/passwd 파일의 접근권한 확인

ls –al /etc/passwd

```
[root@46409ceded40 /]# ls -al /etc/passwd
-rw-r--r-- 1 root root 737 Sep  6  2018 /etc/passwd
```

조치 방법

■ /etc/passwd 파일의 권한 변경

chmod 644 /etc/passwd
chown root /etc/passwd

group 파일 권한 설정

항목설명

Group 파일을 일반 사용자가 접근하여 변조하게 되면 인가되지 않은 사용자가 root 그룹으로 등록되어 root 권한 획득이 가능하다. Group 파일을 일반 사용자들이 수정할 수 없도록 제한하고 있는지 점검하여 타 사용자의 쓰기 권한을 제한해야 한다.

진단 기준

양호

/etc/group 파일의 소유자가 root(또는 bin)이고 권한이 644(rw-r--r--)인 경우

취약

/etc/group 파일의 소유자가 root(또는 bin)가 아니거나 타 사용자에게 쓰기 권한 및 접근 권한이 존재할 경우

진단 방법

■ /etc/group 파일의 접근 권한 확인

ls –al /etc/group

```
[root@46409ceded40 /]# ls -al /etc/group
-rw-r--r-- 1 root root 433 Sep  6  2018 /etc/group
```

조치 방법

■ /etc/group 파일의 권한 변경

chmod 644 /etc/group
chown root /etc/group

패스워드 사용규칙 적용

항목설명

패스워드 추측 공격을 피하고자 패스워드 최소길이가 설정되어 있는지 점검한다. 패스워드 최소길이가 설정되어 있지 않거나 짧게 설정된 경우, 악의적인 사용자가 패스워드를 쉽게 유추할 수 있다.

진단 기준

양호

패스워드 정책에 따른 설정이 적용된 경우

취약

패스워드 정책에 따라 설정이 적용되어 있지 않은 경우

진단 방법

■ 패스워드 최소길이, 최소 사용 기간, 최대 사용 기간 설정 확인 (단위: 일)

```
# cat /etc/login.defs | grep –i "PASS_MAX_DAYS"
# cat /etc/login.defs | grep –i "PASS_MIN_DAYS"
# cat /etc/login.defs | grep –i "PASS_MIN_LEN“
```

```
[root@46409ceded40 /]# cat /etc/login.defs | grep -i "PASS_MAX_DAYS"
#       PASS_MAX_DAYS   Maximum number of days a password may be used.
PASS_MAX_DAYS   99999
[root@46409ceded40 /]# cat /etc/login.defs | grep -i "PASS_MIN_DAYS"
#       PASS_MIN_DAYS   Minimum number of days allowed between password changes.
PASS_MIN_DAYS   0
[root@46409ceded40 /]# cat /etc/login.defs | grep -i "PASS_MIN_LEN"
#       PASS_MIN_LEN    Minimum acceptable password length.
PASS_MIN_LEN    5
```

조치 방법

■ /etc/login.defs에서 아래와 같은 설정으로 변경 (단위: 일)

```
#vi /etc/login.defs
PASS_MIN_LEN 8
PASS_MAX_DAYS 70
PASS_MIN_DAYS 7
```

로그인이 불필요한 계정 shell 제한

항목설명

로그인이 필요하지 않은 사용자들에게는 쉘을 제한함으로 비인가적인 시스템 사용을 방지하여 침해의 가능성을 줄일 수 있다.

진단 기준

양호

시스템 계정 중 로그인이 불필요한 계정에 대해 shell이 제한된 경우

취약

시스템 계정 중 로그인이 불필요한 계정에 대해 shell이 제한되지 않은 경우

진단 방법

■ /etc/passwd 파일의 계정별 shell 확인

cat /etc/passwd

(예시) nobody:x:65534:65534:nobody:/nonexistent:/bin/sh

※ 실행 쉘이 불필요한 계정 및 로그인이 필요하지 않은 계정에 nologin shell 부여 (daemon, bin, sys, listen, adm, nobody, nobody4, noaccess, diag, operator, games, gopher 등 일반적으로 UID 100 이하 60000 이상의 시스템 계정들)

조치 방법

■ 로그인이 필요 없는 계정의 shell 설정 변경

#vi /etc/passwd를 실행하여 아래와 같은 설정으로 변경 (단위: 주)

예) daemon 계정이 로그인하지 못하도록 설정

vi /etc/passwd
daemon:x:1:1::/:/sbin/ksh (수정 전)
daemon:x:1:1::/:/bin/false (수정 후)

SU(Select User) 사용 제한

항목설명

권한이 없는 일반 사용자가 su 명령을 사용한 Password Guessing을 통해 root 권한을 획득할 수 있다.

진단 기준

양호

/etc/pam.d/su 파일에 auth required pam_wheel.so use_uid 라인에 주석(#)이 없고 /etc/group 파일의 wheel 그룹에 계정이 제한되어 있는 경우

취약

/etc/pam.d/su 파일에 auth required pam_wheel.so use_uid 라인에 주석(#)이 있거나 /etc/group 파일의 wheel 그룹에 계정이 제한되어 있지 않은 경우

진단 방법

■ /etc/pam.d/su에서 주석 여부 확인

cat /etc/pam.d/su | grep –v 'trust' | grep 'pam_wheel.so' | grep 'use_uid'

```
[root@46409ceded40 /]# cat /etc/pam.d/su | grep -v 'trust' | grep 'pam_wheel.so'
 | grep 'use_uid'
#auth            required        pam_wheel.so use_uid
```

조치 방법

■ SU 사용 제한 설정

1. /etc/pam.d/su 파일을 아래와 같이 설정.
   auth sufficient /lib/security/pam_rootok.so
   auth required /lib/security/pam_wheel.so use_uid

```
[root@46409ceded40 /]# cat /etc/pam.d/su | grep -v 'trust' | grep 'pam_wheel.so'
 | grep 'use_uid'
auth            required        pam_wheel.so use_uid
```

2. wheel group 생성
   # groupadd wheel
3. /etc/group 파일에서 wheel 그룹에 su 명령어를 사용할 사용자를 추가
   # usermod –G wheel username

사용자 UMASK(User Mask) 설정

항목설명

시스템 내에서 user가 새로 생성하는 파일의 접근 권한은 UMASK에 따라 달라진다. 현재의 user에게 설정된 UMASK를 조회하려면, 명령 프롬프트에서 “umask”를 수행하면 되고, UMASK 값이 “022”를 권장한다. UMASK 값 “022”는 “rw-r—r--” 접근 권한으로 파일이 생성된다.

진단 기준

양호

현재 시스템의 UMASK가 022 또는 027로 설정되어 있으며, Start Profile에 UMASK가 설정되어 있는 경우

취약

현재 시스템의 UMASK가 설정되어 있지 않거나 022 또는 027이 아닌 경우

진단 방법

■ UMASK 확인

1. /etc/pam.d/su 파일을 아래와 같이 설정.
   # umask
   # cat /etc/profile | grep –i "umask“

```
[root@46409ceded40 /]# umask
0022
[root@46409ceded40 /]# cat /etc/profile | grep "umask"
# By default, we want umask to get set. This sets it for login shell
    umask 002
    umask 022
```

조치 방법

■ UMASK 변경

1. /etc/pam.d/su 파일을 아래와 같이 설정.
   # umask 022
   # vi /etc/profile
   umask 022 행 추가

※ 계정의 Start Profile(/etc/profile, /etc/default/login, .cshrc, .kshrc, .bashrc, .login, .profile 등)에 명령을 추가하면, 사용자가 로그인 후에도 변경된 UMASK 값을 적용받음

SUID(Set User-Id), SGID(Set Group-Id)

항목설명

SUID(Set User-ID)와 SGID(Set Group-ID)가 설정된 파일의 경우, BufferOverflow 공격과 Local 공격에 많이 사용되는 파일이다. 보안에 취약한 root 소유의 setuid 파일들의 경우 필요한 파일을 제외하고 setuid, setgid 속성을 제거하며, 해당 파일의 주기적인 진단 및 보안 관리가 필요하다.

진단 기준

양호

불필요한 SUID, SGID가 설정되어 있지 않은 경우

취약

불필요한 SUID, SGID가 설정되어 있는 경우

진단 방법

■ SUID, SGID 검색

```
# find / -user root -type f \( -perm -4000 -o -perm -2000 \) -exec ls -lg {} \;
```

■ 불필요한 Setuid, Setgid 목록

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

조치 방법

■ 불필요한 SUID, SGID 제거

```
# chmod -s [파일명]
```

xsconsole 파일 권한 설정

항목설명

xsconsole 파일에 대한 접근 권한을 제한하고 있는지 점검한다.
xsconsole은 XenServer의 텍스트 모드 콘솔 인터페이스를 제공하며, xsconsole의 접근 권한 설정이 잘못 설정되어 있을 경우 비 인가된 공격자가 설정을 변경할 수 있다.

진단 기준

양호

/usr/bin/xsconsole 파일의 소유자가 root이고, 타 사용자의 쓰기 권한이 없는 경우

취약

/usr/bin/xsconsole 파일의 소유자가 root가 아니거나 타 사용자의 쓰기 권한이 있는 경우

진단 방법

■ /usr/bin/xsconsole 파일의 접근권한 확인

ls –al /usr/bin/xsconsole

```
[root@localhost bin]# ls  -alL /usr/bin/xsconsole
-rwxr-xr-x 1 root root 116 Apr 10 01:41 /usr/bin/xsconsole
```

조치 방법

■ xsconsole 파일 소유자를 root로 변경 및 타사용자 권한 제거

1. xsconsole 파일 소유자를 root로 변경
   # chown root /usr/bin/xsconsole
2. xsconsole 파일에 타사용자 권한을 제거
   # chmod o-w /usr/bin/xsconsole

※ 해당 파일에 링크가 설정되어 있다면 링크된 원본 파일 소유자를 변경함

Crontab 파일 권한 설정 및 관리

항목설명

**일반 사용자가 Cron 관련 파일에 악의적으로 접근 권한을 제한하고 있는지 점검한다. Cron은 작업 스케줄링 기능을 제공하는 프로그램이며, 특정 시간에 특정 작업을 자동으로 수행하도록 하는 프로그램이다.
Cron 관련 파일의 접근 권한 설정이 잘못되어 있을 경우, 비인가자가 다양한 방법으로 사용자 환경을 변경하여 침해사고를 일으킬 수 있다.**

진단 기준

양호

cron 파일 소유자가 root이며, 타사용자의 쓰기 권한이 없고, 예약 실행 파일의 소유자가 root이고, 실행 파일이 744로 설정되어 있는 경우

취약

etcd SSL/cron 파일 소유자가 root가 아니거나, 타사용자의 쓰기 권한이 존재하는 경우 또는 예약 실행 파일의 소유자가 root가 아니거나, 실행 파일이 744로 설정되어 있지 않은 경우, TLS 설정이 적용되지 않은 경우

진단 방법

■ Crontab 관련 파일의 소유자 및 권한 확인

(예시) # ls -al/etc/crontab
아래 파일의 소유자 및 권한 확인필요
/etc/crontab, /etc/cron.daily/*, /etc/cron.hourly/*, /etc/cron.monthly/*, /etc/cron.weekly/*, /var/spool/cron/*

■ Crontab 예약 실행 파일 소유자 및 권한 확인

(예시) # crontab - l
1 15 * * /backup/OS_backup.sh
30 * * * * /opt/sfm/vacuum
ls -al /backup/OS_backup.sh
ls -al /opt/sfm/vacuum

조치 방법

■ Crontab 관련 파일에 타사용자 쓰기 권한 제거

chmod o-w /etc/crontab
chmod o-w /etc/cron.daily/*
chmod o-w /etc/cron.hourly/*
chmod o-w /etc/cron.monthly/*
chmod o-w /etc/cron.weekly/*
chmod o-w /var/spool/cron/*

■ Crontab 예약 파일 소유자

ls -al [file]
chmod 744 [file]

/etc/profile 파일 권한 설정

항목설명

사용자 설정 파일인 /etc/profile 파일에 대한 접근 권한을 제한하고 있는지 점검한다.
/etc/profile 파일은 로그인하는 모든 사용자들의 기본 사용환경 설정을 위한 로그인 스크립트이다. /etc/profile의 접근 권한 설정이 잘못되어 있을 경우 비인가자가 다양한 방법으로 사용자 환경을 변경하여 침해사고를 일으킬 수 있다.

진단 기준

양호

/etc/profile의 소유자가 root(또는 bin)이고, 타 사용자의 쓰기 권한이 없는 경우

취약

/etc/profile의 소유자가 root(또는 bin)가 아니거나, 타 사용자의 쓰기 권한이 존재하는 경우

진단 방법

■ /etc/profile 파일의 소유자 및 권한 확인

ls -al /etc/profile

```
[root@46409ceded40 ~]# ls -al /etc/profile
-rw-r--r-- 1 root root 1750 Jun  7  2013 /etc/profile
```

조치 방법

■ /etc/profile 파일 소유자 변경 및 타사용자 쓰기 권한 제거

1. /etc/profile 파일 소유자 변경
   # chown root /etc/profile
2. /etc/profile 타사용자 쓰기 권한 제거
   # chmod o-w /etc/profile

/etc/hosts 파일 권한 설정

항목설명

호스트네임 등록 파일인 /etc/hosts 파일에 대한 접근 권한을 제한하고 있는지 점검한다.
/etc/hosts 파일은 IP address와 Host name을 매핑하는 데 사용되는 파일이며, 이 파일의 접근 권한 설정이 잘못 설정되어 있을 경우 악의적인 시스템을 신뢰하게 된다.

진단 기준

양호

/etc/hosts 파일의 소유자가 root(또는 bin)이고, 권한에 타 사용자의 쓰기 권한이 없는 경우

취약

/etc/hosts 파일의 소유자가 root(또는 bin)가 아니거나 권한에 타 사용자의 쓰기 권한이 있는 경우

진단 방법

■ /etc/hosts 파일의 소유자 및 권한 확인

ls –al /etc/hosts

```
[root@46409ceded40 ~]# ls -al /etc/hosts
-rw-r--r-- 1 root root 174 Dec  6 06:54 /etc/hosts
```

조치 방법

■ /etc/hosts 파일 소유자 변경 및 타사용자 쓰기 권한 제거

1. /etc/hosts 파일 소유자 변경
   # chown root /etc/hosts
2. /etc/hosts 타사용자 쓰기 권한 제거
   # chmod o-w /etc/hosts

/etc/issue 파일 권한 설정

항목설명

터미널 설정과 관련된 /etc/issue 파일에 대한 접근 권한을 제한하고 있는지 점검한다.

진단 기준

양호

/etc/issue 파일의 소유자가 root (또는 bin)이고 권한에 타 사용자의 쓰기 권한이 없는 경우

취약

/etc/issue 파일의 소유자가 root (또는 bin)가 아니거나 권한에 타 사용자의 쓰기 권한이 있는 경우

진단 방법

■ /etc/issue 파일의 소유자 및 권한 확인

ls -al /etc/issue

```
[root@46409ceded40 ~]# ls -al /etc/issue
-rw-r--r-- 1 root root 23 Dec  9  2015 /etc/issue
```

조치 방법

■ /etc/issue 파일 소유자 변경 및 타사용자 쓰기 권한 제거

1. /etc/issue 파일 소유자 변경
   # chown root /etc/issue
2. /etc/issue 타사용자 쓰기 권한 제거
   # chmod o-w /etc/issue

사용자 홈 디렉터리 및 파일 관리

항목설명

각각의 사용자의 홈 디렉터리 내의 파일을 인가되지 않은 사용자가 접근하여 설정 파일 및 파일을 변조하게 되면 정상적인 사용자의 서비스가 제한된다. 따라서 해당 홈 디렉터리의 계정 외의 일반 사용자들이 해당 홈 디렉터리를 수정할 수 없도록 제한하고 있는지 점검한다.

진단 기준

양호

User 별 홈 디렉터리의 타 사용자의 쓰기 권한이 없는 경우

취약

User 별 홈 디렉터리의 타 사용자의 쓰기 권한이 있는 경우

진단 방법

■ 사용자 홈 디렉터리 및 파일 권한 확인

1. /etc/passwd 파일에서 사용자 홈 디렉터리 확인
2. cd [사용자 홈 디렉터리]
3. ls -al [사용자 홈 디렉터리]

```
[root@46409ceded40 ~]# ls -ldb /root/.cshrc /root/.bash_profile /root/.bashrc
-rw-r--r-- 1 root root 176 Dec 29  2013 /root/.bash_profile
-rw-r--r-- 1 root root 176 Dec 29  2013 /root/.bashrc
-rw-r--r-- 1 root root 100 Dec 29  2013 /root/.cshrc
```

※ 사용자 홈 디렉터리 안의 아래 파일 확인
.profile", ".kshrc", ".cshrc", ".bashrc", ".bash_profile", ".login", ".exrc", ".netrc", ".dtprofile", ".Xdefaults"

조치 방법

■ 사용자 홈 디렉터리 안의 설정 파일에 타사용자 쓰기 권한 제거

chmod o-w [홈 디렉터리 경로] [파일명]

주요 디렉터리 파일 권한 설정

항목설명

주요 디렉터리의 파일 권한이 적절히 설정되어 있는지 점검한다. 주요 디렉터리 접근 권한 설정이 잘못되어 있을 경우 비인가자가 다양한 방법으로 사용자 환경을 변경하여 침해사고를 일으킬 수 있다.

진단 기준

양호

디렉터리의 권한을 root(또는 bin) 소유의 타 사용자의 쓰기 권한이 없는 경우

취약

디렉터리의 권한을 root(또는 bin) 소유의 타 사용자의 쓰기 권한이 있는 경우

진단 방법

■ 주요 디렉터리의 권한

ls -ldb /usr/bin/xsconsole /usr/lib/xsconsole /opt /sbin /etc/ /bin /usr/bin/ /usr/sbin

```
[root@46409ceded40 ~]# ls -ldb /opt /sbin /etc/ /bin /usr/bin/ /usr/sbin
lrwxrwxrwx 1 root root    7 Dec 15  2015 /bin -> usr/bin
drwxr-xr-x 1 root root 4096 Dec  6 06:54 /etc/
drwxr-xr-x 2 root root 4096 Aug 12  2015 /opt
lrwxrwxrwx 1 root root    8 Dec 15  2015 /sbin -> usr/sbin
dr-xr-xr-x 1 root root 4096 Sep  6  2018 /usr/bin/
dr-xr-xr-x 1 root root 4096 Sep  6  2018 /usr/sbin
```

〈주요 디렉터리 목록〉

주요 디렉터리 목록		
/usr/bin/xsconsole	/opt	/sbin,
/usr/lib/xsconsole	/etc	/bin
/usr/sbin	/usr/bin	

조치 방법

■ 디렉터리 소유자 변경 및 타 사용자 쓰기 권한 제거

1. 디렉터리 소유자 변경
   # chown root [디렉터리명]
2. 디렉터리 권한 변경
   # chmod o-w [디렉터리명]

PATH 환경변수 설정

항목설명

root 계정의 PATH 환경변수에 ”.“ (현재 디렉터리 지칭)가 포함되어 있으면, root 계정의 인가자로 인해 비의도적으로 현재 디렉터리에 있는 명령어가 실행될 수 있다. 즉 ”.“이 /usr/bin이나 /bin, /sbin 등 명령어들이 있는 디렉터리보다 우선하여 있을 경우, root 계정의 인가자가 어떠한 명령을 실행했을 때, 비인가자가 불법적으로 위치시킨 파일을 비의도적으로 실행하여, 예기치 않은 결과를 가져올 수 있다.
또한 ”.“ 뿐만 아니라 비인가자가 불법적으로 생성한 디렉터리가 먼저 선택되어 예기치 않은 결과를 가져올 수 있다.

진단 기준

양호

현재 위치를 의미하는 ”.“이 없거나, PATH 맨 뒤에 존재하는 경우

취약

현재 위치를 의미하는 ”.“이 앞이나 중간에 존재하는 경우

진단 방법

■ PATH 설정 확인

echo $PATH

```
[root@46409ceded40 ~]# echo $PATH
/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin
```

조치 방법

■ root 계정의 환경변수 설정파일(.profile, .cshrc등)과 ”/etc/profile“ 등에서 PATH 환경변수에 포함된 현재 디렉터리를 나타내는 ”.“을 제거

/etc/service 파일 권한 설정

항목설명

Service 파일에 관리자가 아닌 사용자에 접근 및 변경 권한이 있는 경우, 악의적인 사용자가 정상적인 서비스를 중단시키거나, 허가되지 않은 서비스 실행하여 침해사고를 발생 시킬 수 있다.

진단 기준

양호

/etc/service 파일의 소유자가 root (또는 bin)이고 권한에 타 사용자의 쓰기 권한이 없는 경우

취약

/etc/service 파일의 소유자가 root (또는 bin)가 아니거나 권한에 타 사용자의 쓰기 권한이 있는 경우

진단 방법

■ /etc/service 권한 확인

ls –alL /etc/services

```
[root@46409ceded40 ~]# ls -alL /etc/services
-rw-r--r-- 1 root root 670293 Jun  7  2013 /etc/services
```

조치 방법

■ /etc/services 소유자 변경 및 타사용자 쓰기 권한 제거

1. /etc/service 파일 소유자 변경
   # chown root /etc/service
2. /etc/service 파일 타사용자 쓰기 권한 제거
   # chmod o-w /etc/service

부팅스크립트 파일 권한 설정

항목설명

OS 상에서 사용하는 기타 중요 파일에 대하여 접근 권한을 제한하고 있는지 점검한다. 시스템 운영상 중요한 파일들의 접근 권한은 반드시 필요한 사용자만 접근할 수 있도록 해야 한다.

진단 기준

양호

기타 중요 파일의 소유자가 root (또는 bin)이고 권한에 타 사용자의 쓰기 권한이 없는 경우

취약

기타 중요 파일의 소유자가 root (또는 bin)가 아니거나 권한에 타 사용자의 쓰기 권한이 있는 경우

진단 방법

■ 기타 중요 파일 권한 확인

```
# ls -alL /opt/*/*
```

〈기타 중요 파일 목록〉

기타 중요 파일 목록		
/opt/*/*	/etc/rc*.d	/etc/inittab
/etc/syslog.conf	/etc/snmp/snmpd.conf	/etc/crontab
/etc/cron daily/*	/etc/cron hourly/*	/etc/cron monthly/*
/etc/cron weekly/*	/etc/spool/cron/*	

조치 방법

■ 기타 중요 파일 소유자 변경 및 타사용자 쓰기 권한 제거

1. 기타 중요 파일 소유자 변경
   # chown root [기타 중요 파일]
2. 기타 중요 파일 타사용자 쓰기 권한 제거
   # chmod o-w [기타 중요 파일]

서비스 Banner 관리

항목설명

시스템에 일반적인 서비스(SSH, SFTP 등)의 접근 시 출력되는 Banner를 관리하여 서비스 버전 유출을 막는다.
서버 사용자 범위를 명시하고, 모든 활동이 모니터링되고 있음을 표시해야 하며, 해당 프로세스의 버전과 시스템의 호스트 명이 노출되지 않도록 배너를 설정한다.
※ sshd_config 설정에 따라 Banner 파일 위치가 다를 수 있다.

진단 기준

양호
Banner에 경고 문구가 설정되어 있는 경우

취약
Banner에 경고 문구가 설정되어 있지 않은 경우

진단 방법

■ Bannar 확인

1. 배너 파일이 존재하는 경로 확인
   # cat /etc/ssh/sshd_config | grep "Banner"
2. 위에서 확인한 경로에서 배너 내용 확인

조치 방법

■ Banner 설정

1. /etc/ssh/sshd_config 파일에 Banner 설정
   # vi /etc/ssh/sshd_config
   Banner /etc/issue.net
2. /etc/issue.net 파일을 생성하고 경고 메시지 삽입 (예시)

```
##################################################################
        This system is for the use of authorized users only.
        Individuals using this computer system without authority, or in
        excess of their authority, are subject to having all of their
        activities on this system monitored and recorded by system
        personnel.

        In the course of monitoring individuals improperly using this
        system, or in the course of system maintenance, the activities
        of authorized users may also be monitored.

        Anyone using this system expressly consents to such monitoring
        and is advised that if such monitoring reveals possible
        evidence of criminal activity, system personnel may provide the
        evidence of such monitoring to law enforcement officials.
##################################################################
```

session timeout 설정

항목설명

**지정된 시간 동안 사용하지 않을 경우 접속된 session을 해당 서버에서 끊도록 설정하였는지 점검한다.
사용하지 않는 session에 대한 time out을 설정하지 않을 경우 기밀성뿐만 아니라 가용성 측면에서도 문제점을 발생시킬 수 있다.
지정된 시간 동안 사용하지 않을 경우 접속된 session을 해당 서버에서 끊도록 설정하는 것이 필요하다. (300초 경과 시 timeout)**

진단 기준

양호

/etc/profile"과 "xsconsole"에 time out이 모두 설정되어 있는 경우

취약

/etc/profile"나 "xsconsole" 한쪽에만 time out이 설정되어 있거나 둘 다 설정되어 있지 않은 경우

진단 방법

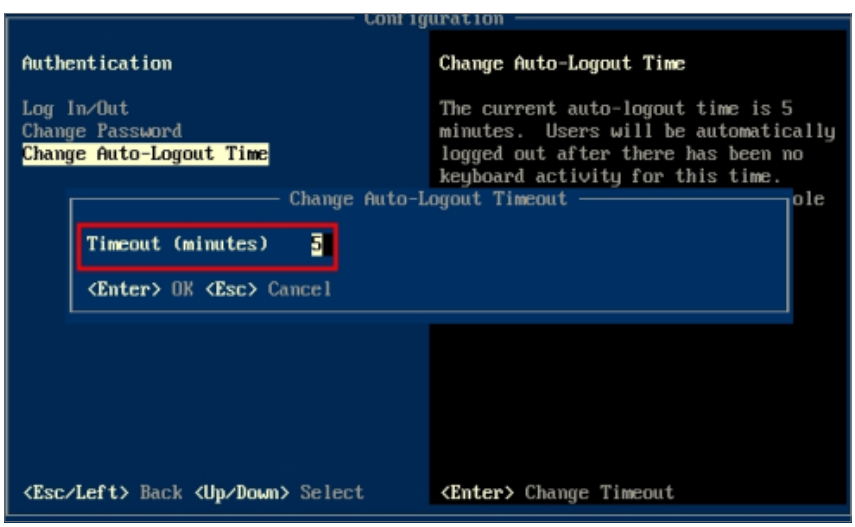
■ /etc/profile에서 session timeout 설정 확인

cat /etc/profile | grep "TMOUT"

```
[root@46409ceded40 ~]# cat /etc/profile | grep "TMOUT"
TMOUT=300
export TMOUT
```

■ xsconsole에서 session timeout 설정 확인

xsconsole → Authentication → Change Auto-Logout Time → Time out(minutes)에서 확인



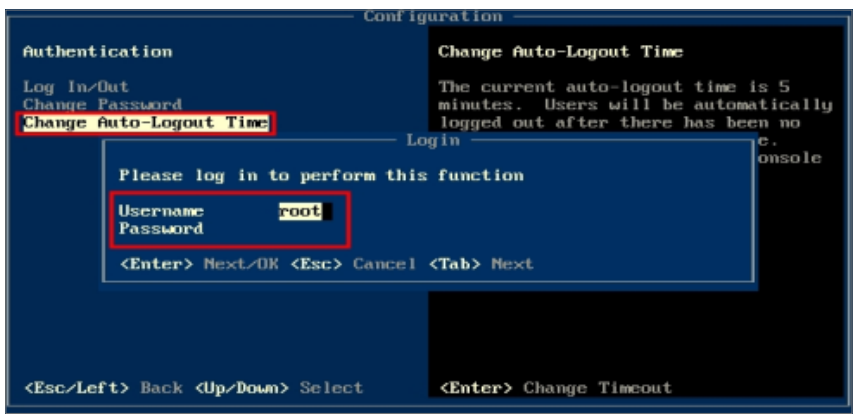
조치 방법

■ /etc/profile 파일에서 설정

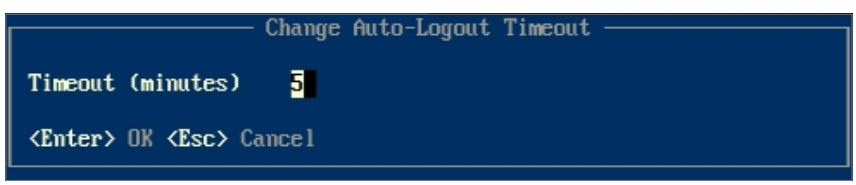
/etc/profile 파일 안에 time out 설정
# vi /etc/profile
TMOUT=300
export TMOUT

■ xsconsole에서 설정

1. xsconsole → Authentication → Change Auto-Logout Time → 로그인



2. Timeout (minutes)에서 설정



root 계정의 ssh 및 sftp 접근 제한

항목설명

root로 직접적인 원격 접근은 보안상 위험하므로, 일반 사용자를 통해 su 명령어를 이용하여, root로 접근할 수 있도록 하는 것이 보안상 필요하다.
어느 계정을 통해 root (슈퍼 user)로 접근했는지 알기 위해 보안상 필요하다.

진단 기준

양호

root 계정으로 ssh 및 sftp 접근이 제한되어 있는 경우

취약

root 계정으로 ssh 및 sftp 접근이 제한되어 있지 않은 경우

진단 방법

■ root 계정 원격 접속 제한 설정 확인

1. /etc/pam.d/login 파일 설정 확인
   # cat /etc/pam.d/login | grep "pam_securetty.so“
   auth required pam_securetty.so
   또는, auth [user_unknown=ignore success=ok ignore=ignore default=bad] pam_securetty.so
   또는, auth required /lib/security/pam_securetty.so
2. /etc/ssh/sshd_config파일 설정 확인
   # cat /etc/ssh/sshd_config | grep "PermitRootLogin“
   PermitRootLogin no

조치 방법

■ root 원격 접속 제한 설정

1. /etc/pam.d/login 파일설정에 추가 설정
   # vi /etc/pam.d/login
   auth required /lib/security/pam_securetty.so
2. /etc/ssh/sshd_config파일 설정 수정(주석제거 또는 신규 삽입)
   # vi /etc/ssh/sshd_config
   PermitRootLogin no

SSH(Secure Shell) 버전 취약점

항목설명

OpenSSH는 SSH(Secure Shell) 프로토콜을 구현한 오픈 소스 프로그램으로 telnet, ftp, rlogin, rsh 등을 대체한다.
OpenSSH는 네트워크 트래픽을 암호화하여 패킷 스니핑과 같은 공격으로부터 중요한 데이터를 보호할 수 있다. 그러나, OpenSSH의 낮은 버전에서는 다수의 취약점이 발견되고 있으며, 이러한 취약점으로 인해 root 권한 획득, DoS 공격 등 다양한 공격의 대상이 될 수 있다.
Citrix에서는 Xenserver 서버에 접근하기 위한 프로토콜로서 SSH를 사용하고 있다.

진단 기준

양호
벤더 사가 권장하는 OpenSSH 버전일 경우

취약
취약한 OpenSSH 버전일 경우

진단 방법

■ ssh 버전 확인

1. /etc/pam.d/login 파일 설정 확인
   # ssh -V

조치 방법

■ ssh 서비스 필요시

OpenSSH 업데이트 권장

■ ssh 서비스 불필요 시

1. 실행 중인 서비스 중지
   # ps -ef | grep sshd
   root 414 0.0 0.7 2672 1692 /usr/sbin/sshd
   # kill 9 414
2. SSH가 시작되지 않도록 시작스크립트의 파일명 변경
   (OS마다 시작 스크립트 위치가 다름)
   # ls -al /etc/rc*. d/* | grep sshd (시작스크립트 파일 위치 확인)
   # mv /etc/rc2.d/S55sshd /etc/rc2.d/_S55sshd

※ SSH 설정에 따라 /etc/ssh/sshd_config 파일 위치가 다를 수 있음

비고

https://www.openssh.com/releasenotes.html

불필요한 서비스 제거

항목설명

서버에 불필요한 서비스의 Port들이 열려 있는 경우 주요 시스템 정보 노출 및 서비스 거부(DOS) 공격이 일어날 수 있다.
Xenserver 이용한 클라우드 컴퓨팅 서비스를 위해 서버 관리용으로 SSH와 VNC를 제공하고 있다.
클라우드 컴퓨팅 서비스에 불필요한 telnet, ftp, rlogin, rsh 등을 사용할 경우 각각의 프로토콜에 대한 취약점으로 인해 root 권한 획득, DoS 공격등 다양한 공격의 대상이 될 수 있다.

진단 기준

양호
불필요한 서비스가 비활성화되어 있는 경우

취약
불필요한 서비스가 활성화되어 있는 경우

진단 방법

■ 서비스 확인

```
# ps -ef | grep [서비스 명]
```

〈불필요한 서비스 목록〉

불필요한 서비스			
echo(7)	chargen(19)	finger(79)	nntp(119)
netbios_dgm (138)	ldap(389)	ntalk(518)	ldaps(636)
nfsd(2049) -NFS 미사용시	discard(9)	time(37)	sftp(115)
ntp(123)	netbios_ssn(139)	printer(515)	uucp(540)
ingreslock(1524)	dtspcd(6112)	daytime(13)	tftp(69)
uucp-path(117)	netbios_ns(137)	bftp(152)	talk(517)
pcserver(600)	www-ldap-gw (1760)		
클라우드 컴퓨팅 서비스에 불필요한 서비스			
FTP	NFS	RPC	SNMP
Sendmail	SWAT	Samba	NIS, NIS+
telnet	RLOGIN	RSH	기타

조치 방법

■ 서비스 필요시

최신 버전 설치

■ 서비스 불필요 시

1. /etc/xinetd.d" 디렉터리 내의 서비스 파일 수정
   # vi /etc/xinetd.d/ [서비스 파일명]
2. xinetd.d 디렉터리 내에서 필요없는 서비스를 Disable 을 yes로 설정
   /etc/xinetd.d/chargen 파일
   service chargen
   {
   Disable = yes
   ... 생략 ...
   }
3. service 재시작
   #service xinetd restart
   〈클라우드 컴퓨팅 서비스에 불필요한 서비스 중지〉
   불필요한 서비스 중지
   # ps -ef | grep [서비스 명]
   # kill * 9 [프로세스 ID]

관리용 원격 접근 제어

항목설명

관리용으로 SSH나 XenCenter를 이용하여 원격에서 XenServer에 접근할 수 있다. 관리자가 XenServer에 원격으로 접근이 불필요한 경우에는 관리자 원격 접근을 제한함으로 비인가적인 시스템 사용을 방지하여 침해의 가능성을 줄일 수 있다.

진단 기준

양호

xsconsole의 [Network and Management Interface] 메뉴에서 “Interface”가 설정되어 있지 않은 경우

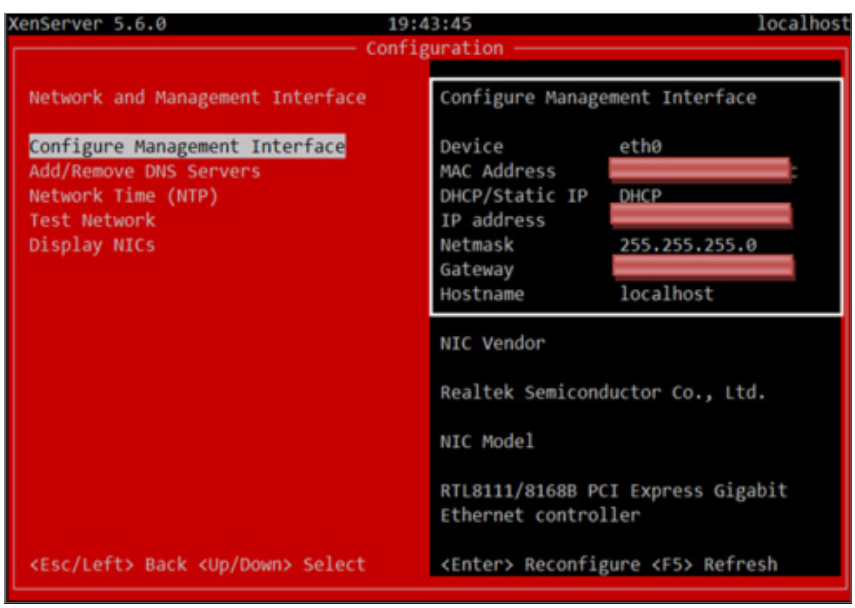
취약

xsconsole의 [Network and Management Interface] 메뉴에서 “Interface”가 설정되어 있는 경우

진단 방법

■ 관리용 원격 접속 접근 제어 설정 확인

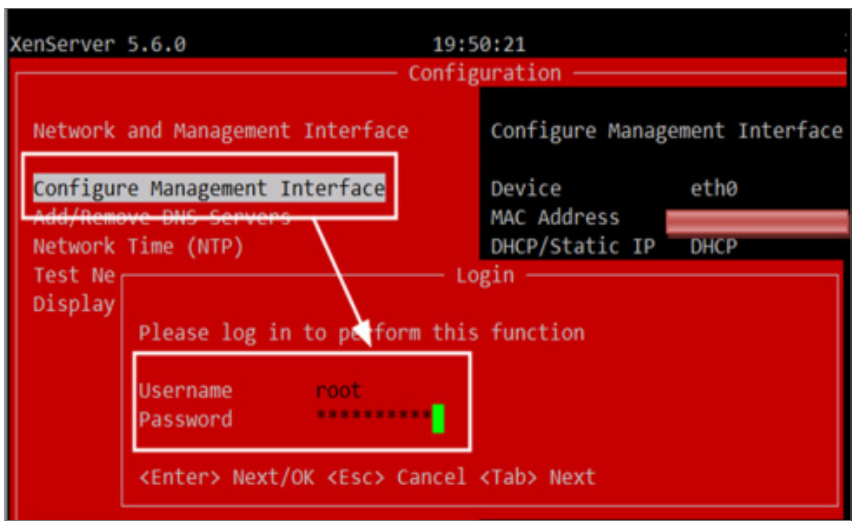
xsconsole → NetWork and Management Interface → Configure Management Interface에서 확인



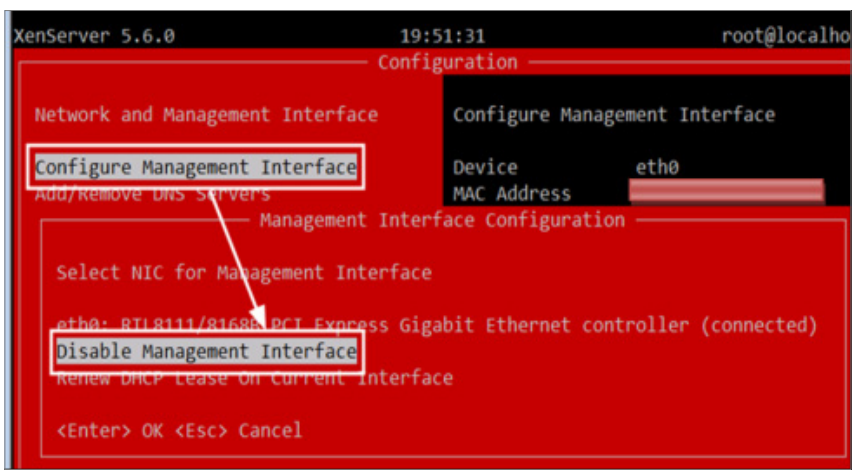
조치 방법

■ 관리용 원격 접속 접근제어 설정

1. xsconsole → Network and Management Interface → Configure Management Interface → Login



2. Login 후 나타나는 Management Interface Configuration 화면에서 Disable Management Interface를 선택하여 관리용도로 원격에서의 접근을 차단 설정



Remote Shell 접근 제어

항목설명

XenServer에 Remote Shell을 이용하여 원격에서 접근할 수 있다.
XenServer에 오직 XenCenter만을 이용하여 접근을 허용하고, Remote Shell을 이용하여 접근이 불필요한 경우에는 관리자 원격 접근을 제한함으로 비인가 시스템 사용을 방지하여 침해의 가능성을 줄일 수 있다.

진단 기준

양호

xsconsole의 [Remote Service Configuration] 메뉴에서 [Enable/Disable Remote Shell]이 disable로 설정되어 있는 경우

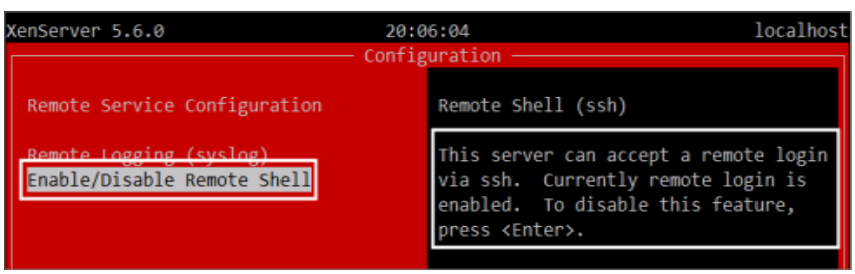
취약

xsconsole의 [Remote Service Configuration] 메뉴에서 [Enable/Disable Remote Shell]이 Enable로 설정되어 있는 경우

진단 방법

■ Remote Shell 접근제어 설정 확인

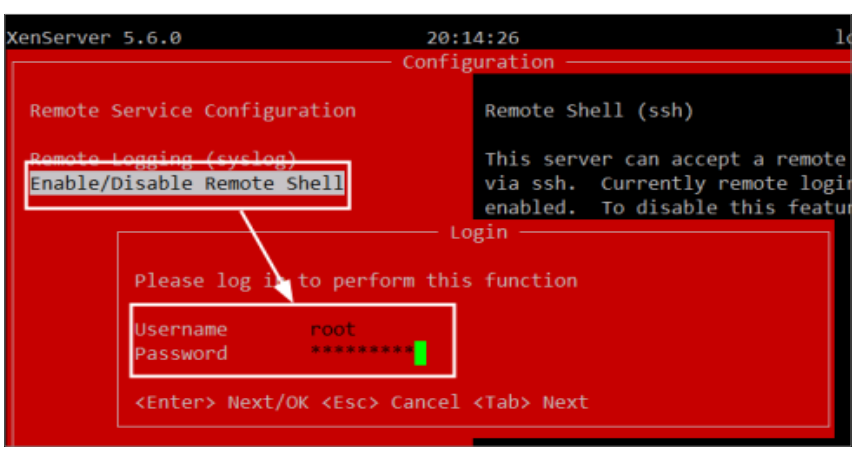
Xsconsole → remote Service Configuration → Enable/Disable Remote Shell에서 확인



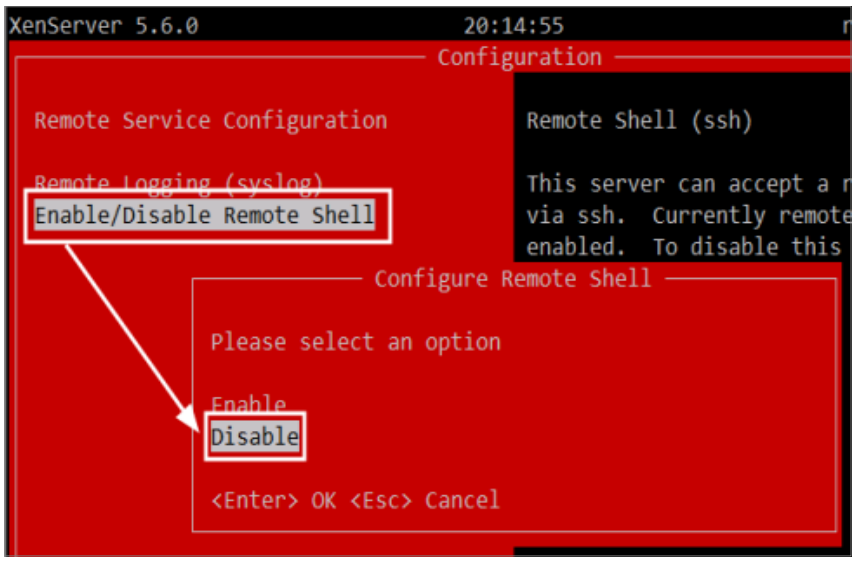
조치 방법

■ Remote Shell 접근 제어 설정

1. xsconsole의 [Remote Service Configuration] 메뉴에서 [Enable/Disable Remote Shell]을 선택한 후 Login



2. Login 후 나타나는 [Configure Remote Shell] 화면에서 “Disable”를 선택하여 원격에서의 Shell 접근 차단을 설정



비고

https://www.openssh.com/releasenotes.html

Guest VM 네트워크 분리

항목설명

Guest 네트워크는 VLAN을 이용하여 트래픽 분리가 가능하고, Guest OS(Virtual Machine) Group 간 네트워크가 연동될 경우 민감한 트래픽에 접근할 가능성이 있다. 반드시 분리되어야 하는 Guest OS(Virtual Machine) Group은 VLAN을 이용하여 트래픽을 분리하여 사용해야 한다.

진단 기준

양호

Guest OS (Virtual Machine) Group이 VLAN을 이용하여 트래픽이 분리되어 있는 경우

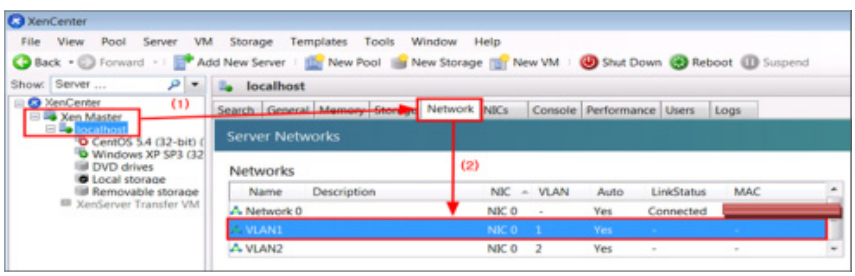
취약

Guest OS (Virtual Machine) Group이 VLAN을 이용하여 트래픽이 분리되어 있지 않은 경우

진단 방법

■ Guest VM 네트워크 설정 확인

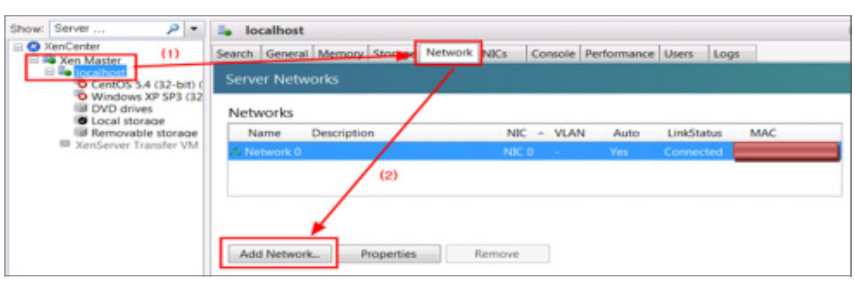
Xen Master → Xenserver → network vlan 확인 → 인터뷰를 통해 분리되어서 설정하고 있는지 확인



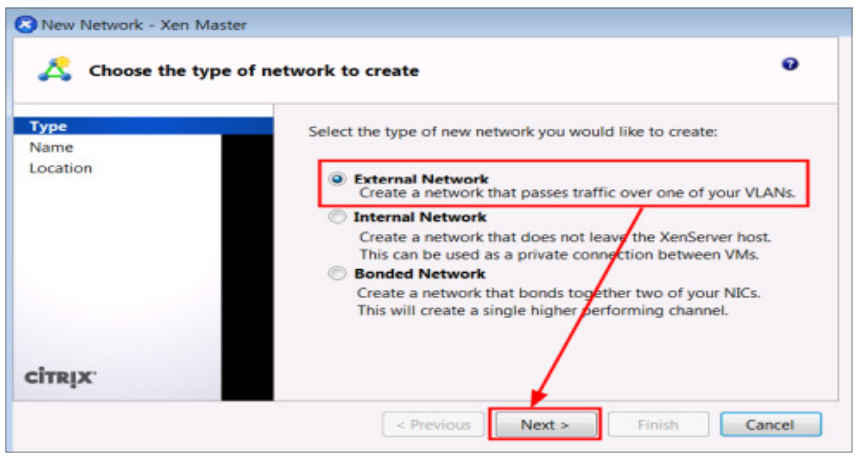
조치 방법

■ Guest VM 네트워크 설정

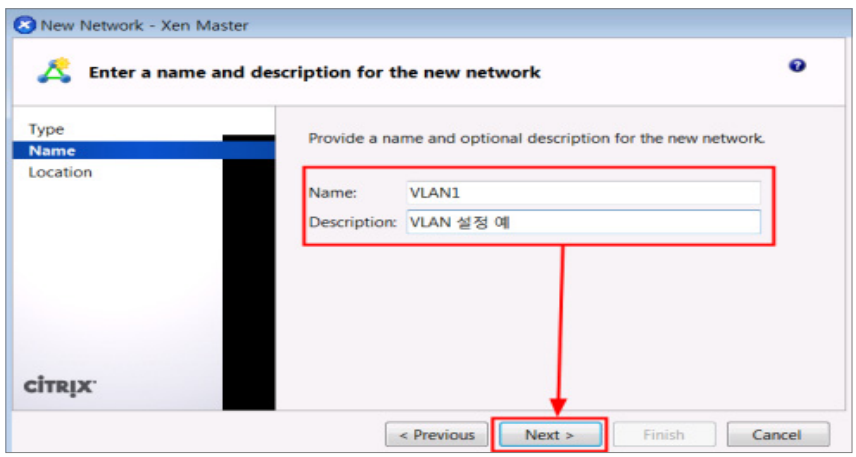
1. XenCenter → XenServer → Network에서 Add Network 선택



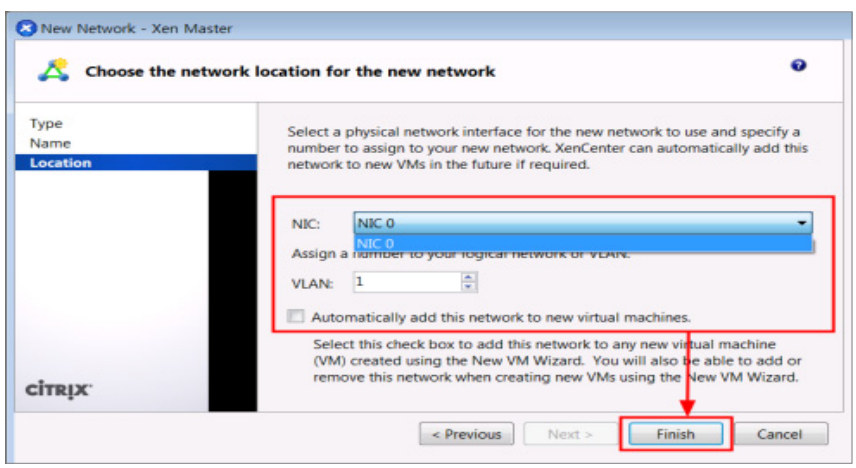
2. 네트워크 생성 화면에서 External Network → Next



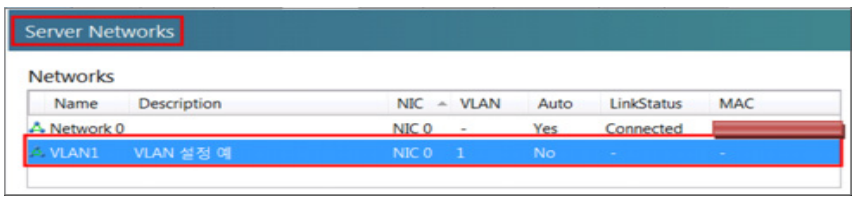
3. 생성하려는 VLAN의 이름, 설명을 입력 → Next



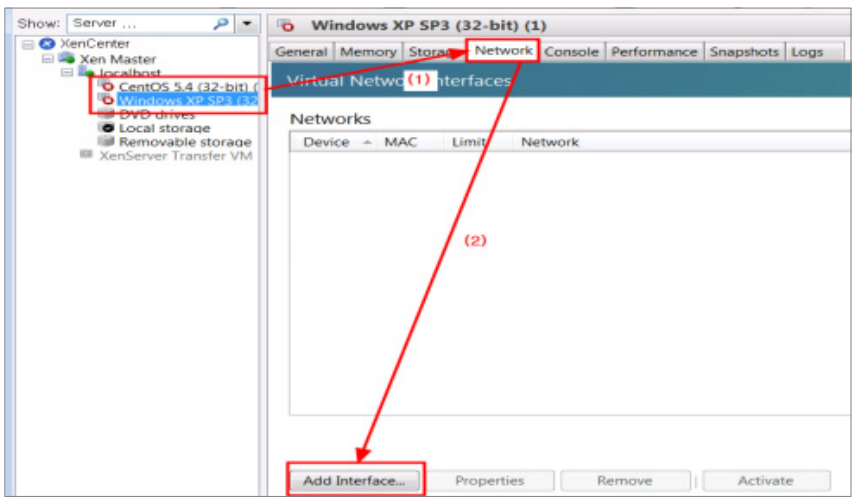
4. VLAN을 설정하는 물리적인 NIC 장치를 선택 → VLAN의 태그 선택 → Finish →VAN 생성
※ 이미 사용중인 태그는 설정할 수 없음



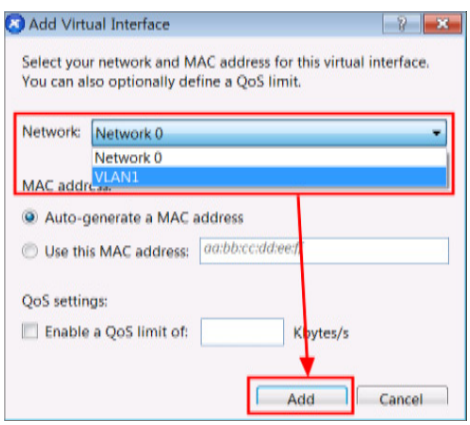
5. Server Networks에서 생성한 VLAN을 확인



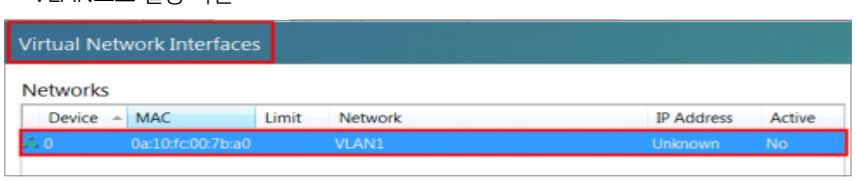
6. 네트워크 분리가 필요한 Guest OS를 선택하고, [Network]를 선택한 후 [Add Interface] 선택
※ Guest OS를 종료되어야 설정할 수 있음.



7. Network에서 생성한 VLAN을 선택 → Add → Guest OS의 Network를 VLAN으로 설정



8. Virtual Network Interfaces에서 Guest OS에 설정된 네트워크를 확인 또는 현재 VLAN으로 설정 확인



SU 로그 설정

항목설명

기본적으로 일반 사용자에서 Super User로 사용되는 기록을 남기기 위해서 su 사용 로그를 남기도록 하는 보안 설정이 필요하다. 시스템의 가용성 및 무결성 등을 침해하는 사건이 발생할 경우, 일반적으로 Super User 권한으로 사건이 진행되기 때문에 su의 로깅이 필요하다. su 로그를 기록하도록 syslog 설정 파일을 수정하고, Authpriv에 관련된 로그를 파일로 남기지 않고 있다면 아래와 같이 설정한다.

진단 기준

양호

/var/log/secure 파일을 확인하여 su 기록이 남고 있는 경우

취약

/var/log/secure 파일을 확인하여 su 기록이 남고 있지 않은 경우

진단 방법

■ /etc/syslog.conf 파일에서 확인 (6버전)

```
# cat /etc/syslog.conf | grep authpriv.*
```

■ /etc/rsyslog.conf 파일에서 확인 (7, 8버전)

```
# cat /etc/rsyslog.conf | grep authpriv.*
```

조치 방법

■ /etc/syslog.conf 파일에서 설정 (6버전)

```
# vi /etc/syslog.conf 파일에서 아래와 같은 설정으로 변경
authpriv.* /var/log/secure
# /etc/rc.d/init.d/syslog restart
```

■ /etc/rsyslog.conf 파일에서 설정 (7, 8 버전)

```
# vi /etc/rsyslog.conf 파일에서 아래와 같은 설정으로 변경
authpriv.* /var/log/secure
# systemctl restart rsyslog
```

syslog 설정

항목설명

기본적으로 시스템 운영 중 발생하는 Info 및 alert 등에 대한 기록을 남기기 위한 “syslog.conf” 파일의 보안 설정이 되었는지 점검한다. Syslog 데몬은 시스템의 로그를 기록하는 전용 데몬으로 원격 또는 로컬 시스템의 커널 메시지 및 시스템 로그를 감시하는 역할을 한다. 이 설정이 제대로 되어있지 않은 경우, 적절한 로그가 시스템 로그 파일에 남지 않아 침입자의 흔적이나 시스템 오류에 대해 분석이 불가하다.

진단 기준

양호

syslog에 중요 로그 정보에 대한 설정이 되어 있을 경우

취약

syslog에 중요 로그 정보에 대한 설정이 되어 있지 않은 경우

진단 방법

[XenServer]

■ /etc/syslog.conf 파일을 점검하여, info, alert 등에 대한 로그 파일 설정을 확인

```
# cat /etc/syslog.conf | egrep "info|alert|notice|debug|warn|error" | egrep "var|log“
```

■ /etc/rsyslog.conf 파일을 점검하여, info, alert 등에 대한 로그 파일 설정을 확인

```
# cat /etc/rsyslog.conf | egrep "info|alert|notice|debug|warn|error" | egrep "var|log“
```

※ Facility : 로그 생성 서비스

*	모든 서비스
authpriv	인증 및 보안 관련 메시지
cron	cron 데몬과 atd 데몬에 의해 발생하는 메시지
daemon	telnet, ftp 등과 같은 데몬에 의한 메시지
kern	kernel에 의한 메시지
lpr	프린터 데몬인 lpd에 의해 발생하는 메시지
mail	sendmail, pop, qmail 등의 메일 시스템에서 발생하는 메시지
news	USENET 등과 같은 뉴스시스템에 의해 발생하는 메시지
user	사용자에 의해 생성된 프로세스
syslog	syslogd에 의해 발생하는 메시지
local0 ~ local7	시스템 부팅 메시지 기록, 기타 여분 서비스에 사용하기 위함

※ Priority : 로그 수준(Level)

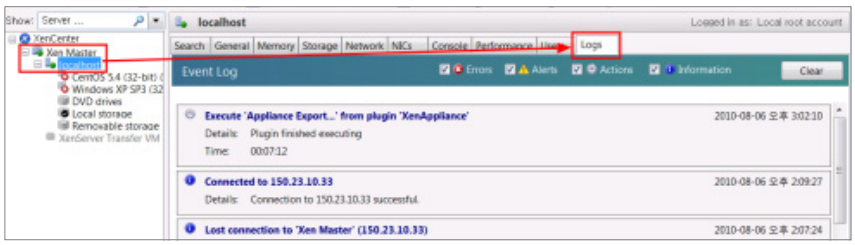
emerg	시스템이 전면 중단되는 패닉 상태, 전체 공지가 필요한 상황 (system is unusable)
alert	즉각적인 조치가 필요한 상황 (action must be taken immediately)
crit	하드웨어 등의 심각한 오류가 발생한 상황 (critical condition)
err	일반적인 에러/오류가 발생한 상황
warning	경고 메시지
notice	에러/오류는 아니지만, 관리자의 조치가 필요한 상황
info	의미 있는 정보 관련 메시지
debug	디버깅용 메시지

※ 로그 수준을 지정하게 되면 해당 수준 이상의 상황이 발생했을 때 로그가 남게 됨

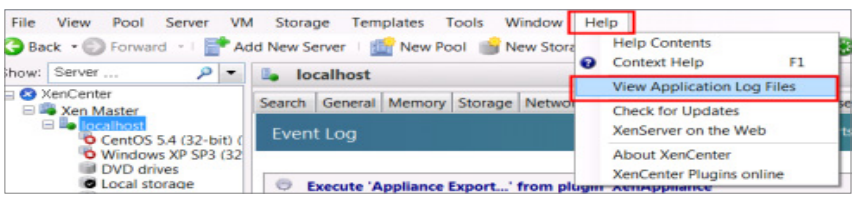
[XenCenter]

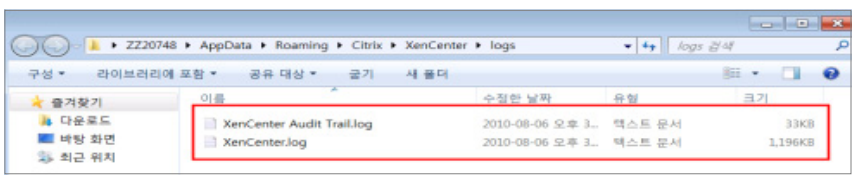
■ syslog 설정 확인

1. XenCenter에서 [XenServer]를 선택한 후 [Logs] 메뉴에서 로그를 확인



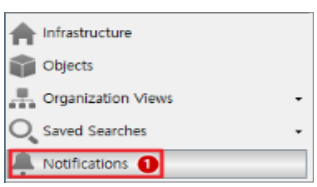
2. XenCenter의 메뉴에서 [Help]를 선택한 후 [View Application Log files] 메뉴에서 로그를 확인



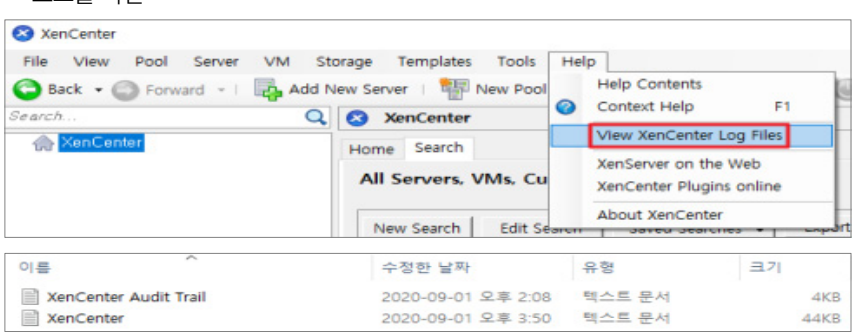


■ syslog 설정 확인 (7 버전, 8 버전)

1. XenCenter에서 왼쪽 패널 하단 Notification에서 Information 로그 설정 확인



2. XenCenter의 메뉴에서 [Help]를 선택한 후 [View Application Log files] 메뉴에서 로그를 확인



※ XenServer/XenCenter 시스템 로그 파일

XenServer 로그 위치	/val/log/ xensource.log
	/var/log/ xenstored-access.log
Windows7 로그 위치	%userprofile%\AppData\Roaming\Citrix\XenCenter\logs\ XenCenter Audit Trail.log
	%userprofile%\AppData\Roaming\Citrix\XenCenter\logs\ XenCenter.log
Windows XP / 2003 로그 위치	%userprofile%\AppData\Citrix\XenCenter\logs\ XenCenter Audit Trail.log
	%userprofile%\AppData\Citrix\XenCenter\logs\ XenCenter.log
Windows Vista 로그 위치	%userprofile%\AppData\Citrix\Roaming\XenCenter\logs\ XenCenter Audit Trail.log
	%userprofile%\AppData\Citrix\Roaming\XenCenter\logs \ XenCenter.log

조치 방법

■ XenServer 로그 파일 설정

1. /etc/(r)syslog.conf 파일을 점검하여, info, alert 등에 대한 로그 파일을 설정

```
# vi /etc/(r)syslog.conf
*.notice      /var/log/messages
*.emerg       *
*.alert       /dev/console

# Set info,warn,error to log to syslog by default
info;audit;syslog:local6
warn;;syslog:xapi
error;;syslog:xapi

# Also print everything (debug<->error) into xensource.log for easier debugging
debug;;file:/var/log/xensource.log
info;;file:/var/log/xensource.log
warn;;file:/var/log/xensource.log
error;;file:/var/log/xensource.log
```

2. "(r)syslog.conf"파일을 수정한 후에는 이것이 적용되도록 다음의 명령을 사용하여 syslogd restart

```
# /etc/rc.d/init.d/syslog restart
```

syslog 전송 포트 차단

항목설명

UDP 514 Port는 Remote로 syslog를 전송하는 Port로 사용되며, 사용 시 보안상 취약하기 때문에 서비스 포트가 열려 있을 경우, 침해사고에 노출될 수 있다. 따라서 Remote Log 서버를 사용하지 않는 경우, syslog 전송 Port 차단을 권고한다.

진단 기준

양호

Remote Log 서버를 사용하지 않을 경우 syslog 전송 Port를 차단한 경우

취약

Remote Log 서버를 사용하지 않고 UDP 514 Port를 사용 중인 경우

진단 방법

■ syslog 전송 포트 차단 설정 확인

1. 인터뷰를 통해 Remote Log 서버 사용 여부 확인
2. udp514포트 확인
   # netstat –an | grep "udp“
   또는
   # netstat –an | grep "udp" | egrep "514“

```
[root@localhost sbin]# netstat -an | grep "udp"
udp        0      0 0.0.0.0:514                 0.0.0.0:*
```

조치 방법

■ Remote Log 서버 필요시

Remote Log 사용 시 보안담당자 및 담당 매니저와의 협의 필요

■ Remote Log 서버 불필요시

syslog.conf 파일 수정(“/etc/sysconfig/syslog” 파일에 “SYSLOGD_OPTIONS”의 “-r” 옵션 삭제)
# vi /etc/sysconfig/syslog
SYSLOGD_OPTIONS="-m 0"

```
# -x disables DNS lookups on messages recieved with -r
# See syslogd(8) for more details
SYSLOGD_OPTIONS="-M 0"
# Options to klogd
# -2 prints all kernel oops messages twice; once for klo
```

■ Remote Log 서버 불필요시 (7 버전, 8 버전)

Syslog.conf 파일 수정(“/etc/sysconfig/rsyslog” 파일에 “SYSLOGD_OPTIONS”의 “-r” 옵션 삭제)
# vi /etc/sysconfig/rsyslog
SYSLOGD_OPTIONS="-m 0"

로깅 수준 설정

항목설명

기본적으로 시스템 운영 중 발생하는 Information 등에 대한 기록을 남기기 위한 로그 설정이 되었는지 점검한다. 시스템에 적절한 로그 파일이 없는 경우, 침입자의 흔적이나 시스템 오류 사항에 대한 분석이 이루어질 수 없다.

진단 기준

양호

/etc/syslog.conf 파일에 “info” 설정이 되어있거나 XenCenter에서 [XenServer]를 선택한 후 [Logs] 메뉴에서 “Information” 로그가 설정되어 있는 경우

취약

/etc/xensource/log.conf 파일에 “info” 설정이 되어있지 않거나 XenCenter에서 [XenServer]를 선택한 후 [Logs] 메뉴에서 “Information” 로그가 설정되어 있지 않은 경우

진단 방법

[XenServer]

■ 로깅 수준 설정 확인

/etc/syslog.conf파일에 “info” 설정 확인
cat /etc/syslog.conf | grep "info"

```
[root@localhost xensource]# cat /etc/syslog.conf | grep "info"
*.info;mail,authpriv,cron,local6,local2,local1,local0.none      -/var/log/messag
es
local3.info                                                     -/var/log/xenstored-acce
ss.log
# xcp-rrdd-plugins (info and above) to local0
local0.info                     -/var/log/xcp-rrdd-plugins.log
authpriv.info                   /var/log/secure
info;;file:/var/log/xensource.log
```

■ 로깅 수준 설정 확인 (7 버전, 8 버전)

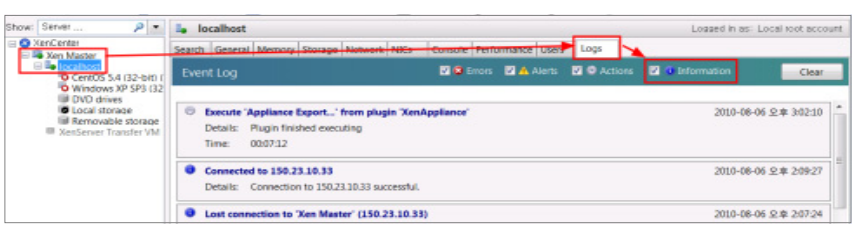
/etc/rsyslog.d/xenserver.conf 파일에 “info” 설정 확인
/etc/rsyslog.d/xenserver.conf | grep "info"

```
# Xapi, xenopsd echo to syslog local5
local5.info_                                                    -/var/log/xensource.log
```

[XenCenter]

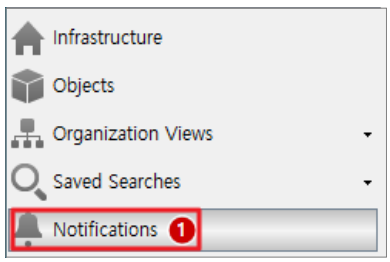
■ 로깅 수준 설정 확인

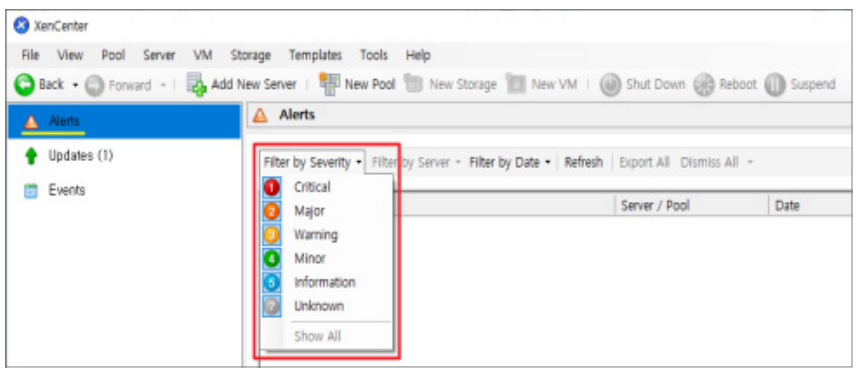
XenCenter에서 [XenServer]를 선택한 후 [Logs] 메뉴에서 Information 로그 설정 확인



■ 로깅 수준 설정 확인 (6.5 이후 버전)

XenCenter에서 왼쪽 패널 하단 Notification에서 Information 로그 설정 확인





조치 방법

[XenServer]

■ 로깅 수준 설정

/etc/syslog.conf" 파일에 "info" 로그를 남기도록 설정
vi /etc/syslog.conf"
info;;file:/var/log/xensource.log

```
# Also print everything (debug<->error)
debug;;file:/var/log/xensource.log
info;;file:/var/log/xensource.log
warn;;file:/var/log/xensource.log
error;;file:/var/log/xensource.log
```

■ 로깅 수준 설정 (7 버전, 8 버전)

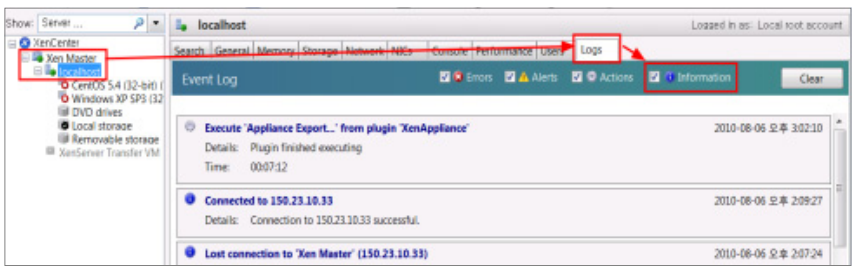
/etc/rsyslog.d/xenserver.conf 파일에 "info" 로그를 남기도록 설정
vi /etc/rsyslog.d/xenserver.conf

```
# Xapi, xenopsd echo to syslog local5
local5.info_                                    -/var/log/xensource.log
```

[XenCenter]

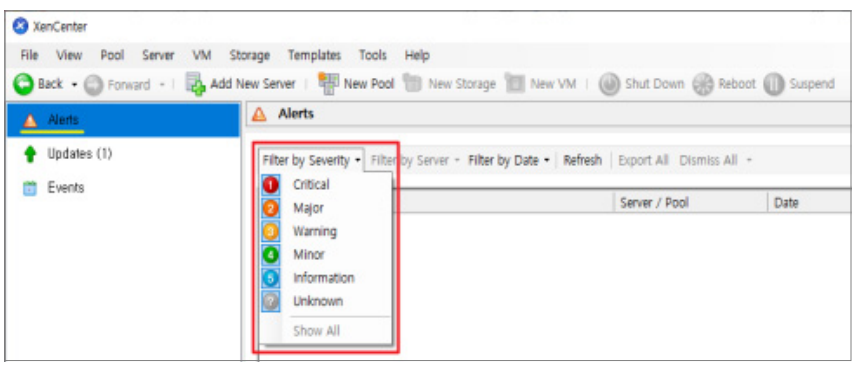
■ 로깅 수준 설정

XenCenter에서 [XenServer]를 선택 한 후 [Logs] 메뉴에서 “Information”에서 로그 설정



■ 로깅 수준 설정 (6.5 이후 버전)

XenCenter에서 왼쪽 패널 하단 Notification에서 Information 로그 설정



로그 파일 권한 설정

항목설명

시스템의 기본 로깅 기록은 관리자 이외에 다른 일반 사용자에게 열람할 수 있는 권한을 부여할 필요가 없으므로 로깅 기록을 저장하는 파일의 소유자 및 읽기 권한을 제한함으로 보안을 강화하는 것이 필요하다. 아래의 로그 파일 권한은 시스템 사용자(root, adm, bin 등) 소유자의 타 사용자 쓰기 권한을 제거한다.

진단 기준

양호

로그 파일의 소유자가 root이고, 타사용자 쓰기 권한이 존재하지 않는 경우

취약

로그 파일의 소유자가 root가 아니거나, 타사용자 쓰기 권한이 존재하는 경우

진단 방법

■ 로그 파일 확인

```
#  ls –alL [로그 파일명]
```

〈보안 강화적용 대상 로그 파일 목록〉

로그 파일	XenServer	로그 파일	XenServer
audit	/var/log/audit.log	btmp	/var/log/btmp
xenstored	/var/log/xenstored-access.log	secure	/var/log/secure
wtmp	/var/log/wtmp	messages	/var/log/messages
lastlog	/var/log/lastlog		

조치 방법

■ 로깅 파일 소유자 및 권한 변경

1. 로그 파일의 소유자 변경 설정
   ```
   # chown  root  [로그 파일명]
   ```
2. 로그파일의 타사용자 쓰기 권한 제거 설정
   ```
   # chmod  o-w  [로그 파일명]
   ```

보안패치 적용

항목설명

XenServer 및 XenCenter Patch는 Xen 시스템을 Citrix에서 출시하고 난 뒤 Xen과 관련된 응용프로그램, 서비스, 실행 파일 등의 오류나 보안취약점 등을 수정하여 적용한 Update 파일이다. Update Patch 발표 후 취약성을 이용한 공격 도구가 먼저 출현할 수 있으므로, Update Patch는 발표 후 가능한 한 빨리 설치할 것을 권장한다.

진단 기준

양호

패치 적용 정책을 수립하여 주기적으로 패치를 관리하는 경우

취약

패치 적용 정책을 수립하지 않거나 주기적으로 패치를 관리하고 있지 않은 경우

진단 방법

■ 인터뷰를 통해 주기적으로 보안 패치 적용 여부 확인

※ HotFix 목록을 이용해 패치 적용 일자 확인
※ 패치 주기 확인
※ XenServer Mainline 버전의 지원 여부 확인

조치 방법

■ 설정 기준 권고 (또는 정책 기준)

1. 보안취약점이 발표되면 시스템 영향도를 평가하고, 긴급 대응책 및 중장기 대응책을 마련하여 계획과 허가에 의해 대응하는 것이 좋다.
2. 패치를 수행할 시 시스템의 영향도에 따라 패치를 차등 수행하도록 한다.
3. 시스템 운영에 영향을 주지 않는 범위 내에서 주기적으로 패치를 수행할 것을 권고함

비고

※ 보안 패치 적용 시, 시스템 영향도를 파악하여 충분한 테스트 후 적용 권고
※ 참고
https://en.wikipedia.org/wiki/Xen
https://support.citrix.com/article/CTX122443
https://www.citrix.com/ko-kr/support/product-lifecycle/product-matrix.html

2.3.

ESXi

2.3. ESXi

계정 관리(4개 항목), 보안 관리(18개 항목), 패치 및 로그 관리(2개 항목) 총 3개 영역에서 24개 항목으로 구성된다.

[표 3] ESXi 진단 체크리스트

구분	진단 항목
가. 계정 관리	root 계정 원격 접속 제한
	취약한 패스워드 사용제한
	계정 잠금 임계값 설정
	사용자 계정 관리
나. 보안 관리	ESXi Shell 사용 제한
	ESXi Shell 자동 종료
	ESXi Shell 및 SSH 세션 타임아웃 설정
	가상스위치 MAC 주소 변경정책 설정
	가상스위치 Promiscuous 모드 정책 설정
	가상스위치 Forged Transmits 모드 정책 설정
	SSH 데몬 빈암호 사용 인증 허용 제한
	SNMP 서비스 확인
	SNMP Community String 복잡성 설정
	접속 IP 및 포트 제한
	FTP 비활성화
	FTP root 접속 설정
	FTP 기본 디렉터리 경로 확인
	NTP 시간 동기화 설정
	SSL 시간 초과 구성 설정 확인
	이미지 프로필 및 VIB 승인 레벨 확인
	MOB(Managed Object Browser) 비활성화
	불필요한 서비스 제거
다. 패치 및 로그 관리	최신 보안패치 및 밴더 권고사항
	로그의 정기적 검토 및 보고

root 계정 원격 접속 제한

항목설명

root 계정으로 직접 로그인이 가능할 경우, 불법적인 침입자의 목표가 될 수 있으므로 root 계정 원격 접속을 금지해야 한다. 또한, 일반 사용자 계정 접속 후 관리자 계정으로의 변경 시 로그가 남지만, 관리자 계정으로 바로 접속하는 경우 어느 사용자가 접속했는지 알 수 없으므로 문제 발생 시 원인 파악이 어렵다.

진단 기준

양호

root 계정의 직접 접속이 제한된 경우

취약

root 계정의 직접 접속이 제한되어 있지 않은 경우

진단 방법

■ root 계정의 ssh 접속이 제한되어 있는지 확인

/etc/ssh/sshd_config 파일에서 “PermitRootLogin no”로 설정되어 있는지 확인
cat /etc/ssh/sshd_config | grep PermitRootLogin

```
[root@localhost:~] cat /etc/ssh/sshd_config | grep PermitRootLogin
PermitRootLogin no
```

조치 방법

■ root 계정의 ssh 접속 제한 설정

1. vi 편집기를 이용하여 /etc/ssh/sshd_config 파일 열기
   # vi /etc/ssh/sshd_config
2. 아래와 같이 설정 변경
   PermitRootLogin no

```
# vPP FCS_SSH_EXT.1.7: rekey after 1GB, 1H (instead of default 4GB for AES)
RekeyLimit 1G, 1H

SyslogFacility auth
LogLevel info

PermitRootLogin no
```

패스워드 복잡성 설정

항목설명

사용자 계정(root 및 일반계정 모두)의 암호 설정 시, 일반적으로 유추하기 쉬운 암호를 설정하여, 비인가 사용자의 시스템 접근을 허용할 수 있다. 따라서 영문(대문자, 소문자), 숫자, 특수문자가 혼합된 8자리 이상의 패스워드로 설정하여 공격자가 추측하기 어려운 패스워드를 사용해야 한다.

진단 기준

양호

패스워드를 영문, 숫자, 특수문자를 혼합 8자리 이상 사용하여 복잡하게 설정한 경우

취약

패스워드가 존재하지 않거나, 패스워드를 영문, 숫자, 특수문자를 혼합 사용하지 않거나 8자리 미만으로 설정한 경우

진단 방법

■ 설정을 통해 확인

1. /etc/pam.d/passwd 파일 내 pam_passwdqc.so 확인
   문자 클래스 3개 또는 4개인 경우, 8자리 이상 적용
   : retry=3 min=disabled,disabled,disabled,8,8
   문자 클래스 2개, 10자리 이상 적용
   : retry=3 min=disabled,10,disabled,disabled,disabled

※ Default 설정
- 문자 클래스 3개 또는 4개인 경우, 7자리 이상 적용
  : retry=3 min=disabled,disabled,disabled,7,7

■ 인터뷰를 통해 확인

인터뷰를 통해 사용 중인 계정의 패스워드의 복잡도를 확인한다. 이때, 패스워드는 복잡도 기준(대/소문자, 숫자, 특수문자 중 2가지 이상 조합 10자리, 3가지 이상 조합 8자리)을 만족해야 한다.

■ 패스워드 크랙 툴인 존 더 립퍼(John the Ripper)를 이용하여 취약한 패스워드 확인함.
존 더 립퍼는 사전에 있는 모든 단어와 그 변화형을 패스워드로 시도하고, 단어 하나하나를 암호화하면서 이미 암호화된 패스워드와 비교하는 방식으로, 취약한 패스워드로 설정된 사용자들을 찾아서 미리 알려줄 수 있다.

조치 방법

■ 설정 확인

1. vi 편집기를 이용해 /etc/pam.d/passwd 파일 내 pam_passwdqc.so 수정
   문자 클래스 3개 또는 4개인 경우, 8자리 이상 적용
   : retry=3 min=disabled,disabled,disabled,8,8
   문자 클래스 2개, 10자리 이상 적용
   : retry=3 min=disabled,10,disabled,disabled,disabled

■ 일반적으로 권장하는 패스워드 설정

1. 패스워드의 길이는 최소 8자 이상으로 설정
2. 영문(대문자, 소문자), 숫자, 특수문자를 혼합하여 패스워드 설정
3. 패스워드는 주기적으로 변경하고, 재사용 금지
4. 사전에 있는 단어나 누구나 유추 가능한 간단한 패스워드 사용 금지

■ ESXi 사용자 계정 패스워드 변경

1. 다른 사용자 계정 패스워드 변경(Root 권한일 때)
   # passwd 변경할 ID
   Enter new password : 변경할 Passwd
   Re-type new passwd : 변경할 Passwd (위와 동일)
2. 접속 중인 자신의 계정 패스워드 변경
   # passwd
   Enter new password : 변경할 Passwd
   Re-type new passwd : 변경할 Passwd (위와 동일)

※ 다음과 같은 패스워드는 피해야 한다.
지역명, 부서명, 담당자, 성명, 대표, 업무명, "root", "root123", "admin", "123admin" 등

계정 잠금 임계값 설정

항목설명

침입자에 의한 패스워드 무작위 대입 공격(Brute Force Attack)이나 패스워드 추측 공격(Password Guessing) 발생 시 암호입력 실패 횟수를 적정하게 제한함으로써 자동공격을 차단하고 공격 시간을 지체시켜 패스워드 유출 위험을 줄일 수 있다.

진단 기준

양호

패스워드 입력 횟수를 5회 이하로 제한한 경우

취약

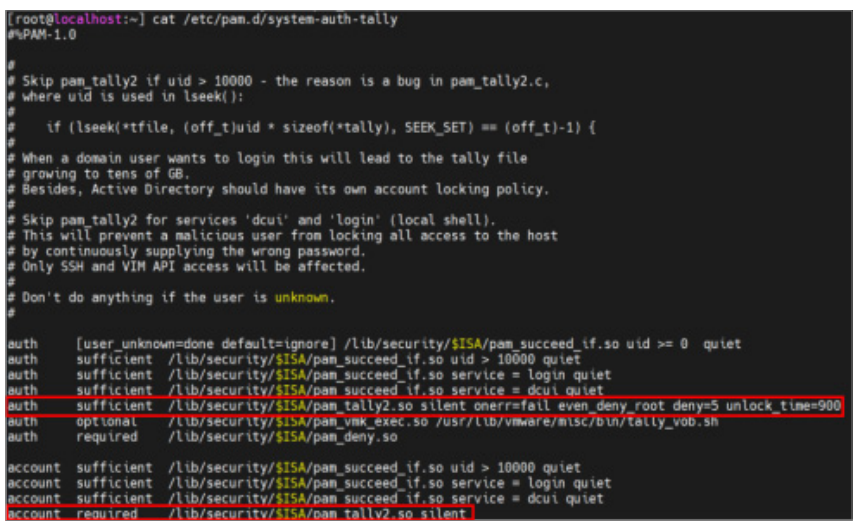
패스워드 입력 횟수를 설정하지 않거나, 5회 초과로 제한한 경우

진단 방법

[CLI]

■ 패스워드 입력 횟수가 제한되어 있는지 해당 설정 파일에서 설정값 확인

```
# cat /etc/pam.d/system-auth-tally
auth sufficient pam_tally2.so silent onerr=fail even_deny_root deny=3
unlock_time=100
(생략)
account required pam_tally2.so silent
```

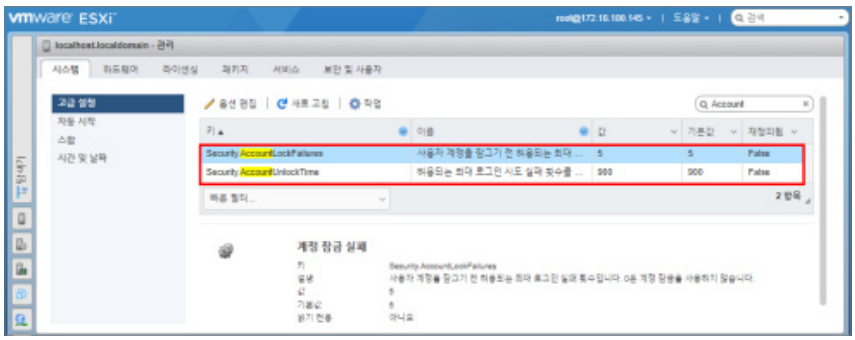


[vClient]

■ 패스워드 입력 횟수가 제한되어 있는지 해당 설정 파일에서 설정값 확인

vClient 실행 → 호스트 → 관리 → 시스템 → 고급설정 → security.AccountLockFailures 및 Security.AccountUnlockTime 검색

※ Security.AccountLockFailures: 사용자 계정이 잠길 때까지 허용되는 최대 로그인 시도 실패 횟수이며, 0은 계정 잠금을 비활성화 함
※ Security.AccountUnlockTime: 사용자가 잠기게 되는 시간(초)



조치 방법

[CLI]

■ 해당 설정 파일에 패스워드 입력 횟수를 제한하는 내용 추가 (예. 5회)

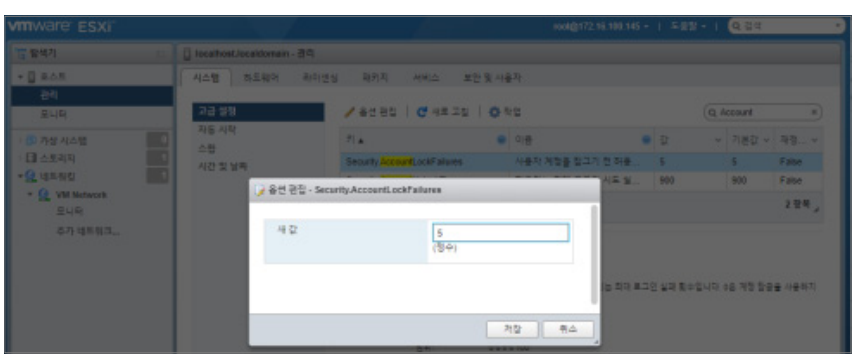
```
# vi /etc/pam.d/system-auth-tally
auth sufficient pam_tally2.so silent onerr=fail even_deny_root deny=5
unlock_time=100
(생략)
account required pam_tally2.so silent
```

```
auth     [user_unknown=done default=ignore] /lib/security/$ISA/pam_succeed_if.so uid >= 0  quiet
auth     sufficient  /lib/security/$ISA/pam_succeed_if.so uid > 10000 quiet
auth     sufficient  /lib/security/$ISA/pam_succeed_if.so service = login quiet
auth     sufficient  /lib/security/$ISA/pam_succeed_if.so service = dcui quiet
auth     sufficient  /lib/security/$ISA/pam_tally2.so silent onerr=fail even_deny_root deny=5 unlock_time=900
auth     optional    /lib/security/$ISA/pam_vmk_exec.so /usr/lib/vmware/misc/bin/tally_vob.sh
auth     required    /lib/security/$ISA/pam_deny.so

account  sufficient  /lib/security/$ISA/pam_succeed_if.so uid > 10000 quiet
account  sufficient  /lib/security/$ISA/pam_succeed_if.so service = login quiet
account  sufficient  /lib/security/$ISA/pam_succeed_if.so service = dcui quiet
account  required    /lib/security/$ISA/pam_tally2.so silent
```

[vClient]

■ 패스워드 입력 횟수를 5회로 변경

vClient 실행 → 호스트 → 관리 → 시스템 → 고급설정 → security.AccountLockFailures 및 Security.AccountUnlockTime 변경



사용자 계정 관리

항목설명

일반 모니터링 계정에 관리자 권한을 부여한 경우, 악의적인 사용자에 의한 시스템 조작, 서비스 장애, 정보 유출, VM 사용자 정보를 악용한 공격에 노출될 수 있다.

진단 기준

양호

불필요한 계정이 없거나 모니터링 계정에 최소한의 권한만 부여한 경우

취약

불필요한 계정이 존재하거나 모니터링 계정과 관리자 계정을 구분하지 않고 사용한 경우

진단 방법

[CLI]

■ 사용자 계정 확인

$ /etc/passwd

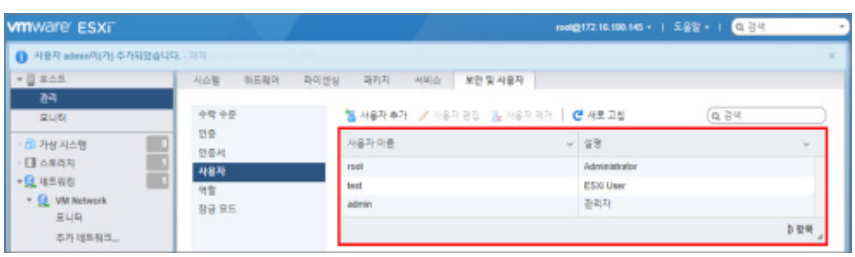
```
[root@localhost:~] cat /etc/passwd
root:x:0:0:Administrator:/:/bin/sh
daemon:x:2:2:System daemons:/:/sbin/nologin
nfsnobody:x:65534:65534:Anonymous NFS User:/:/sbin/nologin
dcui:x:100:100:DCUI User:/:/sbin/nologin
vpxuser:x:500:100:VMware VirtualCenter administration account:/:/sbin/nologin
```

※ 인터뷰를 통해 사용 중인 계정의 용도 확인이 필요함

[vClient]

■ 사용자 계정 권한 확인

vClient 실행 → 탐색기 → 호스트 → 관리 → 보안 및 사용자



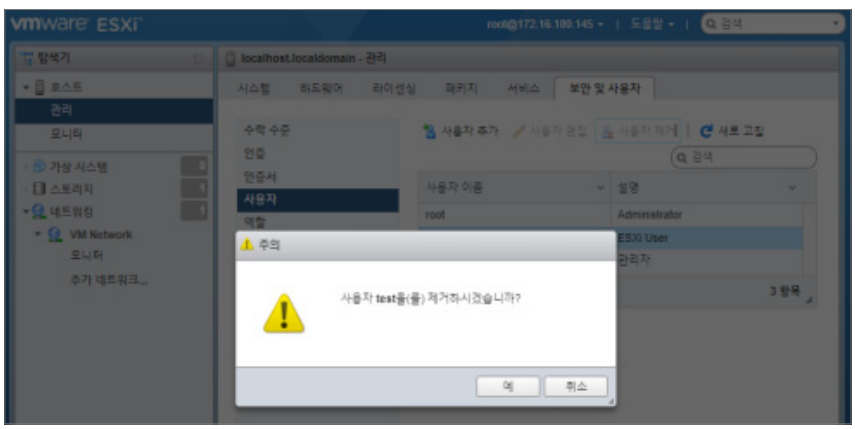
※ 관리자 계정만 ssh 접속이 가능함

조치 방법

[vClient]

■ 사용자 계정 권한 설정

vClient 실행 → 탐색기 → 호스트 → 관리 → 보안 및 사용자 → 용도 파악 후 불필요한 계정이 있는 경우 제거하고 사용자의 경우 최소한의 권한만 부여



ESXi Shell 사용 제한

항목설명

ESXi Shell은 VMware의 ESXi 가상화 플랫폼에서 제공하는 콘솔 기반의 명령 줄 인터페이스(CLI)이다. ESXi Shell을 사용하면 로컬(콘솔 Shell)로 또는 원격(SSH)으로 ESXi 호스트에 접속하여 명령을 입력할 수 있다. ESXi Shell은 대부분 유지 보수 및 관리 작업 용도로 사용되기 때문에 필요한 경우에만 사용하도록 설정해야 한다.

진단 기준

양호

ESXi Shell이 비활성화되어 있는 경우

취약

ESXi Shell이 활성화되어 있는 경우

진단 방법

[CLI]

■ ESXi Shell 사용 여부 확인

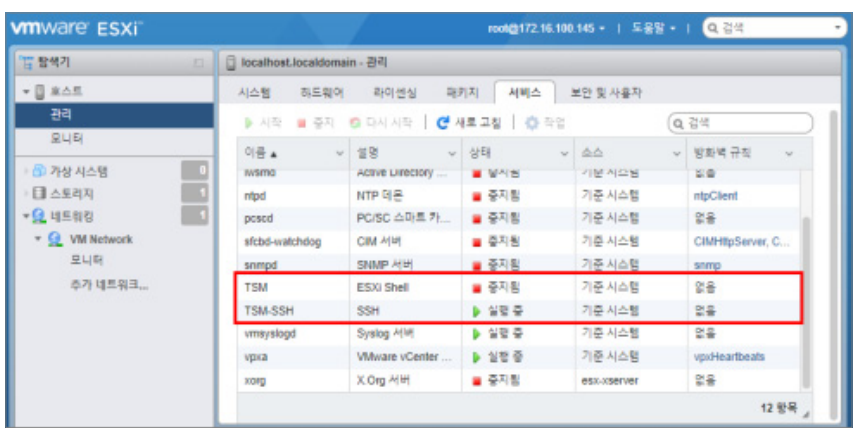
/etc/init.d/ESXShell status 입력 후 ESXi Shell 활성화 여부 확인

```
[root@localhost:~] /etc/init.d/ESXShell status
ESX shell login is enabled
```

[vClient]

■ ESXi Shell 사용 여부 확인 (ESXi 6.x 기준)

vClient 실행 → ESXi 호스트 → 관리 → 서비스 → TSM과 TSM-SSH 항목의 상태 확인



조치 방법

[CLI]

■ ESXi Shell 사용하지 않을 경우, 사용 제한 설정

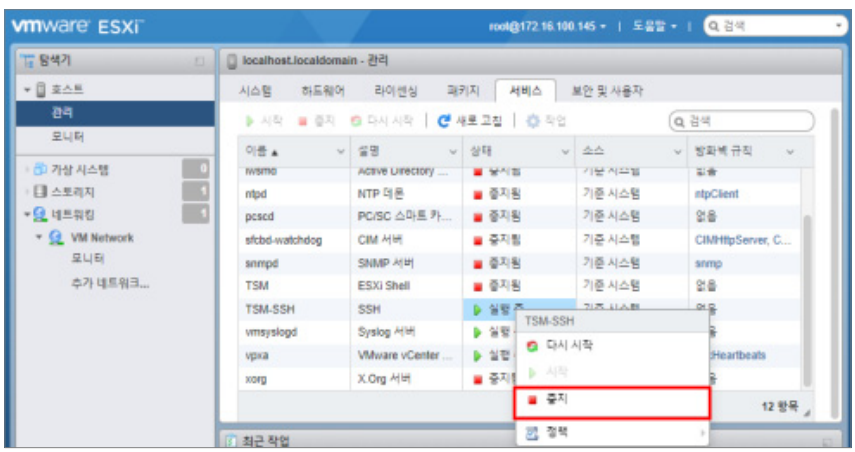
/etc/init.d/ESXShell ESXi Shell 비활성화

```
[root@localhost:~] /etc/init.d/ESXShell status
ESX shell login is disabled
```

[vClient]

■ ESXi Shell 사용하지 않을 경우, 사용 제한 설정 (ESXi 6.x 기준)

vClient 실행 → ESXi 호스트 → 관리 → 서비스 → TSM과 TSM-SSH 항목을 오른쪽 클릭하여 "중지"



ESXi Shell 자동 종료

항목설명

ESXi Shell은 기본적으로 사용하지 않도록 설정되어 있으나 Shell을 사용한 후 Shell을 닫는 것을 잊을 수 있다. 이때 ESXi Shell의 가용성 시간 초과를 설정하여 보안을 강화할 수 있다.

진단 기준

양호

ESXi Shell 시간 초과 설정이 적용된 경우

취약

ESXi Shell 시간 초과 설정이 적용되지 않은 경우

진단 방법

[CLI]

■ ESXi Shell 시간 초과 설정 확인

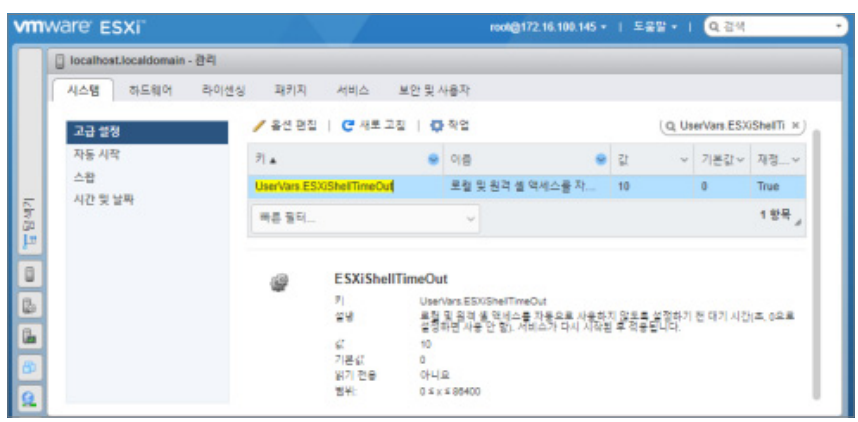
esxcli system settings advanced list –o "/UserVars/ESXiShellTimeOut" 입력 후 Int Value 값 확인

```
[root@localhost:~] esxcli system settings advanced list -o "/UserVars/ESXiShellTimeOut
"
   Path: /UserVars/ESXiShellTimeOut
   Type: integer
   Int Value: 0
   Default Int Value: 0
   Min Value: 0
   Max Value: 86400
   String Value:
   Default String Value:
   Valid Characters:
   Description: Time before automatically disabling local and remote shell access (in
seconds, 0 disables).  Takes effect after the services are restarted.
```

[vClient]

■ ESXi Shell 시간 초과 설정 확인 (ESXi 6.x 기준)

vClient 실행 → 호스트 → 관리 → 시스템 → 고급설정 → UserVars.ESXiShellTimeOut에서 시간 확인



조치 방법

[CLI]

■ ESXi Shell 시간 초과 설정

esxcli system settings advanced set –o /UserVars/ESXiShellTimeOut –i 〈원하는_대기시간_분 단위〉

변경된 설정이 적용되도록 ESXi 호스트를 다시 부팅하거나, 변경된 설정을 즉시 적용하려면 다음 명령어 사용

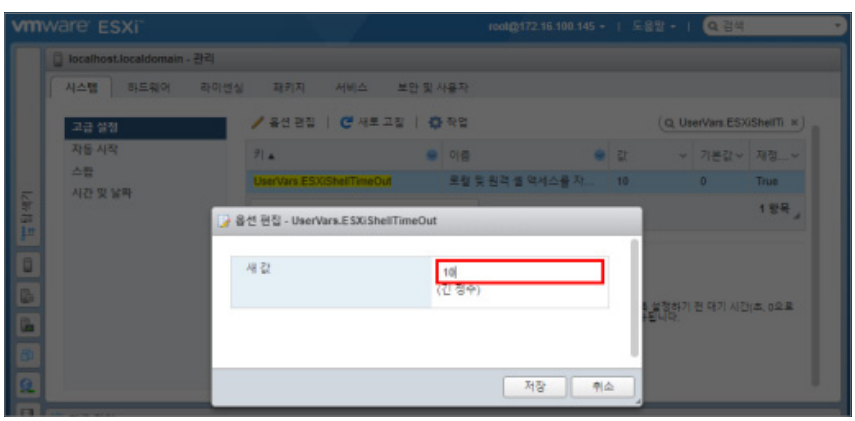
esxcli hardware reboot

```
[root@localhost:~] esxcli system settings advanced set -o /UserVars/ESXiShellTimeOut -
i 10
[root@localhost:~] esxcli system settings advanced list -o "/UserVars/ESXiShellTimeOut
"
   Path: /UserVars/ESXiShellTimeOut
   Type: integer
   Int Value: 10
   Default Int Value: 0
   Min Value: 0
   Max Value: 86400
   String Value:
   Default String Value:
   Valid Characters:
   Description: Time before automatically disabling local and remote shell access (in
seconds, 0 disables).  Takes effect after the services are restarted.
```

[vClient]

■ ESXi Shell 시간 초과 설정 (ESXi 6.x 기준)

vClient 실행 → 호스트 → 관리 → 시스템 → 고급설정 → UserVars.ESXiShellTimeOut에서 시간 변경(10분)



ESXi Shell 및 SSH 세션 타임아웃 설정

항목설명

사용자가 호스트에서 ESXi Shell SSH를 사용하고 로그아웃하는 것을 잊는 경우 유휴 세션이 무기한 연결 상태로 유지되며, 유휴 세션을 통해 호스트의 액세스 권한을 획득하는 악의적인 사용자가 발생할 수 있다. ESXi Shell 및 SSH 세션 타임아웃 설정을 통하여 ESXi 호스트에서 사용자가 일정 시간 동안 활동하지 않으면 해당 세션을 자동으로 종료하도록 한다.

진단 기준

양호
세션 타임아웃 설정이 적용된 경우

취약
세션 타임아웃 설정이 적용되지 않은 경우

진단 방법

[CLI]

■ 세션 타임아웃 설정 확인

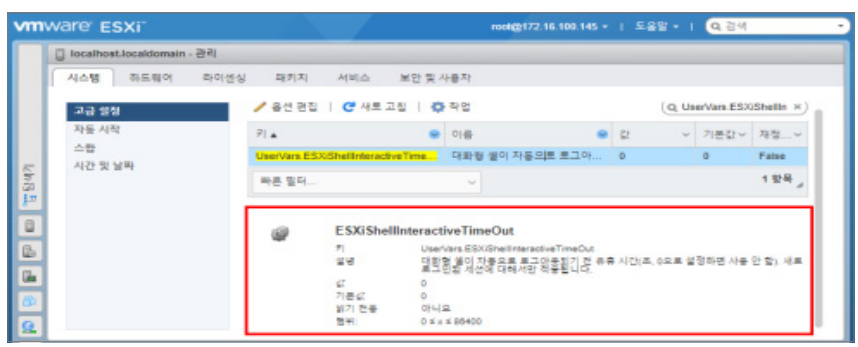
esxcli system settings advanced list –o "/UserVars/ESXiShellInteractiveTimeOut" 입력 후 Int Value 값 확인 (초 단위)

```
[root@localhost:~] esxcli system settings advanced list -o "/UserVars/ESXiShellInterac
tiveTimeOut"
   Path: /UserVars/ESXiShellInteractiveTimeOut
   Type: integer
   Int Value: 0
   Default Int Value: 0
   Min Value: 0
   Max Value: 86400
   String Value:
   Default String Value:
   Valid Characters:
   Description: Idle time before an interactive shell is automatically logged out (in
seconds, 0 disables).  Takes effect only for newly logged in sessions.
```

[vClient]

■ 세션 타임아웃 설정 확인 (ESXi 6.x 기준)

vClient 실행 → 호스트 → 관리 → 시스템 → 고급설정 → UserVars.ESXiShellInteractiveTimeOut에서 시간 확인



※ /UserVars/ESXiShellInteractiveTimeOut: 대화형 ESXi Shell 세션의 타임아웃을 설정

조치 방법

[CLI]

■ 세션 타임아웃 설정

esxcli system settings advanced set –o "/UserVars/ESXiShellInteractiveTimeOut" –i 600 (초 단위) 입력

```
[root@localhost:~] esxcli system settings advanced set -o "/UserVars/ESXiShellInteract
iveTimeOut" -i 600
[root@localhost:~] esxcli system settings advanced list -o "/UserVars/ESXiShellInterac
tiveTimeOut"
   Path: /UserVars/ESXiShellInteractiveTimeOut
   Type: integer
   Int Value: 600
   Default Int Value: 0
   Min Value: 0
   Max Value: 86400
   String Value:
   Default String Value:
   Valid Characters:
   Description: Idle time before an interactive shell is automatically logged out (in
seconds, 0 disables).  Takes effect only for newly logged in sessions.
```

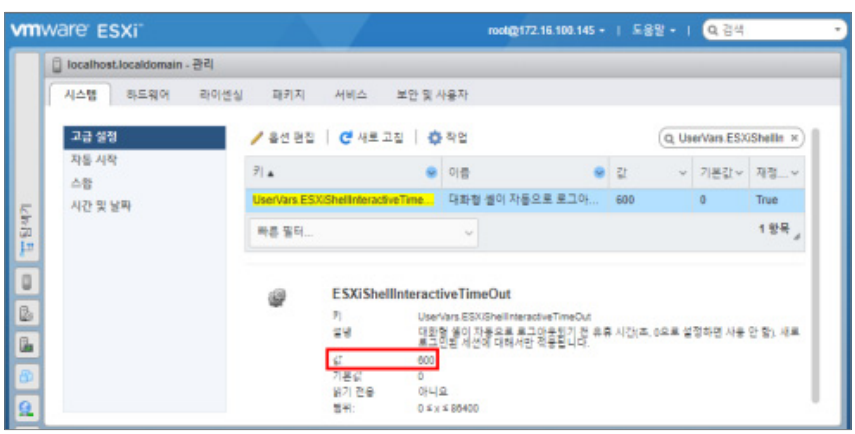
변경된 설정이 적용되도록 ESXi 호스트를 다시 부팅하거나, 변경된 설정을 즉시 적용하려면 다음 명령어를 사용함

esxcli hardware reboot

[vClient]

■ ESXi Shell 시간 초과 설정 (ESXi 6.x 기준)

vClient 실행 → 호스트 → 관리 → 시스템 → 고급설정 → UserVars.ESXiShellInteractiveTimeOut에서 시간 설정 (초 단위)



가상스위치 MAC 주소 변경정책 설정

항목설명

가상 시스템 운영체제에서 MAC 주소가 변경 가능할 경우, 인증된 네트워크 어댑터를 가장하여 네트워크 장치에 악의적인 공격을 수행할 수 있다.

진단 기준

양호

가상스위치의 MAC 주소 변경정책이 거부로 되어있는 경우

취약

가상스위치의 MAC 주소 변경정책이 허용으로 되어있는 경우

진단 방법

[CLI]

■ 가상스위치 MAC 주소 변경정책 확인

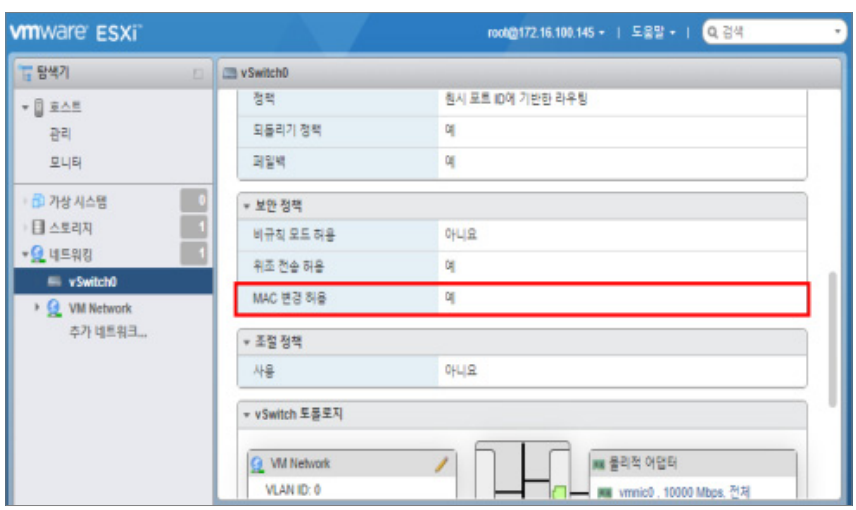
esxcli network vswitch standard policy security get –v "vSwitch0"(가상스위치 이름) 입력 후 MAC Address Change 값 확인

```
[root@localhost:~] esxcli network vswitch standard policy security get -v "vSwitch0"
   Allow Promiscuous: false
   Allow MAC Address Change: true
   Allow Forged Transmits: true
```

[vClient]

■ 가상스위치 MAC 주소 변경정책 확인 (ESXi 6.x 기준)

vClient 실행 → 호스트 → 네트워킹 → vSwitch0 → 보안 정책 → MAC 변경 허용 값 확인



조치 방법

[CLI]

■ 가상스위치 MAC 주소 변경정책 설정

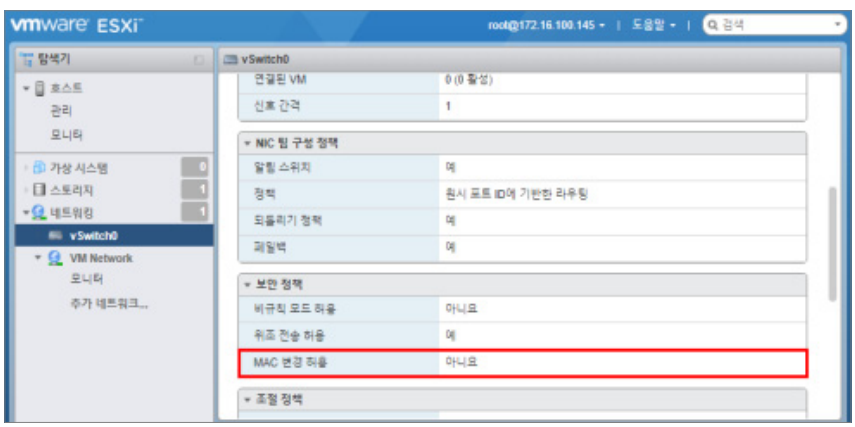
esxcli network vswitch standard policy security set –v vSwitch0(가상스위치 이름) –m false 입력

```
[root@localhost:~] esxcli network vswitch standard policy security set -v vSwitch0 -m
false
[root@localhost:~] esxcli network vswitch standard policy security get -v "vSwitch0"
   Allow Promiscuous: false
   Allow MAC Address Change: false
   Allow Forged Transmits: true
```

[vClient]

■ 가상스위치 MAC 주소 변경정책 설정 (ESXi 6.x 기준)

vClient 실행 → 호스트 → 네트워킹 → vSwitch0 → 보안 정책 → MAC 변경 허용 값 “아니요” 변경



가상스위치 Promiscuous 모드 정책 설정

항목설명

가상스위치에서 Promiscuous 모드가 허용으로 설정되어 있으면, 해당 가상 스위치에 연결된 가상 머신들이 네트워크 트래픽을 모니터링할 수 있다. 그러나 악의적인 사용자가 해당 스위치를 통해 네트워크 트래픽을 감시하거나 캡처할 수 있으므로 보안 정책 및 요구사항을 준수하여 설정해야 한다.

진단 기준

양호

가상스위치의 Promiscuous 모드 정책이 거부로 되어있는 경우

취약

가상스위치의 Promiscuous 모드 정책이 허용으로 되어있는 경우

진단 방법

[CLI]

■ 가상스위치 Promiscuous 모드 정책 확인

esxcli network vswitch standard policy security get -v "vSwitch0(가상스위치 이름)" 입력 후 Promiscuous Mode 속성 확인

```
[root@localhost:~] esxcli network vswitch standard policy security get -v "vSwitch0"
   Allow Promiscuous: false
   Allow MAC Address Change: false
   Allow Forged Transmits: true
```

[vClient]

■ 가상스위치 Promiscuous 모드 정책 확인 (ESXi 6.x 기준)

vClient 실행 → 호스트 → 네트워킹 → vSwitch0 → 보안 정책 → "비규칙 모드 허용" 값 확인

조치 방법

[CLI]

■ 가상스위치 Promiscuous 모드 정책 변경

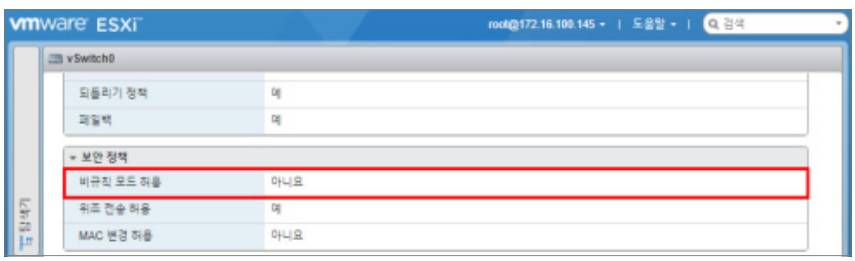
esxcli network vswitch standard policy security set –v "vSwitch0(가상스위치 이름)" –p false 입력

```
[root@localhost:~] esxcli network vswitch standard policy security get -v "vSwitch0"
   Allow Promiscuous: false
   Allow MAC Address Change: false
   Allow Forged Transmits: true
```

[vClient]

■ 가상스위치 Promiscuous 모드 정책 변경 (ESXi 6.x 기준)

vClient 실행 → 호스트 → 네트워킹 → vSwitch0 → 보안 정책 → "비규칙 모드 허용" 값을 "아니요" 변경



가상스위치 Forged Transmits 모드 정책 설정

항목설명

가상 시스템 운영체제에서 가상스위치 Forged Transmits 모드가 허용되어 있으면 인증된 네트워크 어댑터를 가장하여 네트워크 장치에 악의적인 공격을 수행할 수 있다.

진단 기준

양호

가상스위치의 Forged Transmits 정책이 거부로 설정된 경우

취약

가상스위치의 Forged Transmits 정책이 허용으로 설정된 경우

진단 방법

[CLI]

■ 가상스위치 Forged Transmits 모드 정책 확인

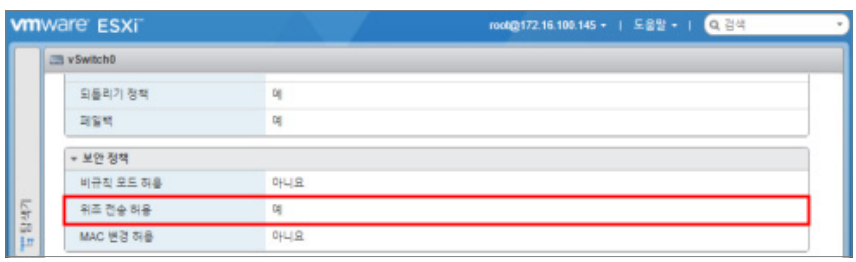
esxcli network vswitch standard policy security get –v "vSwitch0"(가상스위치 이름) 입력 후 Forged Transmits 값 확인

```
[root@localhost:~] esxcli network vswitch standard policy security get -v "vSwitch0"
   Allow Promiscuous: false
   Allow MAC Address Change: false
   Allow Forged Transmits: true
```

[vClient]

■ 가상스위치 Forged Transmits 모드 정책 확인 (ESXi 6.x 기준)

vClient 실행 → 호스트 → 네트워킹 → vSwitch0 → 보안 정책 → "위조 전송 허용" 값 확인



조치 방법

[CLI]

■ 가상스위치 Forged Transmits 모드 정책 변경

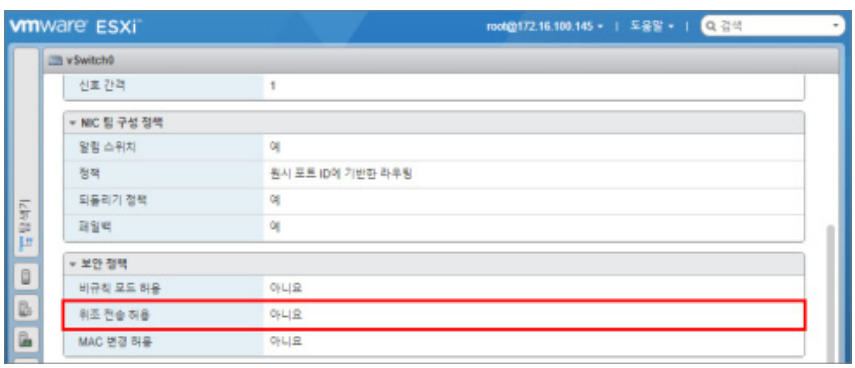
esxcli network vswitch standard policy security set –v "vSwitch0(가상스위치 이름)" –f false 입력

```
[root@localhost:~] esxcli network vswitch standard policy security set -v vSwitch0 -f
false
[root@localhost:~] esxcli network vswitch standard policy security get -v "vSwitch0"
   Allow Promiscuous: false
   Allow MAC Address Change: false
   Allow Forged Transmits: false
```

[vClient]

■ 가상스위치 Forged Transmits 모드 정책 변경 (ESXi 6.x 기준)

vClient 실행 → 호스트 → 네트워킹 → vSwitch0 → 보안 정책 → “위조 전송 허용“ 값을 ”아니요“ 변경



SSH 데몬 빈암호 사용 인증 허용 제한

항목설명

ESXi에서 SSH 데몬을 구성하여 빈 암호를 사용한 인증을 허용하거나 제안하기 위해서는 SSH 서버의 설정과 관련이 있으며, 빈 암호 인증을 허용할 경우 공격자가 패스워드 인증 없이 시스템에 침투할 수 있다.

진단 기준

양호

etc/ssh/sshd_config 설정에 PermitEmptyPasswords 설정이 없거나 no인 경우

취약

/etc/ssh/sshd_config 설정에 PermitEmptyPasswords 설정이 yes인 경우

진단 방법

■ ssh 빈 암호 인증 허용 사용 여부 확인 (ESXi 6.x 기준)

cat /etc/ssh/sshd_config | grep PermitEmptyPasswords 입력 후 PermitEmptyPasswords 값 확인

```
[root@localhost:~] cat /etc/ssh/sshd_config | grep PermitEmptyPasswords
PermitEmptyPasswords yes
```

조치 방법

■ ssh 빈 암호 인증 허용 사용 제한 설정

1. vi 편집기를 이용하여 /etc/ssh/sshd_config 파일을 연 후
   # vi /etc/ssh/sshd_config
2. 아래와 같이 설정 변경
   PermitEmptyPasswords no

```
PermitRootLogin yes

PermitEmptyPasswords no

PrintMotd yes
PrintLastLog no
```

SNMP 서비스 확인

항목설명

SNMP를 사용할 경우 모니터링 정보를 악의적인 호스트로 보내고 해당 정보를 이용하여 공격을 계획할 수 있으므로 불필요한 경우는 비활성화하도록 한다.

진단 기준

양호
불필요한 SNMP가 비활성화되어 있는 경우

취약
불필요한 SNMP가 활성화되어 있는 경우

진단 방법

[CLI]

■ SNMP 활성화 여부 확인

esxcli system snmp get | grep Enable 입력 후 Enable 값 확인

```
[root@localhost:~] esxcli system snmp get | grep Enable
   Enable: false
```

[vClient]

■ SNMP 활성화 여부 확인

vClient 실행 → 호스트 → 관리 → 서비스 → SNMP 검색 (ESXi 6.x 기준)

조치 방법

[CLI]

■ SNMP 비활성화 설정

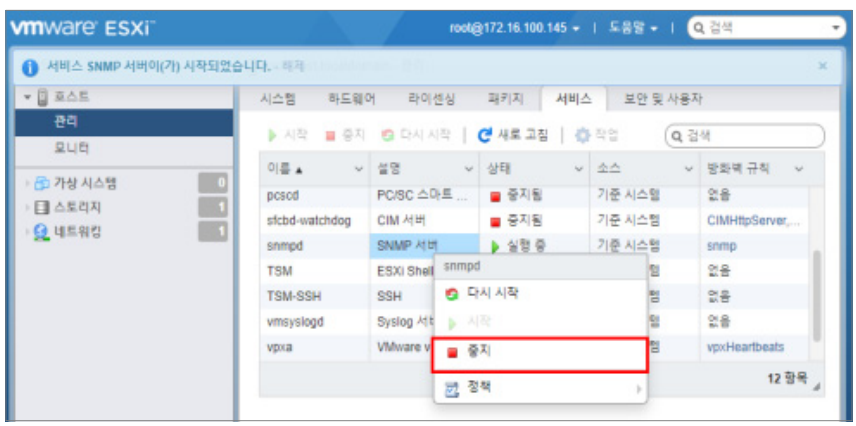
esxcli system snmp set –e no 입력

```
[root@localhost:~] esxcli system snmp set -e no
[root@localhost:~] esxcli system snmp get | grep Enable
   Enable: false
```

[vClient]

■ SNMP 비활성화 설정

vClient 실행 → 호스트 → 관리 → 서비스 → SNMP 중지 (ESXi 6.x 기준)



SNMP Community String 복잡성 설정

항목설명

SNMP에서 community string은 SNMP(데몬)와 클라이언트가 데이터를 교환하기 전에 인증하는 일종의 패스워드로써 초기값으로 설정된 Public, Private과 같은 SNMP default community string을 이용할 경우 해당 장비의 routing table, MAC address 등의 중요한 정보가 외부로 노출될 가능성이 존재한다.
이를 그대로 사용하는 것은 패스워드를 사용하지 않는 계정을 사용하는 것 이상 위험함에도 불구하고 대부분 시스템, 네트워크 관리자들이 기본적인 문자열인 public을 그대로 사용하거나 다른 문자열로 변경을 해도 상호나 monitor, router, mrtg 등 사회 공학적으로 추측할 수 있는 문자열을 사용하고 있어 문제가 되고 있다.

진단 기준

양호

SNMP Community String에 추측 가능한 문자열을 사용하고 있지 않은 경우

취약

SNMP Community String에 추측 가능한 문자열을 사용하고 있는 경우

진단 방법

■ Community String 값 확인

esxcli system snmp get | grep Communities 입력 후 Communities 값 확인

```
[root@localhost:~] esxcli system snmp get | grep Communities
   Communities:
```

조치 방법

■ Community String 값 변경

esxcli system snmp set –c “수정할 Community String 값” 입력

```
[root@localhost:~] esxcli system snmp set -c test!@#123
[root@localhost:~] esxcli system snmp get | grep Communities
   Communities: test!@#123
```

접속 IP 및 포트 제한

항목설명

ESXi 시스템이 제공하는 SSH, FTP 등 많은 네트워크 서비스를 통한 외부 비인가자의 불법적인 접근 및 시스템 침해사고를 방지하기 위하여 Firewall을 통해 제한된 IP 주소에서만 접속할 수 있도록 설정한다.

진단 기준

양호

원격접속 가능한 서비스에 IP 제한 설정이 적용된 경우

취약

원격접속 가능한 서비스에 IP 제한 설정이 적용되지 않은 경우

진단 방법

[CLI]

■ firewall 설정 확인

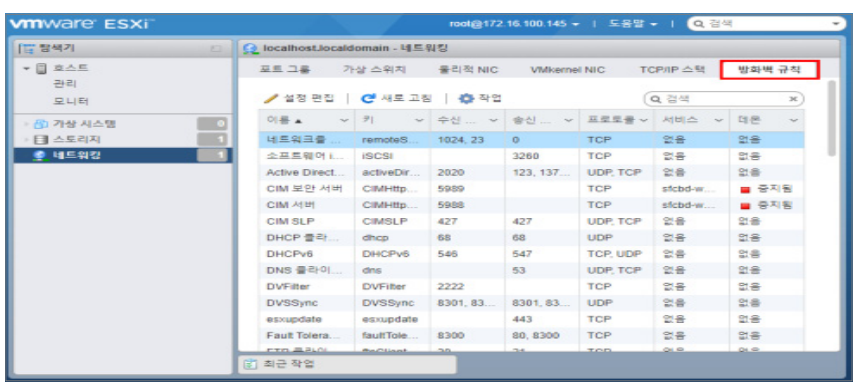
esxcli network firewall ruleset allowedip list 입력 후 IP 제한 설정 확인

```
[root@localhost:~] esxcli network firewall ruleset allowedip list
Ruleset                Allowed IP Addresses
---------------------  --------------------
sshServer              All
sshClient              All
nfsClient              All
nfs41Client            All
dhcp                   All
dns                    All
snmp                   All
ntpClient              All
CIMHttpServer          All
CIMHttpsServer         All
CIMSLP                 All
iSCSI                  All
vpxHeartbeats          All
updateManager          All
faultTolerance         All
webAccess              All
vMotion                All
vSphereClient          All
activeDirectoryAll     All
```

[vClient]

■ firewall 설정 확인

vClient 실행 → 호스트 → 네트워킹 → 방화벽 규칙 → 서비스별 IP 제한 설정 확인



조치 방법

[CLI]

■ 서비스별 허용할 IP 설정

1. 해당 서비스에서 모든 IP 차단
   # esxcli network firewall ruleset set --ruleset-id sshServer --allowed-all false 입력

```
[root@localhost:~] esxcli network firewall ruleset set --ruleset-id sshServer --allowed-all f
alse
```

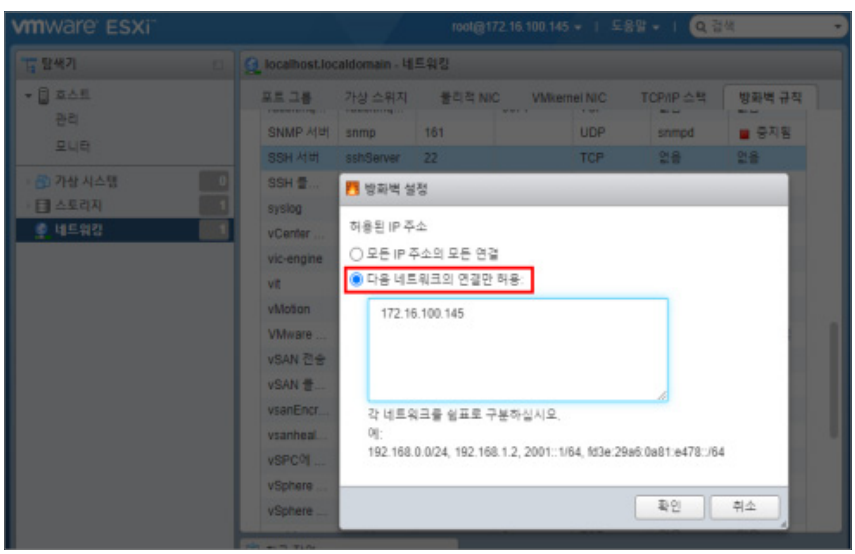
2. 허용할 IP 설정
   # esxcli network firewall ruleset allowedip add --ruleset-id sshServer --ip-address IP 주소 또는 대역 입력

```
[root@localhost:~] esxcli network firewall ruleset allowedip add --ruleset-id sshServer --ip-
address 172.16.100.145
```

[vClient]]

■ 서비스별 허용할 IP 설정

vClient 실행 → 설정 → 보안 프로파일 → Firewall → 속성에서 각 서비스별 IP 제한 설정



※ ESXi Shell에서 IP 제한 설정 시 설정할 서비스에서 모든 IP에 대해 deny 설정 후 허용할 IP 설정

FTP 비활성화

항목설명

불필요한 FTP가 활성화되어 있는 경우, 해당 서비스 포트가 외부에서 활성화되어 해커의 침입 경로로 이용될 위험이 있다.

진단 기준

양호

FTP 서비스가 비활성화되어 있는 경우

취약

FTP 서비스가 활성화되어 있는 경우

진단 방법

[CLI]

■ FTP 구동 여부 확인

esxcli network ip connection list에서 21 port의 proftpd 확인

```
[tester@localhost:/etc] esxcli network ip connection list
Proto  Recv Q  Send Q  Local Address                Foreign Address      State        World ID  CC Algo  World Name
-----  ------  ------  ---------------------------  -------------------  -----------  --------  -------  ----------------
tcp         0       0  127.0.0.1:55635              127.0.0.1:80         TIME_WAIT           0
tcp         0       0  127.0.0.1:8307               127.0.0.1:50446      CLOSE_WAIT      71788  newreno  hostd-worker
tcp         0       0  127.0.0.1:50446              127.0.0.1:8307       FIN_WAIT_2      72205  newreno  rhttpproxy-work
tcp         0       0  127.0.0.1:53840              127.0.0.1:80         TIME_WAIT           0
tcp         0       0  192.168.163.128:22           192.168.163.1:52090  ESTABLISHED     66354  newreno  busybox
tcp         0       0  127.0.0.1:8307               127.0.0.1:35627      ESTABLISHED     71786  newreno  hostd-worker
tcp         0       0  127.0.0.1:35627              127.0.0.1:8307       ESTABLISHED     72197  newreno  rhttpproxy-work
tcp         0       0  192.168.163.128:443          192.168.163.1:51145  ESTABLISHED     67118  newreno  rhttpproxy-IO
tcp         0       0  0.0.0.0:21                   0.0.0.0:0            LISTEN         756348  newreno  proftpd
tcp         0       0  127.0.0.1:8307               127.0.0.1:26746      CLOSED          71776  newreno  hostd-worker
tcp         0       0  127.0.0.1:12001              0.0.0.0:0            LISTEN          71567  newreno  hostd-worker
```

※ ESXi 7.x 이상 버전에는 내장된 FTP 서버가 없으며, ESXi 호스트 자체에서 직접 FTP 서버를 실행하는 옵션이 기본적으로 제공되지 않음

조치 방법

[CLI]

■ FTP 구동 중지

/etc/init.d/proftpd stop

```
[tester@localhost:/etc] /etc/init.d/proftpd stop
Stopping proftpd
```

FTP root 접속 설정

항목설명

OS 상에서 사용하는 기타 중요 파일에 대하여 접근 권한을 제한하고 있는지 점검한다. 시스템 운영상 중요한 파일들의 접근 권한은 반드시 필요한 사용자만 접근할 수 있도록 해야 한다.

진단 기준

양호

root로 원격접속이 불가능할 경우

취약

root로 원격접속이 가능할 경우

진단 방법

■ FTP root 접속 설정 확인

cat /etc/proftpd.conf에서 RootLogin확인

```
[tester@localhost:/etc] cat proftpd.conf
# Run the daemon as root and allow root login:
RootLogin off
```

조치 방법

■ FTP root 접속 제한 설정

1. vi 편집기를 이용하여 /etc/proftpd.conf 파일을 연 후
   # vi /etc/proftpd.conf
2. 아래와 같이 설정 변경
   RootLogin off

FTP 기본 디렉터리 경로 확인

항목설명

DefaultRoot를 변경하지 않고 Root 최상위 디렉터리로 사용할 경우, 악의적인 FTP 사용자가 시스템 설정에 접근하여 다운로드 후 2차 공격의 정보로 활용할 수 있는 위험이 존재한다.

진단 기준

양호

DefaultRoot 설정이 변경되어있는 경우

취약

DefaultRoot 설정이 최상위 Root 설정이거나 시스템 설정 디렉터리로 설정되어 있는 경우

진단 방법

■ FTP root 접속 설정 확인

cat /etc/proftpd.conf에서 DefaultRoot확인

```
[tester@localhost:/etc] cat proftpd.conf
# Set the default directory and allow files to be overwritten:
DefaultRoot /
```

조치 방법

■ FTP root 접속 제한 설정

1. vi 편집기를 이용하여 /etc/proftpd.conf 파일을 연 후
   # vi /etc/proftpd.conf
2. 아래와 같이 설정 변경
   DefaultRoot /test(지정할 디렉터리 경로)

NTP 시간 동기화 설정

항목설명

여러 ESXi 호스트 또는 가상머신 간의 정확한 시간 동기화는 가상화 환경에서 매우 중요하다. 정확한 시간 동기화가 없으면 로그, 이벤트 및 시스템 동작의 정확성이 훼손될 수 있다.

진단 기준

양호

NTP 시간 동기화 설정이 적용된 경우

취약

NTP 시간 동기화 설정이 적용되지 않은 경우

진단 방법

[CLI]

■ NTP 활성화 여부 확인

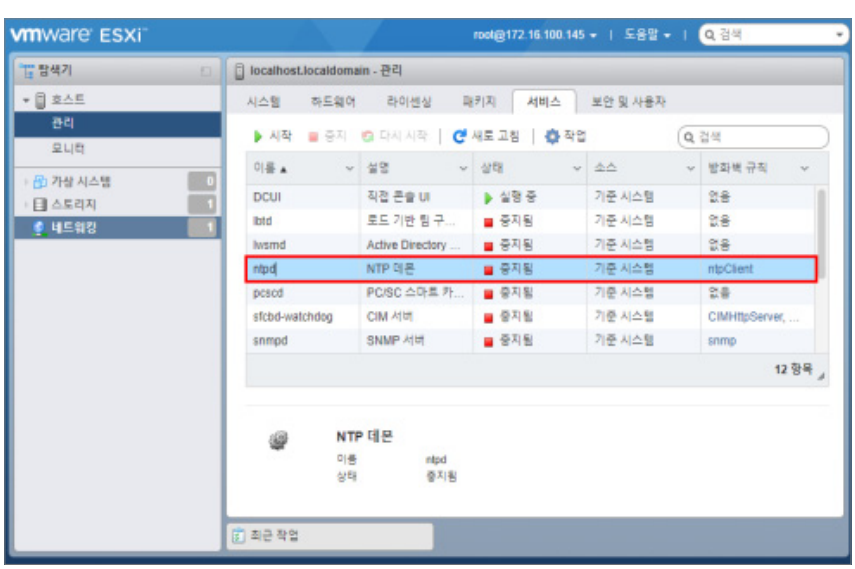
esxcli network ip connection list | grep ntpd 입력 후 ntp 목록 확인

```
[root@localhost:~] esxcli network ip connection list | grep ntpd
udp         0       0  [fe80:2::20c:29ff:fefb:d3d5]:123  [::]:0                  2151703  ntpd
udp         0       0  [fe80:1::1]:123                   [::]:0                  2151703  ntpd
udp         0       0  [::1]:123                         [::]:0                  2151703  ntpd
udp         0       0  172.16.100.145:123                0.0.0.0:0               2151703  ntpd
udp         0       0  127.0.0.1:123                     0.0.0.0:0               2151703  ntpd
udp         0       0  0.0.0.0:123                       0.0.0.0:0               2151703  ntpd
udp         0       0  [::]:123                          [::]:0                  2151703  ntpd
```

[vClient]

■ NTP 활성화 여부 확인

vClient 실행 → 호스트 → 관리 → 서비스 → ntpd 활성화 여부 확인



조치 방법

[CLI]

■ NTP 활성화

vi 편집기를 이용하여 /etc/ntp.conf 파일에서 server time.bora.net(ntp 서버) 설정
vi /etc/ntp.conf

```
restrict default nomodify notrap nopeer noquery
restrict 127.0.0.1
server time.bora.net
driftfile /etc/ntp.drift
```

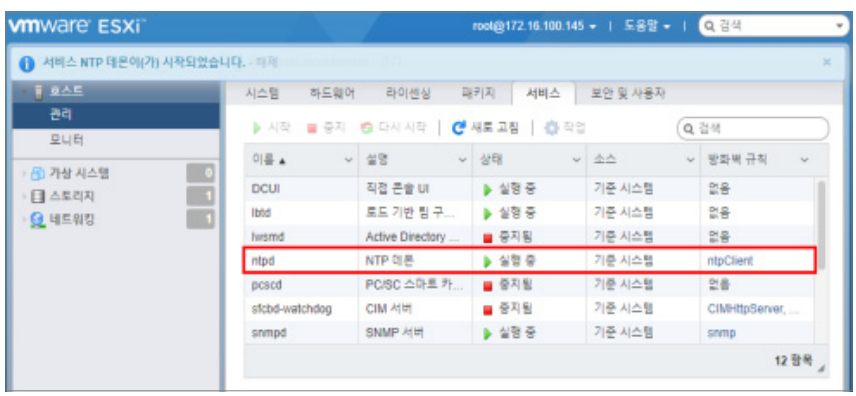
2. NTP 데몬 시작
/etc/init.d/ntpd start

```
[root@localhost:~] /etc/init.d/ntpd start
Starting ntpd
```

[vClient]

■ NTP 활성화

vClient 실행 → 호스트 → 관리 → 서비스 → ntpd 활성화



SSL 시간 초과 구성 설정 확인

항목설명

기본적으로 완전하게 설정된 SSL 연결은 시간제한이 없으므로, 악의적인 사용자가 많은 SSL 연결을 통해 서비스 거부 공격을 시행할 위험이 존재하므로 유휴 연결에 대하여 시간 초과 기간을 설정하여야 한다.

*** 읽기 시간 초과 설정(readTimeoutMs): 데이터 수신에 대한 타임아웃을 설정함. 이는 클라이언트가 서버에서 데이터를 읽는 동안 소요되는 최대 시간을 의미하며 만약 클라이언트가 특정 시간 동안 데이터를 수신하지 않으면 연결이 종료될 수 있음**

*** 핸드셰이크 시간 초과 설정(handshakeTimeoutMs): TCP 핸드셰이크에 대한 타임아웃을 설정함. 즉, 클라이언트가 서버에 연결을 시도하고 핸드셰이크가 완료되기까지의 시간을 제한함.**

진단 기준

양호

SSL 유휴 연결에 대해 시간 초과 기간을 설정한 경우

취약

SSL 유휴 연결에 대해 시간 초과 기간을 설정하지 않은 경우

진단 방법

■ SSL 시간 초과 설정 확인 (ESXi 6.5 이상)

1. config.xml 파일에서 readTimeoutMS, handShakeTimeoutMS 확인
   # cat /etc/vmware/rhttpproxy/config.xml

조치 방법

■ SSL 시간 초과 설정 방법 (ESXi 6.5 이상)

vi 편집기를 이용하여 /etc/vmvare/rhttpproxy/config.xml파일에서 readTimeoutMS, handShakeTimeoutMS 설정

```
〈vmacore〉
  ...
 〈handshakeTimeoutMs〉20000〈/handshakeTimeoutMs〉
  ...
 〈/ssl〉
  ...
〈/vmacore〉
```

2. hostd 재시작
   # /etc/init.d/hostd restart

비고

※ 변경 시에는 성능 및 안정성에 미치는 영향을 고려하여 테스트해야 함

이미지 프로필 및 VIB 승인 레벨 확인

항목설명

* VIB 승인 레벨은 4단계가 있으며 그중 Community Supported 승인 수준은 VMWare 파트사 사와 관계없는 개인이나 회사에서 생성한 VIB를 설치할 수 있도록 한다. Community Supported 수준에서는 디지털 서명이 존재하지 않으므로 기술지원 등을 받을 수 없다.
* VIB: Vsphere Install Bundle로 VMware Update Manager이나 로컬 CLI를 통해 직접 설치하는 ESXi 소프트웨어 패키지를 말한다.

진단 기준

양호

VIB 승인 레벨이 Partner Supported 이상인 경우

취약

VIB 승인 레벨이 Community Supported인 경우

진단 방법

[CLI]

■ 승인 레벨 확인

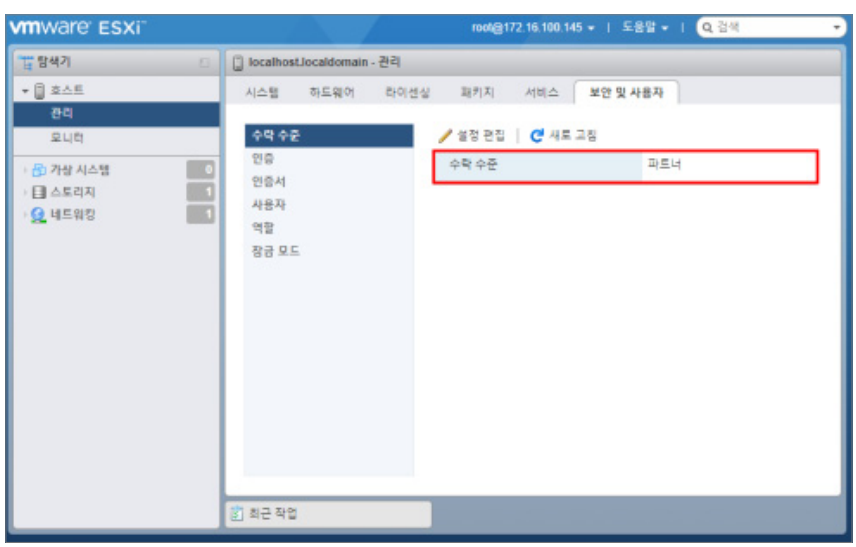
esxcli software acceptance get 입력 후 승인 레벨 확인

```
[root@localhost:~] esxcli software acceptance get
PartnerSupported
```

[vClient]

■ 승인 레벨 확인

vClient 실행 → 구성 → 보안 프로파일 → 호스트 이미지 프로파일 수락 수준에서 확인



조치 방법

[CLI]

■ 승인 레벨 변경

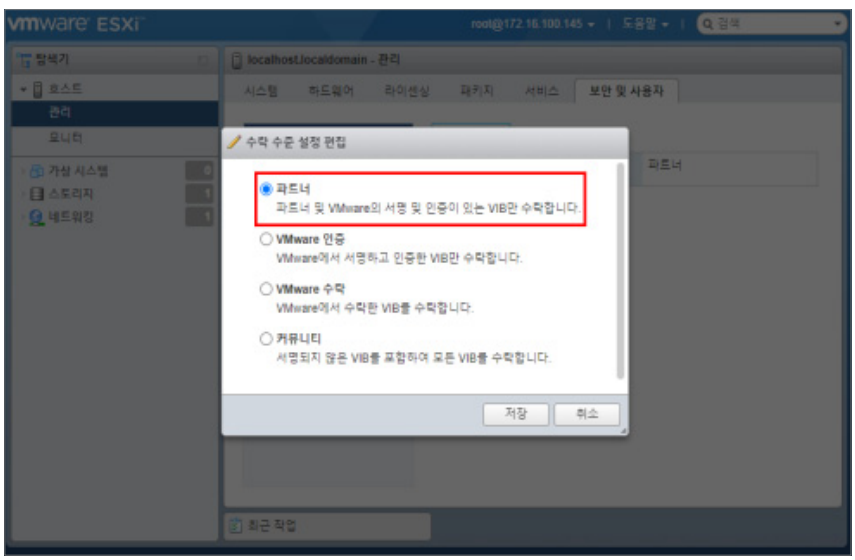
esxcli software acceptance set --level PartnerSupported 입력

```
[root@localhost:~] esxcli software acceptance set --level PartnerSupported
Host acceptance level changed to 'PartnerSupported'.
[root@localhost:~] esxcli software acceptance get
PartnerSupported
```

[vClient]

■ 승인 레벨 변경

vClient 실행 → 호스트 → 관리 → 보안 및 사용자 → 수락 수준 설정 → Edit에서 변경



비고

※ ESXi VIB 수락 수준
- VMwareCerfified: VMWare 사에서 테스트 및 인증한 VIB만 설치 가능
- VMwareAccepted: 파트너사가 테스트하고 VMware사에서 결과를 확인한 VIB 설치 가능
- PartnerSupported: 신뢰하는 파트너사가 테스트 및 결과 학인을 한 VIB 설치 가능
- CommunitySupported: VMware사와 관계없는 개인 및 회사가 생성한 VIB 설치 가능

MOB(Managed Object Browser) 비활성화

항목설명

MOB(Managed Object Browse)는 관리 대상 객체 브라우저로 호스트를 관리하는 데 사용되는 객체 모델을 탐색하는 방법을 제공하지만 동시에 호스트의 설정 구성도 변경이 가능하므로 MOB를 비활성화하는 것이 좋다.

진단 기준

양호

MOB가 비활성화되어 있는 경우

취약

MOB가 활성화되어 있는 경우

진단 방법

[CLI]

■ MOB 활성화 여부 확인

vim-cmd proxysvc/service_list 입력 후 확인

```
(vim.ProxyService.LocalServiceSpec) {
   dynamicType = <unset>,
   serverNamespace = "/guestFile",
   accessMode = "httpsWithRedirect",
   port = 8309,
},
(vim.ProxyService.LocalServiceSpec) {
   dynamicType = <unset>,
   serverNamespace = "/ha-nfc",
   accessMode = "httpAndHttps",
   port = 12001,
},
(vim.ProxyService.LocalServiceSpec) {
   dynamicType = <unset>,
   serverNamespace = "/host",
   accessMode = "httpsWithRedirect",
   port = 8309,
},
(vim.ProxyService.NamedPipeServiceSpec) {
   dynamicType = <unset>,
   serverNamespace = "/mob",
   accessMode = "httpsWithRedirect",
   pipeName = "/var/run/vmware/proxy-mob",
```

조치 방법

[CLI]

■ MOB 비활성화

vim-cmd proxysvc/remove_service "/mob" "httpsWithRedirect" 입력

```
~ # vim-cmd proxysvc/remove_service "/mob" "httpsWithRedirect"
Successfully removed service.
~ #
```

불필요한 서비스 제거

항목설명

서버에 불필요한 서비스의 Port들이 열려 있는 경우 주요 시스템 정보 노출 및 서비스 거부(DOS) 공격이 발생할 수 있다. ESXi를 이용한 클라우드 컴퓨팅 서비스를 위해 서버 관리용으로 SSH와 Vsphere Client를 제공하고 있으며, 클라우드 컴퓨팅 서비스에 불필요한 ftp 등을 사용할 경우 각각의 프로토콜에 대한 취약점으로 인해 root 권한 획득, DoS공격 등 다양한 공격의 대상이 될 수 있다.

진단 기준

양호

불필요한 서비스가 비활성화되어 있는 경우

취약

불필요한 서비스가 활성화되어 있는 경우

진단 방법

■ 오픈된 서비스 확인

esxcli network ip connection list

```
[root@localhost:~] vi /etc/vmware/rhttpproxy/config.xml
tcp           0      0  172.16.100.145:427        0.0.0.0:0          LISTEN      2098852  newreno
tcp           0      0  127.0.0.1:427             0.0.0.0:0          LISTEN      2098852  newreno
tcp           0      0  127.0.0.1:549             0.0.0.0:0          LISTEN      2098491  newreno  rhttp
proxy
tcp           0      0  0.0.0.0:443               0.0.0.0:0          LISTEN      2098491  newreno  rhttp
proxy
tcp           0      0  [::]:443                  [::]:0             LISTEN      2098491  newreno  rhttp
proxy
tcp           0      0  0.0.0.0:80                0.0.0.0:0          LISTEN      2098491  newreno  rhttp
proxy
tcp           0      0  [::]:80                   [::]:0             LISTEN      2098491  newreno  rhttp
proxy
tcp           0      0  127.0.0.1:8303            0.0.0.0:0          LISTEN      2098414  newreno  hostd
CgiServer
tcp           0      0  [::]:9080                 [::]:0             LISTEN      2098257  newreno  ioFil
terVPServer
tcp           0      0  [::]:8000                 [::]:0             LISTEN      2098071  newreno
tcp           0      0  [::]:902                  [::]:0             LISTEN      2098055  newreno  busyb
ox
tcp           0      0  0.0.0.0:902               0.0.0.0:0          LISTEN      2098055  newreno  busyb
ox
tcp           0      0  [::]:8300                 [::]:0             LISTEN      2098043  newreno
udp           0      0  [fe80:2::20c:29ff:fefb:d3d5]:123  [::]:0              2151703           ntpd
udp           0      0  [fe80:1::1]:123           [::]:0                       2151703           ntpd
udp           0      0  [::1]:123                 [::]:0                       2151703           ntpd
```

ESXi 설치 시 기본적으로 열리는 포트			
SSH Server(22)	DNS Client(53)	DHCP Client(68)	SNMP(161)
HTTP(80)	SLPv2(427)	SSL(443)	인증 및 원격접속 프로토콜(902)

조치 방법

■ 서비스 사용 여부 확인 후 비활성화 또는 최신 보안 패치

1. 서비스가 필요한 경우
   최신 보안 패치 적용 버전 설치
2. 서비스가 필요하지 않은 경우
   vClient 실행 → 호스트 → 관리 → 서비스 → 속성에서 필요한 서비스 확인 후 중지

최신 보안패치 및 밴더 권고사항

항목설명

주기적인 패치 적용을 통하여 보안성 및 시스템 안전성을 확보하는 것이 시스템 운용의 중요한 요소이다. 서비스 중인 시스템에서 패치 적용에 따라 발생하는 서비스 영향도를 확인하고 패치 적용 시 많은 부분을 고려해야 한다.

진단 기준

양호

최신 보안 패치가 적용되거나 보안 취약점이 존재하지 않는 버전을 사용하는 경우

취약

보안 취약점이 존재하거나 지원이 종료된 버전을 사용하는 경우

진단 방법

■ 명령어를 통해 버전 확인

esxcli system version get

```
[root@localhost:~] esxcli system version get
   Product: VMware ESXi
   Version: 6.7.0
   Build: Releasebuild-14320388
   Update: 3
   Patch: 73
```

※ 인터뷰를 통해 주기적으로 보안 패치 적용 여부 확인

조치 방법

■ 설정 기준 권고 (또는 정책 기준)

1. 보안 취약점이 발표되면 시스템 영향도를 평가하고, 긴급 대응책 및 중장기 대응책을 마련하여 계획과 허가에 의해 대응하는 것이 좋다.
2. 패치를 수행할 시 시스템의 영향도에 따라 패치를 차등 수행하도록 한다.
3. 시스템 운영에 영향을 주지 않는 범위 내에서 주기적으로 패치를 수행할 것을 권고함

※ 최신 버전을 사용하도록 권고하고 있으나, 시스템 운영상 적용이 어려운 경우 알려진 취약점이 존재하지 않는 버전도 허용하고 있음

비고

※ 보안 패치 적용 시, 시스템 영향도를 파악하여 충분한 테스트 후 적용 권고

로그의 정기적 검토 및 보고

항목설명

로그 관리는 시스템 상태를 모니터링하고 잠재적인 문제를 식별하는 데 핵심적인 부분이므로 주기적으로 로그를 검토하고 분석하여 시스템 침입 흔적과 취약점을 확인할 수 있다.

진단 기준

양호

로그 기록의 검토, 분석, 리포트 작성 및 보고 등이 정기적으로 이루어지고 있는 경우

취약

로그 기록의 검토, 분석, 리포트 작성 및 보고 등이 정기적으로 이루어지지 않는 경우

진단 방법

■ 인터뷰를 통해 정기적인 로그 분석에 대한 결과물 확인

※ 인터뷰를 통해 로그 기록과 보고 및 검토의 주기 확인이 필요함

조치 방법

■ 로그 파일에는 해킹의 흔적들이 남겨져 있을 수 있으므로, 다음과 같이 로그 파일의 백업에 대한 검토 필요

1. 반복적인 로그인 실패에 관한 로그
2. 로그인 거부 메시지에 관한 로그
3. ESXi의 로그 파일은 주로 /var/log 디렉터리에 위치

2.4.

Hyper-V

2.4. Hyper-V

파일 관리(3개 항목), 보안 설정(6개 항목), 패치 관리(1개 항목) 총 3개 영역에서 10개 항목으로 구성된다.

[표 4] Hyper-V 진단 체크리스트

구분	진단 항목
가. 파일 관리	가상 머신 기본 경로 변경
	가상 하드디스크 기본 경로 변경
	Hyper-V 및 가상 컴퓨터 보안 관련 파일
나. 보안 설정	인가된 IP만 접근 가능하도록 설정
	administrator외에 hyper-v 관리자 전용 계정 사용
	WMI 원격실행 제한
	가상OS의 MAC 주소 스푸핑 사용 제한
	가상OS의 DHCP 가드 사용
	가상OS의 라우터 알람 가드 사용
다. 패치 관리	최신 보안 패치 적용

가상 머신 기본 경로 변경

항목설명

가상 머신이 기본 경로로 설정되어 있는 서비스에 비인가자가 해킹에 성공할 경우 시스템 자원을 이용한 침해사고가 발생할 수 있다.

진단 기준

양호

가상 머신 기본 경로를 변경하여 사용하고 있는 경우

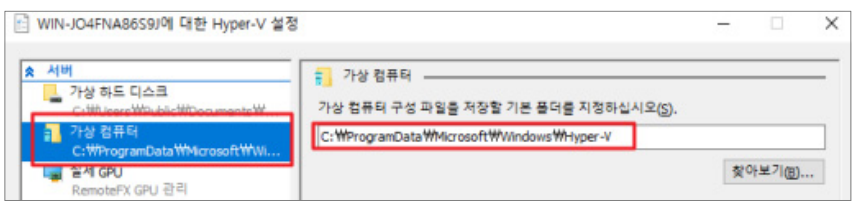
취약

가상 머신 기본 경로를 변경하여 사용하고 있지 않은 경우

진단 방법

■ 가상 머신 기본 경로 확인

1. Hyper-v 관리자 → 해당 가상 OS 작업 → Hyper-v 설정 → 가상 컴퓨터



조치 방법

■ 가상 머신 기본 경로 변경

유추하기 어려운 경로로 폴더를 생성하여 변경

가상 하드디스크 기본 경로 변경

항목설명

가상 하드디스크의 경로가 기본 경로인 서비스에 비인가자가 해킹에 성공할 경우 시스템 자원을 이용한 침해사고가 발생할 수 있다.

진단 기준

양호

패스워드를 복잡하게 설정한 경우

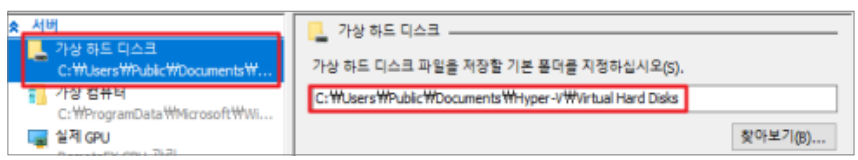
취약

패스워드를 취약하게 설정한 경우

진단 방법

■ 가상 머신 기본 경로 확인

1. Hyper-v 관리자 → 해당 가상 OS 작업 → Hyper-v 설정 → 가상 하드 디스크



조치 방법

■ 가상 머신 기본 경로 변경

유추하기 어려운 경로로 폴더를 생성하여 변경

Hyper-V 및 가상 컴퓨터 보안 관련 파일

항목설명

Hyper-V에 접근할 수 있는 계정 중 Administrator 및 관련 계정 외 불필요한 계정이 존재할 경우 권한 없는 사용자가 시스템에 익명으로 액세스할 수 있으므로 비인가자 접근, 정보 유출 등 보안 위험에 노출 될 수 있다.

진단 기준

양호

가상 머신 및 가상 하드디스크 디렉터리 권한에 Administrator 및 생성한 소유자 외 권한이 존재하지 않을 경우

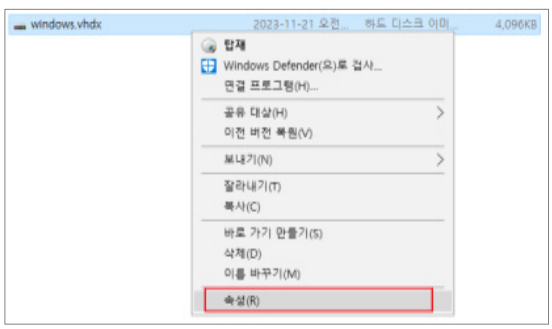
취약

가상 머신 및 가상 하드디스크 디렉터리 권한에 Administrator 및 생성한 소유자 외 권한이 존재할 경우

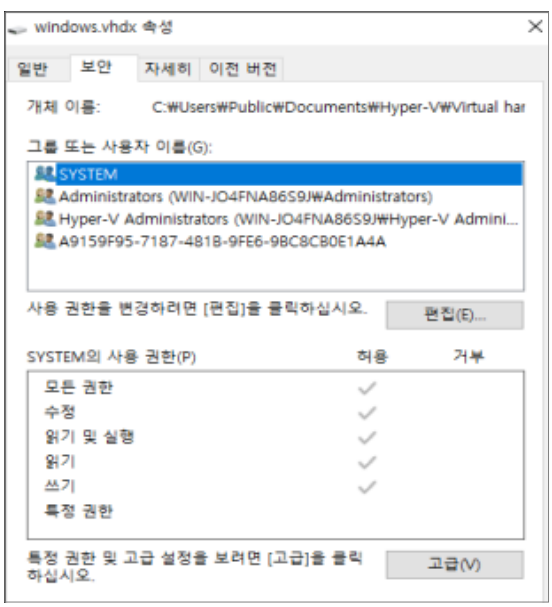
진단 방법

■ Hyper-V 설정 파일의 디렉터리 권한 확인

1. Hyper-v 설정 파일 → 속성

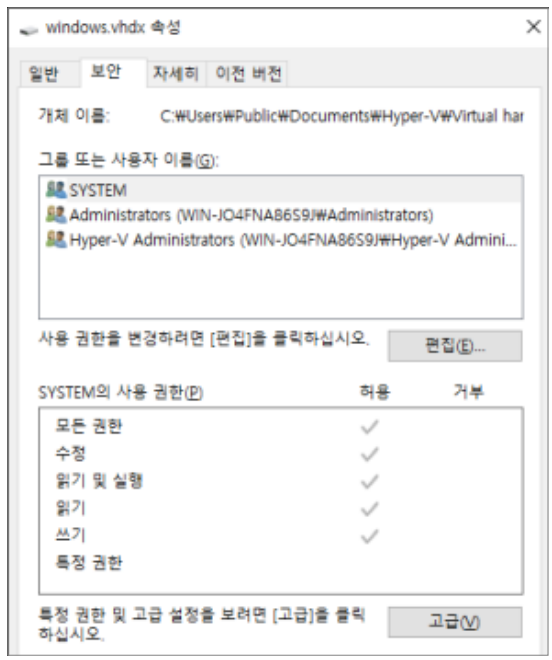


2. 보안 탭에서 계정 별 권한 확인



조치 방법

■ 가상 머신 및 가상 하드디스크 디렉터리 권한에 Administrators 및 생성한 소유자 외의 계정 및 권한 제거



비고

■ 명확하게 파악되지 않은 계정을 삭제하는 경우 해당 계정과 관련한 업무에 장애 발생 가능성이 존재함

인가된 IP만 접근 가능하도록 설정

항목설명

허용할 호스트에 대한 IP 제한이 적용되어 있지 않은 경우 외부 비인가자의 불법적인 접근 및 시스템 침해사고가 발생할 수 있으므로 제한된 IP만 접근 가능하도록 설정한다.

※ WMI(Windows Management Instrumentation)란 윈도우 관리 도구로, Windows 기반 운영 체제에서 데이터 관리 및 작업을 위한 인프라이자 시스템 관리 기술을 의미한다.

진단 기준

양호

WMI 관련 규칙이 활성화 되어 있고 원격 IP주소를 설정한 경우

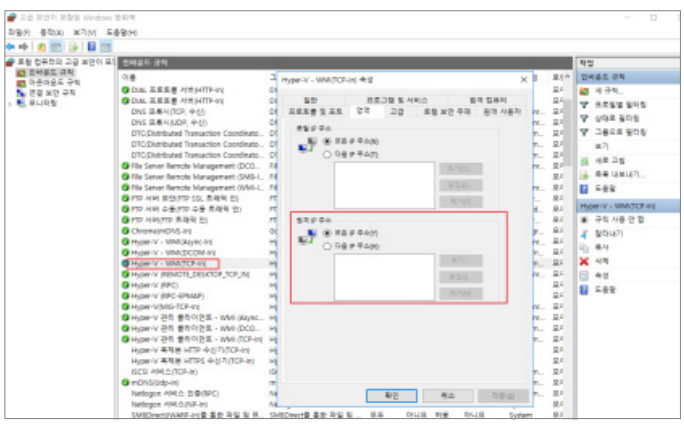
취약

WMI 관련 규칙이 활성화 되어 있지 않거나, 원격 IP주소를 설정하지 않은 경우

진단 방법

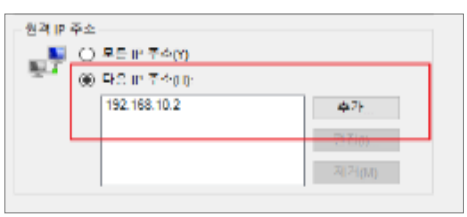
■ Windows 방화벽 내 IP 설정 확인

고급 보안이 포함된 windows 방화벽 → 인/아웃바운드 규칙 → Hyper-V WMI(TCP-in) 정책 → 영역→ 원격 IP주소 확인



조치 방법

■ 인가된 IP만 접근 가능하도록 IP 주소 설정



Administrator외에 Hyper-V 관리자 전용 계정 사용

항목설명

Administrator 계정을 이용하여 Hyper-V를 사용할 경우, 시스템에 제한 없는 권한을 부여 받을 수 있어 시스템에 영향을 미치는 침해 사고가 발생할 수 있으므로 Hyper-V 전용 계정을 사용하여 관리해야 한다.

진단 기준

양호

Administrator 계정으로 Hyper-V를 사용하고 있는 경우

취약

Hyper-V 전용 계정을 부여하여 관리하고 있는 경우

진단 방법

■ 서버 내 계정 목록 확인

net user → 계정 목록 확인

조치 방법

■ Administrator 계정 외 별도의 Hyper-V 계정을 생성하여 Hyper-V를 관리

WMI 원격실행 제한

항목설명

WMI(Windows Management Instrumentation)는 매우 강력한 도구이며, 악의적인 사용자가 시스템에 접근하거나 데이터를 조작할 수 있는 경로를 제공할 수 있다. WMI를 통한 원격 실행이 허용되면, 악성 코드 배포, 데이터 유출, 시스템 통제 권한의 상실 등의 위험이 존재한다.

진단 기준

양호

WMI 그룹 내 불필요한 사용자 및 원격 실행 권한이 존재하지 않은 경우

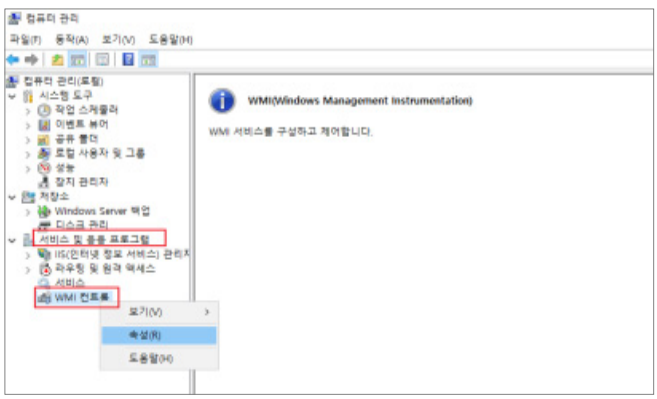
취약

WMI 그룹 내 불필요한 사용자 및 원격 실행 권한이 부여되어 있는 경우

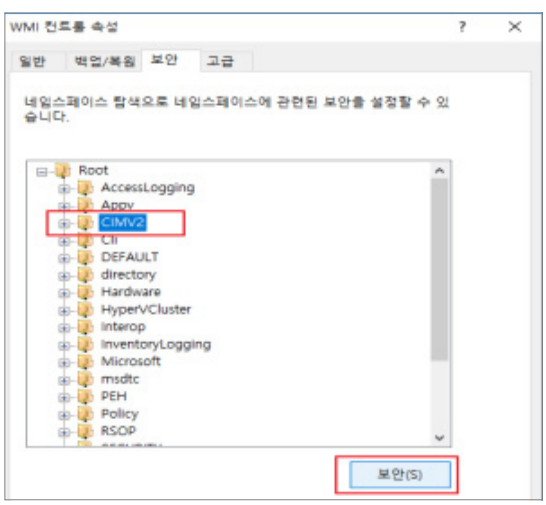
진단 방법

■ 계정 내 원격 사용 설정 확인

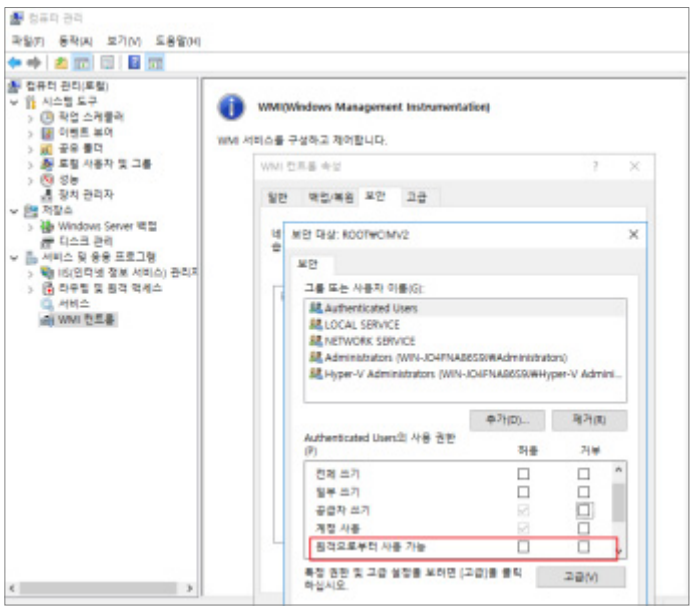
1. 시작 → 관리 도구 → 컴퓨터 관리 → 서비스 및 응용프로그램 → WMI 컨트롤러 → 속성



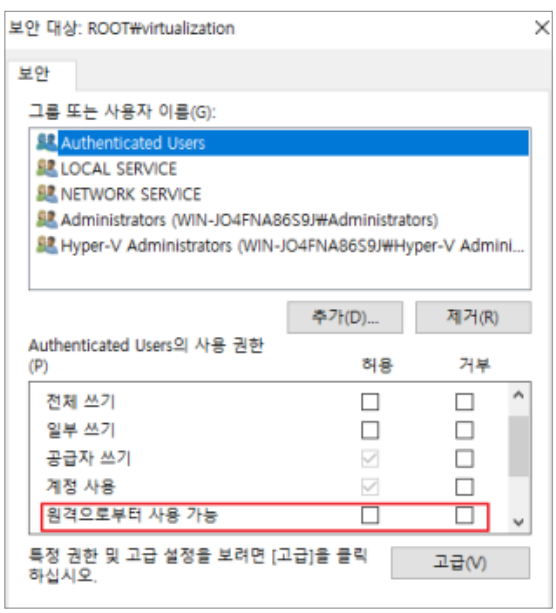
2. WMI 컨트롤 속성의 보안 탭 → Root\CIMV2 → 보안



3. Root\CIMV2 내 그룹 또는 사용자 이름에서 권한 확인

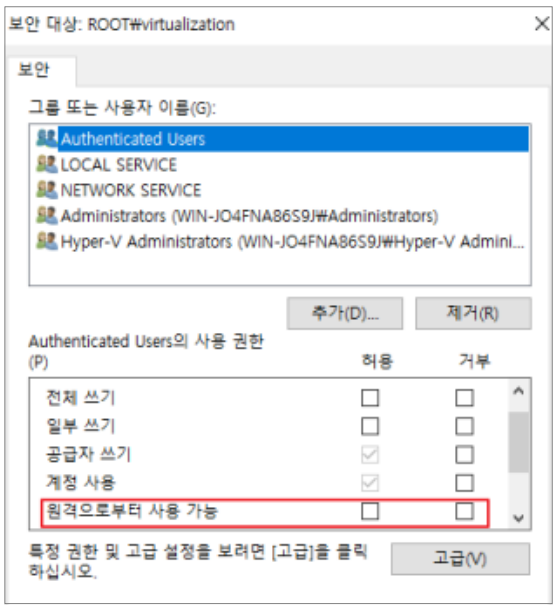


4. WMI 컨트롤 속성의 보안 탭 → Root\virtualization → 보안 → 그룹 또는 사용자 이름에서 권한 확인



조치 방법

■ Root\CIMV2와 Root\virtualization의 불필요한 계정 및 RemoteAccess 권한 제거



가상OS의 MAC 주소 스푸핑 사용 제한

항목설명

MAC 주소란 네트워크 인터페이스에 할당된 물리적 고유 식별 주소이다. MAC 주소는 고유 장비를 식별하는데 사용하며, 악의적 사용자는 MAC 주소 스푸핑을 사용하여 자신의 신원을 숨기고 네트워크 상에서 활동을 익명으로 유지할 수 있다. 이는 민감한 정보에 무단 접근을 허용할 수 있으므로 MAC 주소 스푸핑 사용 기능을 제한해야 한다.

진단 기준

양호

가상OS 내 MAC 주소 스푸핑 사용 기능을 사용하고 있지 않은 경우

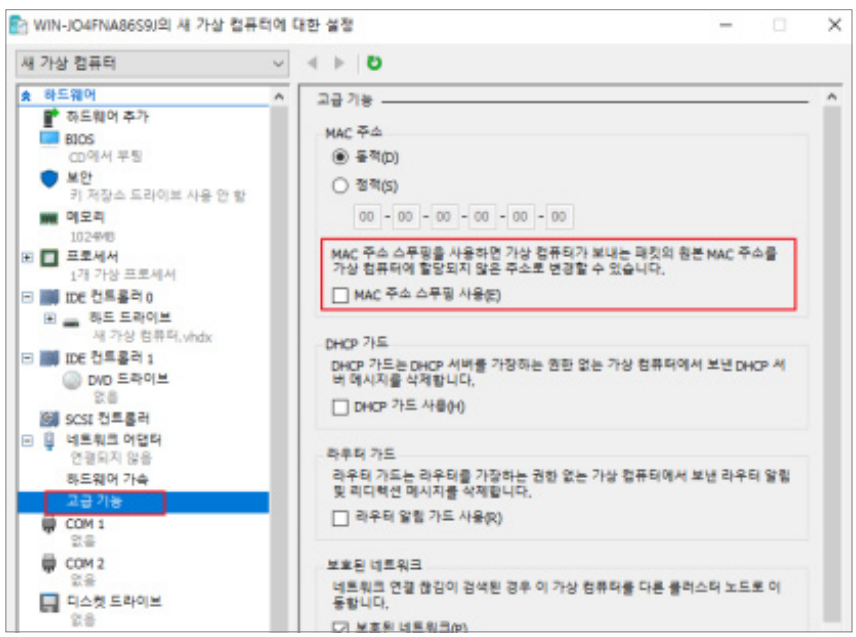
취약

가상OS 내 MAC 주소 스푸핑 사용 기능을 사용하고 있는 경우

진단 방법

■ 가상 OS 내 MAC 주소 스푸핑 사용 기능 확인

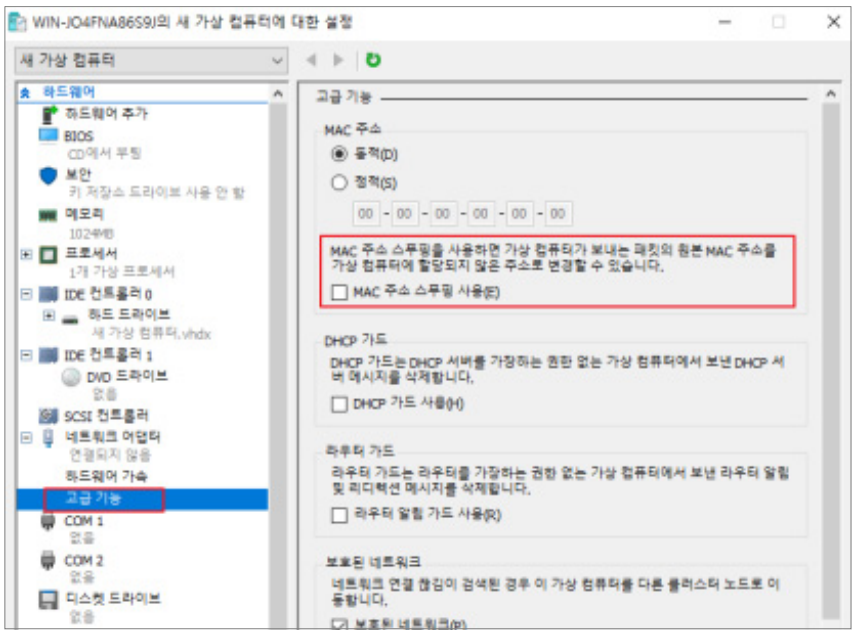
1. Hyper-V 관리자 → 해당 가상 OS 설정 → 네트워크 어댑터 → 고급 기능 → MAC 주소 확인



조치 방법

■ 가상 OS 내 MAC 주소 스푸핑 사용 체크 해제

1. Hyper-V 관리자 → 해당 가상 OS 설정 → 네트워크 어댑터 → 고급 기능 → “MAC 주소 스푸핑 사용” 체크 해제



가상OS의 DHCP 가드 사용

항목설명

DHCP 가드는 네트워크 내에서 무단으로 DHCP 서버가 구동되는 것을 방지한다. 무단 DHCP 서버는 네트워크에 장애를 일으키거나 악의적인 목적으로 사용될 수 있으므로 사전에 제한해야 한다.

진단 기준

양호

가상OS 내 DHCP 가드를 사용하고 있는 경우

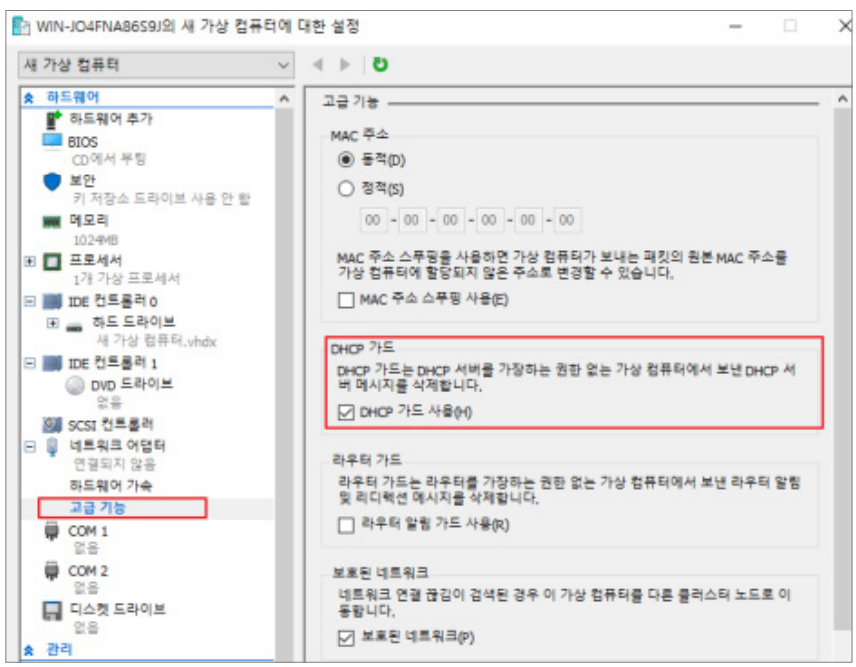
취약

가상OS 내 DHCP 가드를 사용하고 있지 않은 경우

진단 방법

■ 가상 OS 내 DHCP 가드 확인

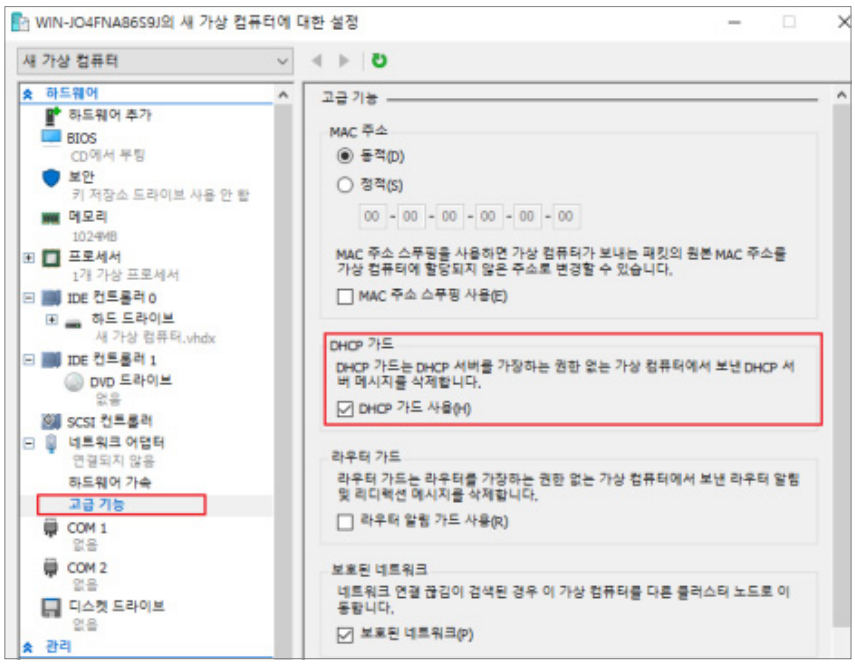
1. Hyper-V 관리자 → 해당 가상 OS 설정 → 네트워크 어댑터 → 고급 기능 → DHCP 가드 확인



조치 방법

■ 가상 OS 내 DHCP 가드 사용

1. Hyper-V 관리자 → 해당 가상 OS 설정 → 네트워크 어댑터 → 고급 기능 → "DHCP 가드 사용" 체크



가상OS의 라우터 알람 가드 사용

항목설명

라우터 알람 가드는 가상 네트워크 내에서 무단 라우터 메시지의 전송을 방지한다. 악의적인 사용자가 무단으로 라우터 알람을 보내 네트워크 트래픽을 가로챌 수 있으므로 해당 기능을 통해 위험을 차단해야 한다.

진단 기준

양호

가상OS 내 라우터 알람 가드 기능을 사용하고 있는 경우

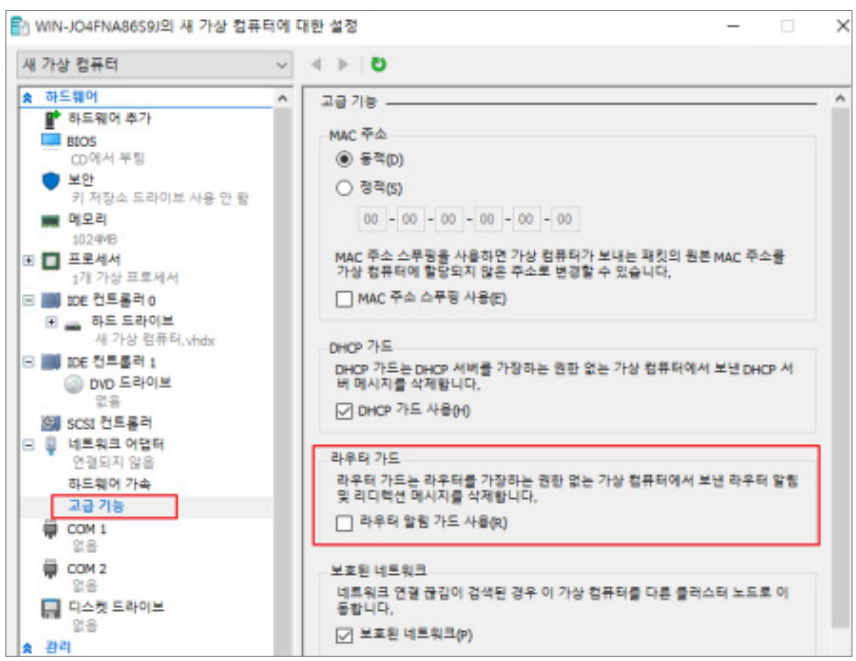
취약

가상OS 내 라우터 알람 가드 기능을 사용하고 있지 않은 경우

진단 방법

■ 가상 OS 내 라우터 가드 확인

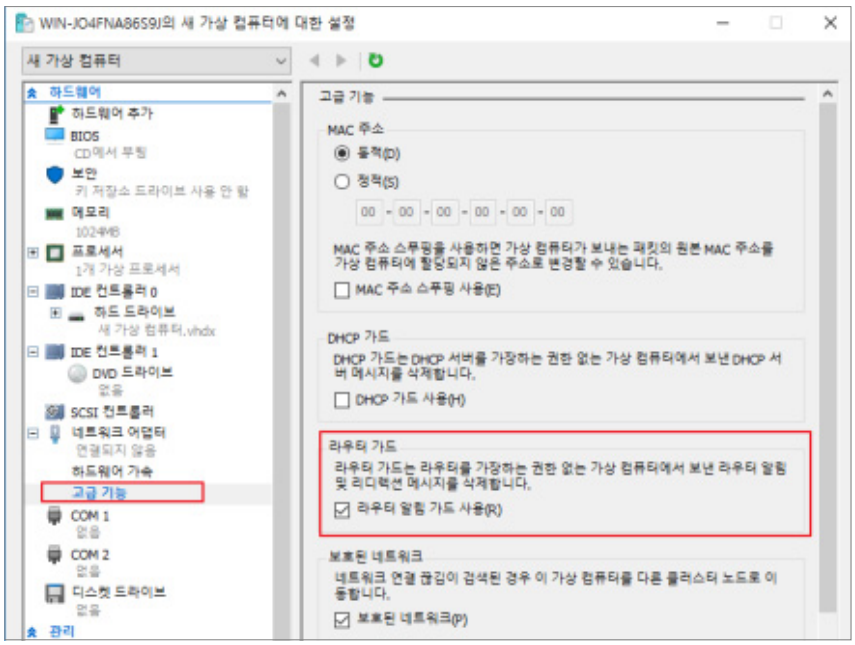
1. Hyper-V 관리자 → 해당 가상 OS 설정 → 네트워크 어댑터 → 고급 기능 → 라우터 가드 확인



조치 방법

■ 가상 OS 내 라우터 알람 가드 사용

1. Hyper-V 관리자 → 해당 가상 OS 설정 → 네트워크 어댑터 → 고급 기능 → “라우터 알람 가드” 체크



최신 보안 패치 적용

항목설명

Hyper-V 취약 버전을 사용할 경우 알려진 취약점을 이용한 공격이나 시스템 정보 탈취가 가능하므로, 최신 보안 버전이 적용된 버전으로 업데이트를 유지해야 한다.

진단 기준

양호

패치 적용 정책을 수립하여 주기적으로 패치를 관리하고 있는 경우

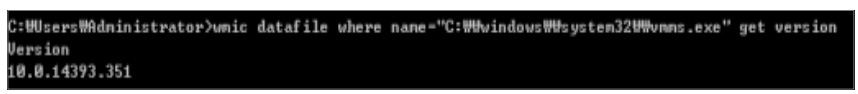
취약

패치 적용 정책을 수립하지 않거나 주기적으로 패치를 관리하고 있지 않은 경우

진단 방법

■ Hyper-V 패치 버전 확인

1. 명령 프롬프트 〉 wmic datafile where name="C:\\windows\\system32\\vmms.exe" get version



조치 방법

■ 알려진 취약점이 조치되어 보안패치가 적용된 버전으로 업그레이드

아래 사이트를 참고하여 적절한 버전의 Hyper-V 설치
https://www.microsoft.com/ko-kr/evalcenter/evaluate-hyper-v-server-2019

비고

시스템 업데이트는 영향도를 산정하여 진행하여야 한다.

2.5.

Server(Linux)

2.5. Server(Linux)

계정 관리(5개 항목), 파일 및 디렉터리 관리(14개 항목), 서비스 관리(15개 항목), 패치 및 로그 관리(2개 항목) 총 4개 영역에서 36개 항목으로 구성된다.

[표 5] Server(Linux) 진단 체크리스트

구분	진단 항목
가. 계정 관리	root 계정 원격 접속 제한
	패스워드 복잡도 설정
	계정 잠금 임계값 설정
	패스워드 최대 사용 기간 설정
	패스워드 파일 보호
나. 파일 및 디렉터리 관리	root 홈, 디렉터리 소유자 설정
	파일 및 디렉터리 소유자 설정
	/etc/passwd 파일 소유자 및 권한 설정
	/etc/shadow 파일 소유자 및 권한 설정
	/etc/hosts 파일 소유자 및 권한 설정
	/etc/(x)inetd.conf 파일 소유자 및 권한 설정
	/etc/syslog.conf 파일 소유자 및 권한 설정
	/etc/services 파일 소유자 및 권한 설정
	SUID, SGID, Sticky bit 설정 파일 점검
	사용자, 시스템 시작파일 및 환경파일 소유자 및 권한 설정
	world writable 파일 점검
	$HOME/.rhosts, hosts.equiv 사용 금지
	접속 IP 및 포트 제한
	cron파일 소유자 및 권한 설정
다. 서비스 관리	Finger 서비스 비활성화
	Anonymous FTP 서비스 비활성화
	r 계열 서비스 비활성화
	DoS 공격에 취약한 서비스 비활성화
	NFS 서비스 비활성화
	NFS 접근통제
	automountd 제거
	RPC 서비스 확인
	NIS, NIS+ 점검
	tftp, talk 서비스 비활성화
	Sendmail 버전 점검
	스팸 메일 릴레이 제한
	일반 사용자의 Sendmail 실행 방지
	DNS 보안 버전 패치
	DNS Zone Transfer 설정
라. 패치 및 로그 관리	최신 보안 패치 및 벤더 권고 사항 적용
	로그의 정기적 검토 및 백업

root 계정 원격 접속 제한

항목설명

root 계정으로 직접 로그인을 하도록 허용하면 불법적인 침입자의 목표가 될 수 있으므로 root 계정 원격 접속을 금지해야 한다. 또한, 일반 사용자 계정 접속 후 관리자 계정으로 변경 시 로그가 남지만, 관리자 계정으로 바로 접속하는 경우 어느 사용자가 접속했는지 알 수 없으므로 문제 발생 시 책임소재 파악이 용이하지 않다.

진단 기준

양호

root 계정의 원격 접속이 제한되어 있는 경우

취약

root 계정의 원격 접속이 제한되어 있지 않은 경우

진단 방법

■ root 계정 telnet 제한 확인

1) pts/0 ~ pts/x 관련 설정 존재 확인
   # cat /etc/securetty

※ CentOS 8, Ubuntu 20.04 이상부터 /etc/securetty 파일이 존재하지 않으며 telnet 비활성화 디폴트 적용

■ root 계정 ssh 제한 확인

1) “PermitRootLogin no”로 설정되어 있는지 확인
   # cat /etc/ssh/sshd_config | grep PermitRootLogin

※ default : #PermitRootLogin yes 주석처리 상태도 취약으로 진단

조치 방법

■ root 계정 telnet 접속 제한 설정

1) /etc/securetty 파일에서 pts/0 ~ pts/x 설정 제거 또는 주석처리

■ root 계정 ssh 접속 제한 설정

1) /etc/ssh/sshd_config 파일에서 PermitRootLogin no 설정

비고

PermitRootLogin 인수	
yes	root 계정 원격 접속 허용
without-password	root 계정 원격 접속 시 패스워드 이증 비활성화
forced-commands-only	root 계정 원격 접속 시 PK 인증 허용
no	root 계정 원격 접속 제한
default(미설정)	root 계정 원격 접속 허용(yes)

패스워드 복잡도 설정

항목설명

패스워드 복잡성 설정이 되어 있지 않은 사용자 계정이 존재할 경우 비인가자가 각종 공격(무작위 대입 공격, 사전 대입 공격 등)을 통해 사용자 계정의 패스워드 탈취가 가능하며, 해당 사용자 계정을 악용하여 시스템에 접근할 수 있는 위험이 존재한다.

진단 기준

양호

패스워드 복잡도 설정(영문자(대문자, 소문자), 숫자, 특수문자 조합 중 3가지 조합 8자리 이상, 2가지 조합 10자리 이상)을 만족하는 경우

취약

패스워드가 영문자(대문자, 소문자), 숫자, 특수문자 조합 중 3가지 조합 8자리 이상, 2가지 조합 10자리 이상을 만족하지 않은 경우

진단 방법

■ 패스워드 복잡도 설정 적용 확인 (RedHat 계열)

1) system-auth 파일에서 복잡도 설정 및 enforce_for_root 확인
   # cat/etc/pam.d/system-auth

```
# Generated by authselect on Tue Oct 31 05:05:56 2023
# Do not modify this file manually.

auth        required                                     pam_env.so
auth        required                                     pam_faildelay.so delay=2000000
auth        sufficient                                   pam_fprintd.so
auth        [default=1 ignore=ignore success=ok]         pam_usertype.so isregular
auth        [default=1 ignore=ignore success=ok]         pam_localuser.so
auth        sufficient                                   pam_unix.so nullok
auth        [default=1 ignore=ignore success=ok]         pam_usertype.so isregular
auth        sufficient                                   pam_sss.so forward_pass
auth        required                                     pam_deny.so

account     required                                     pam_unix.so
account     sufficient                                   pam_localuser.so
account     sufficient                                   pam_usertype.so issystem
account     [default=bad success=ok user_unknown=ignore] pam_sss.so
account     required                                     pam_permit.so

password    requisite                                    pam_pwquality.so local_users_only
password    sufficient                                   pam_unix.so sha512 shadow nullok use_authtok
password    sufficient                                   pam_sss.so use_authtok
password    required                                     pam_deny.so

session     optional                                     pam_keyinit.so revoke
session     required                                     pam_limits.so
-session    optional                                     pam_systemd.so
session     [success=1 default=ignore]                   pam_succeed_if.so service in crond quiet use_uid
session     required                                     pam_unix.so
session     optional                                     pam_sss.so
ss
```

2) pwquality.comf 파일에서 복잡도 설정 확인
   # cat /etc/security/pwquality.conf

```
[root@localhost pam.d]# cat /etc/security/pwquality.conf
# Configuration for systemwide password quality limits
# Defaults:
#
# Number of characters in the new password that must not be present in the
# old password.
# difok = 1
#
# Minimum acceptable size for the new password (plus one if
# credits are not disabled which is the default). (See pam_cracklib manual.)
# Cannot be set to lower value than 6.
# minlen = 8
#
# The maximum credit for having digits in the new password. If less than 0
# it is the minimum number of digits in the new password.
# dcredit = 0
#
# The maximum credit for having uppercase characters in the new password.
# If less than 0 it is the minimum number of uppercase characters in the new
# password.
# ucredit = 0
#
# The maximum credit for having lowercase characters in the new password.
# If less than 0 it is the minimum number of lowercase characters in the new
# password.
# lcredit = 0
#
# The maximum credit for having other characters in the new password.
# If less than 0 it is the minimum number of other characters in the new
# password.
# ocredit = 0
#
```

■ 패스워드 복잡도 설정 적용 확인 (Debian 계열)

1) common-password 파일에서 복잡도 설정 및 enforce_for_root 확인
cat /etc/pam.d/common-password | grep -v "#"

```
root@ubuntu:~# cat /etc/pam.d/common-password | grep -v "#"

password        requisite                       pam_pwquality.so retry=3
password        [success=2 default=ignore]      pam_unix.so obscure use_authtok try_first_pass yescrypt
password        sufficient                      pam_sss.so use_authtok
password        requisite                       pam_deny.so
password        required                        pam_permit.so
password        optional        pam_gnome_keyring.so
```

2) pwquality.conf 파일에서 복잡도 설정 확인
cat /etc/security/pwquality.conf | grep -v "#"

```
root@ubuntu:~# cat /etc/security/pwquality.conf | grep -v "#"
root@ubuntu:~#
```

조치 방법

■ 패스워드 복잡도 설정 및 enforce_for_root 적용 (RedHat 계열)

1) system-auth 패스워드 복잡도 설정 및 enforce_for_root 설정 적용
vi /etc/pam.d/system-auth

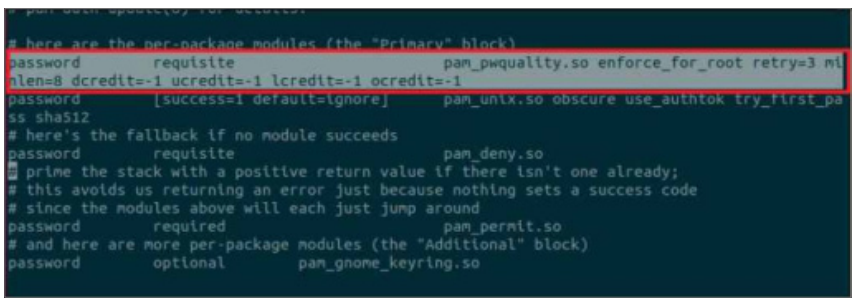
```
#%PAM-1.0
# This file is auto-generated.
# User changes will be destroyed the next time authconfig is run.
auth        required      pam_env.so
auth        required      pam_faildelay.so delay=2000000
auth        sufficient    pam_unix.so nullok try_first_pass
auth        requisite     pam_succeed_if.so uid >= 1000 quiet_success
auth        required      pam_deny.so

account     required      pam_unix.so
account     sufficient    pam_localuser.so
account     sufficient    pam_succeed_if.so uid < 1000 quiet
account     required      pam_permit.so

password    requisite     pam_pwquality.so try_first_pass local_users_only enforce_for_root
retry=3 authtok_type= minlen=8 dcredit=-1 ucredit=-1 lcredit=-1 ocredit=-1
password    sufficient    pam_unix.so md5 shadow nullok try_first_pass use_authtok
password    required      pam_deny.so

session     optional      pam_keyinit.so revoke
session     required      pam_limits.so
session     optional      pam_systemd.so
session     [success=1 default=ignore] pam_succeed_if.so service in crond quiet use_uid
session     required      pam_unix.so
```

2) pwquality.comf 패스워드 복잡도 설정 적용
# vi /etc/security/pwquality.conf
minlen = 8, dcredit=-1, ucredit=-1,lcredit=-1,ocredt=-1으로 수정

※ 복잡도 설정은 system-auth 또는 pwquality.conf 파일에 적용해야 하지만 enforce_for_root 설정은 반드시 system-auth 파일에 적용해야 함

■ 패스워드 복잡도 설정 및 enforce_for_root 적용 (Debian 계열)

1) common-password 패스워드 복잡도 설정 및 enforce_for_root 설정 적용
   # vi /etc/pam.d/common-password



2) pwquality.comf 패스워드 복잡도 설정 적용
   # vi /etc/security/pwquality.conf
   minlen = 8, dcredit=-1, ucredit=-1,lcredit=-1,ocredt=-1으로 수정

※ 복잡도 설정은 common-password 또는 pwquality.conf 파일에 적용해야 하지만
   enforce_for_root 설정은 반드시 common-password 파일에 적용해야 함

계정 잠금 임계값 설정

항목설명

로그인 실패 임계값이 설정되어 있지 않을 경우 반복된 로그인 시도를 차단하지 않아 각종 공격(무작위 대입 공격, 사전 대입 공격, 추측 공격 등)에 취약하며, 비인가자에게 사용자 계정 패스워드를 탈취 당할 수 있다.

진단 기준

양호

계정 잠금 임계값이 5회 이하로 설정되어 있는 경우

취약

계정 잠금 임계값이 5회 이하로 설정되어 있지 않은 경우

진단 방법

■ 계정 임계값 설정 확인 (Debian 계열)

1) common-password 파일 확인
cat /etc/pam.d/common-auth | grep deny

```
auth required pam_tally2.so deny=5 no_magic_root (첫 번째 단락 2번째 줄)
```

■ 계정 임계값 설정 확인 (RedHat 계열)

1) system-auth 파일 확인
cat /etc/pam.d/system-auth | grep deny

```
[root@localhost ~]# cat /etc/pam.d/system-auth | grep accoun
t
account     required      pam_unix.so
account     required      pam_tally2.so deny=5 no_magic_root
account     sufficient    pam_localuser.so
account     sufficient    pam_succeed_if.so uid < 1000 quiet
account     required      pam_permit.so
```

2) password-auth 파일 확인
cat /etc/pam.d/password-auth | grep deny

```
[root@localhost ~]# cat /etc/pam.d/password-auth | grep auth
# User changes will be destroyed the next time authconfig is
 run.
auth        required      pam_env.so
auth        required      pam_tally2.so deny=5 no_magic_root
auth        required      pam_faildelay.so delay=2000000
auth        sufficient    pam_unix.so nullok try_first_pass
auth        requisite     pam_succeed_if.so uid >= 1000 quie
t_success
```

조치 방법

■ 계정 임계값 5회 이하로 설정 (Debian 계열)

1) common-password 파일 수정
vi /etc/pam.d/common-auth

```
auth required pam_tally2.so deny=5 no_magic_root (첫 번째 단락 2번째 줄)
```

■ 계정 임계값 5회 이하로 설정 (RedHat 계열)

1) system-auth 파일 수정
vi /etc/pam.d/system-auth

(RHEL 7 이하)

```
auth required pam_tally2.so deny=5 no_magic_root (첫 번째 단락 2번째 줄)
```

(RHEL 8 이상)

```
account required pam_faillock.so preauth silent audit deny=5 unlock_time=600
```

※ RHEL 계열의 경우, /etc/pam.d/system-auth 파일은 Console 접근, password-auth 파일은 SSH 접근 시 영향 받으므로 2가지 파일 모두 설정해야 함

2) password-auth 파일 확인
vi /etc/pam.d/password-auth

(RHEL 7 이하)

```
account required pam_tally2.so deny=5 no_magic_root (두 번째 단락 2번째 줄)
```

(RHEL 8 이상)

```
account required pam_faillock.so preauth silent audit deny=5 unlock_time=600
```

비고

※ RHEL 계열 8 이상의 경우, /etc/pam.d/system-auth 파일, password-auth 파일 모두 직접 수정하지 않고 pam_faillock 명령어를 입력하여 계정 잠금 임계값 설정을 권고함

패스워드 최대 사용 기간 설정

항목설명

패스워드 최대 사용 기간을 설정하지 않은 경우, 유출된 패스워드로 일정 기간 경과 후에도 접속이 가능하다. 악의적인 사용자로부터 노출된 패스워드를 이용한 접속을 차단하기 위해 패스워드 최대 사용 기간을 설정하여 주기적으로 변경해야 한다.

진단 기준

양호

보안 정책에 따른 최대 사용 기간(90일 이내)이 설정되어 있는 경우

취약

보안 정책에 따른 최대 사용 기간이 설정되어 있지 않거나, 90일 초과인 경우

진단 방법

■ 패스워드 최대 사용 기간 설정 확인

1) # cat /etc/login.defs
PASS_MAX_DAYS 값 확인

■ 계정별 패스워드 최대 사용 기간 설정 확인

1) # cat /etc/passwd

```
sshd:!!:18323::::::
avahi:!!:18323::::::
postfix:!!:18323::::::
tcpdump:!!:18323::::::
sjko:$1$lxvebFkE$GWoI2y4/AV9cLDYmJwbAV.:18323:0 99999 7:::
saned:!!:18324::::::
couchdb:!!:18526::::::
[root@localhost ~]#
```

조치 방법

■ 패스워드 최대 사용 기간 90일 이하로 설정

1) # vi /etc/login.defs
PASS_MAX_DAYS 90

■ 계정별 패스워드 최대 사용 기간 설정

1) # chage –M 90 [계정명]

```
[root@localhost ~]# chage -M 90 sjko
[root@localhost ~]# cat /etc/shadow | grep sjko
sjko:$1$lxvebFkE$GWoI2y4/AV9cLDYmJwbAV.:18323:0 90 7:::
[root@localhost ~]#
```

패스워드 파일 보호

항목설명

/etc/passwd 파일은 일반 사용자도 읽기 권한이 있으므로 passwd 파일에 계정의 비밀번호가 포함되어 있을 경우, 크랙을 통해 root 비밀번호를 취득할 수 있다, 따라서 보안에 취약한 passwd 파일이 아닌, 특별 권한이 있는 사용자만 접근 가능한 shadow 파일에 패스워드를 저장하여 관리해야 한다.

진단 기준

양호

패스워드가 /etc/shadow 파일에 저장되어 있는 경우

취약

패스워드가 /etc/passwd 파일에 저장되어 있는 경우

진단 방법

■ /etc/shadow 파일 존재 확인

ls -l /etc/shadow

```
root@ubuntu:~# ls -l /etc/shadow
-rw-r----- 1 root shadow 1787 12월   7 10:56 /etc/shadow
```

■ /etc/passwd 파일 내 두 번째 필드가 “x”표시가 되어 있는지 확인

cat /etc/passwd

```
root@ubuntu:~# cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
```

조치 방법

■ 쉐도우 패스워드 정책 적용 방법

1) # pwconv

■ 일반 패스워드 정책 적용 방법

1) # pwunconv

root 홈, 패스 디렉터리 권한 패스 설정

항목설명

root 계정의 PATH 환경변수에 "." (현재 디렉터리 지칭)이 포함되어 있으면, root 계정의 인가자로 인해 비의도적으로 현재 디렉터리에 위치하고 있는 명령어가 실행될 수 있다. 즉 "."이 /usr/bin이나 /bin, /sbin 등 명령어들이 위치하고 있는 디렉터리보다 우선하여 위치하고 있을 경우, root 계정의 인가자가 특정 명령을 실행하면, 비인가자가 불법적으로 위치시킨 파일을 실행하여 예기치 않은 결과를 가져올 수 있다. 잘못된 PATH의 우선순위 등이 침해 사고에 이용될 수 있으므로 "." 뿐만 아니라 비인가자가 불법적으로 생성한 디렉터리를 우선으로 가리키지 않도록 설정한다.

진단 기준

양호

PATH 환경변수에 “.”이 맨 앞이나 중간에 포함되지 않은 경우

취약

PATH 환경변수에 “.”이 맨 앞이나 중간에 포함되어 있는 경우

진단 방법

■ echo $PATH 명령어로 현재 설정된 PATH 값 확인

1) # echo $PATH

```
root@ubuntu:~# echo $PATH
/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin:/usr/games:/usr/local/games:/snap/bin
```

2) PATH 내 “.” 포함 여부 확인

※ 홈 디렉터리에 설정된 값이 가장 늦게 적용되어 최종 PATH로 설정됨

조치 방법

■ vi 편집기를 이용하여 root 계정의 설정 파일(~/.profile 과 /etc/profile)을 연 후

1) # vi /etc/profile

■ 아래와 같이 수정

(수정 전) PATH=.:$PATH:$HOME/bin
(수정 후) PATH=$PATH:$HOME/bin

※ 환경변수 파일은 OS별로 약간씩 다를 수 있음

파일 및 디렉터리 소유자 설정

항목설명

소유자나 그룹이 존재하지 않는 파일 및 디렉터리는 현재 권한이 없는 자(퇴직자 등)의 소유였거나, 관리 소홀로 인해 생긴 파일일 가능성이 있다. 중요 파일 및 디렉터리의 소유자 및 그룹이 존재하지 않는 경우 문제가 발생할 수 있으므로 관리가 필요하다.

진단 기준

양호

소유자나 그룹이 존재하지 않는 파일 및 디렉터리가 없는 경우

취약

소유자나 그룹이 존재하지 않는 파일 및 디렉터리가 있는 경우

진단 방법

■ 시스템에서 소유자나 그룹이 존재하지 않는 파일 및 디렉터리를 검색

1) # find / –nouser –nogroup 또는

2) # find /etc /tmp /bin /sbin \(–nouser –o –nogroup \) –xdev –exec ls –al {} \; 2〉 /dev/null

```
root@ubuntu:~# find /etc /tmp /bin /sbin \( -nouser -o -nogroup \) -xdev -exec ls -al {} \; 2> /dev/null
root@ubuntu:~#
```

조치 방법

■ 소유자가 존재하지 않는 파일이나 디렉터리가 불필요한 경우 rm 명령으로 삭제

1) # rm 〈file_name〉

2) # rm –rf 〈directory_name〉

■ 필요한 경우 chown 명령으로 소유자 및 그룹 변경

1) # chown 〈user_name〉 〈file_name〉

/etc/passwd 파일 소유자 및 권한 설정

항목설명

관리자(root) 외 사용자가 "/etc/passwd" 파일의 변조가 가능할 경우 shell 변조, 사용자 추가/삭제, root를 포함한 사용자 권한 획득 시도 등 악의적인 행위가 가능하다.

진단 기준

양호

/etc/passwd 파일의 소유자가 root이고, 권한이 644(-rw-r--r--) 이하인 경우

취약

/etc/passwd 파일의 소유자가 root가 아니거나, 권한이(-rw-r--r--) 644 초과인 경우

진단 방법

■ /etc/passwd 파일의 접근 권한 및 소유자 확인

1) # ls –l /etc/passwd

```
root@ubuntu:~# ls -l /etc/passwd
-rw-r--r-- 1 root root 3408 12월   7 10:56 /etc/passwd
```

조치 방법

■ /etc/passwd 파일 소유자 및 권한 변경

1) # chown root /etc/passwd

```
root@ubuntu:~# chown root /etc/passwd
root@ubuntu:~#
```

2) # chmod 644 /etc/passwd

```
root@ubuntu:~# chmod 644 /etc/passwd
root@ubuntu:~#
```

/etc/shadow 파일 소유자 및 권한 설정

항목설명

해당 파일에 대한 권한 관리가 이루어지지 않을 시 ID 및 패스워드 정보가 외부로 노출될 수 있다.

진단 기준

양호

/etc/shadow 파일의 소유자가 root이고, 권한이 400(-r--------) 이하인 경우

취약

/etc/shadow 파일의 소유자가 root가 아니거나, 권한이 400(-r---------) 초과인 경우

진단 방법

■ /etc/shadow 파일 접근 권한 및 소유자 확인

1) # ls –l /etc/shadow

```
root@ubuntu:~# ls -l /etc/shadow
-rw-r----- 1 root shadow 1787 12월  7 10:56 /etc/shadow
root@ubuntu:~#
```

조치 방법

■ /etc/shadow 파일 소유자 및 권한 변경

1) # chown root /etc/shadow

```
root@ubuntu:~# chown root /etc/shadow
root@ubuntu:~#
```

2) # chmod 400 /etc/shadow

```
root@ubuntu:~# chmod 400 /etc/shadow
root@ubuntu:~#
```

/etc/hosts 파일 소유자 및 권한 설정

항목설명

hosts 파일에 비인가자 쓰기 권한이 부여된 경우, 공격자는 hosts파일에 악의적인 시스템을 등록하여 정상적인 DNS를 우회하는 등 악성사이트로 접속을 유도하는 파밍(Pharming)공격에 악용될 수 있다.

진단 기준

양호

/etc/hosts 파일의 소유자가 root이고, 권한이 644(-rw-r--r--) 이하인 경우

취약

/etc/hosts 파일의 소유자가 root가 아니거나, 권한이 644(-rw-r--r--) 초과인 경우

진단 방법

■ /etc/hosts 파일 접근 권한 및 소유자 확인

1) # ls –l /etc/hosts

```
root@ubuntu:~# ls -l /etc/hosts
-rw-r--r-- 1 root root 235  8월   7 15:12 /etc/hosts
root@ubuntu:~#
```

조치 방법

■ /etc/hosts 파일 접근 권한 644, 소유자 root로 변경

1) # chmod 644 /etc/hosts

```
root@ubuntu:~# chmod 644 /etc/hosts
root@ubuntu:~#
```

2) # chown root /etc/hosts

```
root@ubuntu:~# chown root /etc/hosts
root@ubuntu:~#
```

/etc/(x)inetd.conf 파일 소유자 및 권한 설정

항목설명

(x)inetd.conf 파일에 비인가자의 쓰기 권한이 부여되어 있을 경우, 비인가자가 악의적인 프로그램을 등록하여 root 권한으로 불법적인 서비스를 실행할 수 있다.

진단 기준

양호

/etc/(x)inetd.conf 파일의 소유자가 root이고, 권한이 644(-rw-r--r--) 이하인 경우

취약

/etc/(x)inetd.conf 파일의 소유자가 root가 아니거나, 권한이 644(-rw-r--r--) 초과인 경우

진단 방법

■ /etc/(x)inetd.conf 파일 접근 권한 및 소유자 확인

1) # ls –l /etc/(x)inetd.conf

```
[root@localhost ~]# ls -l /etc/xinetd.conf
-rw-r--r--. 1 root root 0 Sep 16 13:44 /etc/xinetd.conf
```

조치 방법

■ /etc/(x)inetd.conf 파일 접근 권한 644, 소유자 root로 변경

1) # chmod 644 /etc/(x)inetd.conf

```
[root@localhost ~]# chmod 644 /etc/xinetd.conf
```

2) # chown root /etc/(x)inetd.conf

```
[root@localhost ~]# chown root /etc/xinetd.conf
[root@localhost ~]# ls -l /etc/xinetd.conf
-rw-r--r--. 1 root root 0 Sep 16 13:44 /etc/xinetd.conf
```

/etc/(r)syslog.conf 파일 소유자 및 권한 설정

항목설명

(r)syslog.conf 파일의 접근권한이 적절하지 않을 경우, 침해사고 및 장애 등 이슈상황을 파악하기 위한 시스템 로그가 정상적으로 기록되지 않을 수 있다.

진단 기준

양호

/etc/(r)syslog.conf 파일의 소유자가 root이고, 권한이 644(-rw-r--r--) 이하인 경우

취약

/etc/(r)syslog.conf 파일의 소유자가 root가 아니거나, 권한이 644(-rw-r--r--) 초과인 경우

진단 방법

■ /etc/(r)syslog.conf 파일 접근 권한 및 소유자 확인

1) # ls –l /etc/(r)syslog.conf

```
root@ubuntu:~# ls -l /etc/rsyslog.conf
-rw-r--r-- 1 root root 1382 12월  24  2021 /etc/rsyslog.conf
root@ubuntu:~#
```

조치 방법

■ /etc/(r)syslog.conf 파일 접근 권한 644, 소유자 root로 변경

1) # chmod 644 /etc/(r)syslog.conf

```
root@ubuntu:~# chmod 644 /etc/rsyslog.conf
root@ubuntu:~#
```

2) # chown root /etc/(r)syslog.conf

```
root@ubuntu:~# chown root /etc/rsyslog.conf
root@ubuntu:~#
```

비고

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

/etc/services 파일 소유자 및 권한 설정

항목설명

services 파일의 접근권한이 적절하지 않을 경우, 비인가 사용자가 운영 포트 번호를 변경하여 정상적인 서비스를 제한하거나, 허용되지 않은 포트를 오픈하여 악성 서비스를 의도적으로 실행할 수 있다.

진단 기준

양호

/etc/services 파일의 소유자가 root이고, 권한이 644(-rw-r--r--) 이하인 경우

취약

/etc/services 파일의 소유자가 root가 아니거나, 권한이 644(-rw-r--r--) 초과인 경우

진단 방법

■ /etc/services 파일 접근 권한 및 소유자 확인

1) # ls –l /etc/services

```
root@ubuntu:~# ls -l /etc/services
-rw-r--r-- 1 root root 12813  3월  28  2021 /etc/services
```

조치 방법

■ /etc/services 파일의 퍼미션을 644로, 소유자를 root로 변경

1) # chmod 644 /etc/services

```
root@ubuntu:~# chmod 644 /etc/services
root@ubuntu:~#
```

2) # chown root /etc/services

```
root@ubuntu:~# chown root /etc/services
root@ubuntu:~#
```

SUID, SGID, Sticky bit 설정 파일 점검

항목설명

SUID, SGID 파일의 접근권한이 적절하지 않을 경우 SUID, SGID 설정된 파일로 특정 명령어를 실행하여 root 권한 획득 및 정상 서비스 장애를 발생시킬 수 있다.

진단 기준

양호

주요 실행파일의 권한에 SUID와 SGID에 대한 설정이 부여되어 있지 않은 경우

취약

주요 실행파일의 권한에 SUID와 SGID에 대한 설정이 부여되어 있는 경우

진단 방법

■ 명령어를 통해 SUID와 SGID 파일 검색하여 주요 파일의 권한 확인

1) # find / -user root -type f \(-perm -4000 -o -perm -2000 \) -exec ls -lg {} \;

```
root@ubuntu:~# find / -user root -type f \( -perm -4000 -o -perm -2000 \) -exec ls -lg {} \
find: '/proc/28019/task/28019/fdinfo/6': 그런 파일이나 디렉터리가 없습니다
find: '/proc/28019/fdinfo/5': 그런 파일이나 디렉터리가 없습니다
-rwsr-xr-x 1 root 131832  9월  16 05:13 /snap/snapd/20290/usr/lib/snapd/snap-confine
-rwsr-xr-x 1 root 131832  8월  26 02:26 /snap/snapd/20092/usr/lib/snapd/snap-confine
-rwxr-sr-x 1 shadow 72184 11월  24  2022 /snap/core22/864/usr/bin/chage
```

조치 방법

■ SUID, SGID Sticky bit 설정 파일 제거

1) # chmod -s 〈file_name〉

■ 주기적인 감사 방법

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

```
root@ubuntu:~# find / -user root -type f \( -perm -04000 -o -perm -02000 \) -xdev -exec ls -al {} \;
find: warning: you have specified the global option -xdev after the argument -user, but global options
those specified after it.  Please specify global options before other arguments.
-rwsr-xr-x 1 root root 18736  2월  26  2022 /usr/libexec/polkit-agent-helper-1
-rwxr-sr-x 1 root mail 22856  6월  20 03:23 /usr/libexec/camel-lock-helper-1.2
```

■ 반드시 사용이 필요한 경우 특정 그룹에서만 사용하도록 제한하는 방법(일반 사용자의 Setuid 사용을 제한함, 임의의 그룹만 가능)

1) # /usr/bin/chgrp 〈group_name〉 〈setuid_file_name〉

2) # /usr/bin/chmod 4750 〈setuid_file_name〉

비고

※ SUID, SGID, Sticky bit 설정 파일 제거 시, OS 및 응용 프로그램 등 서비스 영향도를 파악하여 충분한 테스트 후 적용 권고

사용자, 시스템 시작파일, 환경파일 소유자 및 권한 설정

항목설명

홈 디렉터리 내의 사용자 파일 및 사용자별 시스템 시작파일 등과 같은 환경변수 파일의 접근권한 설정이 적절하지 않을 경우 비인가자가 환경변수 파일을 변조하여 정상 사용 중인 사용자의 서비스가 제한될 수 있다.

진단 기준

양호

사용자, 시스템 시작파일 및 환경 파일 소유자가 root 또는 해당 계정이고 권한이 644(-rw-r--r--)로 설정되어 있는 경우

취약

사용자, 시스템 시작파일 및 환경 파일 소유자가 root 또는 해당 계정이 아니거나 권한이 644(-rw-r--r--)로 설정되어 있지 않은 경우

진단 방법

■ 사용자 홈 디렉터리 확인

1) # cat /etc/passwd | grep /home

```
root@ubuntu:~# cat /etc/passwd | grep /home
syslog:x:104:111::/home/syslog:/usr/sbin/nologin
cups-pk-helper:x:115:122:user for cups-pk-helper service,,,:/home/cups-pk-helper:/usr/sbin/nologin
[redacted]:x:1000:1000:ksel,,,:/home/[redacted]:/bin/bash
mongodb:x:136:65534::/home/mongodb:/usr/sbin/nologin
```

■ 해당 홈 디렉터리 소유자 및 권한 확인

1) # ls –ld 〈사용자 홈 디렉터리〉

```
root@ubuntu:~# ls -ld /home/[redacted]
drwxr-x--- 22 [redacted] 4096 12월  11 19:40 /home/[redacted]
```

2) # ls –al 〈사용자 홈 디렉터리〉

```
root@ubuntu:~# ls -al /home/[redacted]
합 계  232
drwxr-x--- 22 [redacted]  4096 12월  11 19:40 .
drwxr-xr-x  3 [redacted]  4096  8월   7 15:14 ..
-rw-------  1 [redacted]   104 12월  11 19:40 .Xauthority
-rw-------  1 [redacted] 10897 12월   7 14:25 .bash_history
-rw-r--r--  1 [redacted]   220  8월   7 15:14 .bash_logout
-rw-rw-r--  1 [redacted]   251 12월   4 10:20 .bash_profile
-rw-r--r--  1 [redacted]  3771  8월   7 15:14 .bashrc
drwx------ 11 [redacted]  4096  9월  22 10:33 .cache
drwx------ 11 [redacted]  4096  8월   7 15:46 .config
```

조치 방법

■ 소유자 변경

1) # chown 〈user_name〉 〈file_name〉

```
root@ubuntu:~# chown root /home/[redacted].bashrc
```

■ 일반 사용자 쓰기 권한 제거

2) # chmod o-w 〈file_name〉

world writable 파일 점검

항목설명

시스템 파일(중요 파일)에 world writable 설정이 될 경우, 악의적인 사용자가 해당 파일을 마음대로 수정할 수 있어 시스템의 무단 접근 및 시스템 장애를 유발할 수 있다.

진단 기준

양호

world writable 파일이 존재하지 않거나, 존재 시 설정 이유를 확인하고 있는 경우

취약

world writable 파일이 존재하나 해당 설정 이유를 확인하고 있지 않는 경우

진단 방법

■ world writable 파일 존재 여부 확인

1) # find / -type f -perm -2 -exec ls -l {} \;

```
root@ubuntu:~# find / -type f -perm -2 -exec ls -l {} \;
-rw-rw-rw- 1 root root 0 12월  11 20:49 /proc/sys/kernel/ns_last_pid
-rw-rw-rw- 1 root root 0 12월  11 10:59 /proc/pressure/io
-rw-rw-rw- 1 root root 0 12월  11 10:59 /proc/pressure/cpu
```

※ /tmp 디렉터리의 경우, 시스템 재시작 시, 디렉터리 내 파일이 제거될 수 있는 임시 디렉터리이므로 점검 범위에서 제외

조치 방법

■ 일반 사용자 쓰기 권한 제거

1) # chmod o-w 〈file_name〉

```
root@ubuntu:~# chmod o-w /proc/30176/attr/current
```

■ 파일 삭제 방법

1) # rm -rf 〈world-writable 파일명〉

$HOME/.rhosts, hosts.equiv 사용 금지

항목설명

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 있다. 또한 공격자 백도어 등으로도 활용될 수 있다.

진단 기준

양호

login, shell, exec 서비스를 사용하지 않거나, 사용 시 아래와 같은 설정이 적용된 경우

/etc/hosts.equiv 및 $HOME/.rhosts 파일 소유자가 root 또는, 해당 계정인 경우

/etc/hosts.equiv 및 $HOME/.rhosts 파일 권한이 600(-rw-------) 이하인 경우

/etc/hosts.equiv 및 $HOME/.rhosts 파일 설정에 '+' 설정이 없는 경우

/etc/hosts.equiv 파일 또는 .rhosts 파일이 존재하지 않을 경우

취약

login, shell, exec 서비스를 사용하거나, 사용 시 아래와 같은 설정이 적용되어 있지 않은 경우

/etc/hosts.equiv 및 $HOME/.rhosts 파일 소유자가 root 또는, 해당 계정인 경우

/etc/hosts.equiv 및 $HOME/.rhosts 파일 권한이 600(-rw-------) 이하인 경우

/etc/hosts.equiv 및 $HOME/.rhosts 파일 설정에 '+' 설정이 없는 경우

/etc/hosts.equiv 파일 또는 .rhosts 파일이 존재하지 않을 경우

진단 방법

■ 파일 소유자 및 권한 확인

1) # ls -al /etc/hosts.equiv
2) # ls -al $HOME/.rhosts

■ 계정 별 '+' 부여 적절성 확인

1) # cat /etc/hosts.equiv
2) # cat $HOME/.rhosts

조치 방법

■ .rhosts, hosts.equiv 파일 미사용 시

1) .rhosts, hosts.equiv 파일 삭제
   # rm -f [삭제 할 파일 및 디렉터리 경로]
   # rm -f $HOME/.rhosts 또는 or /etc/ hosts.equiv

■ .rhosts, hosts.equiv 파일 사용 시

1) "/etc/hosts.equiv" 및 "$HOME/.rhosts" 파일의 소유자 root 또는, 해당 계정으로 변경
   # chown root /etc/hosts.equiv
   # chown [계정 명] $HOME/.rhosts
2) "/etc/hosts.equiv" 및 "$HOME/.rhosts" 파일의 퍼미션을 600 이하로 변경
   # chmod 600 /etc/hosts.equiv
   # chmod 600 $HOME/.rhosts
3) "/etc/hosts.equiv" 및 "$HOME/.rhosts" 파일에서 "+"를 제거하고 허용 호스트 및 계정 등록
   # vi /etc/hosts.equiv (or $HOME/.rhosts)

접속 IP 및 포트 제한

항목설명

허용할 호스트에 대한 IP 및 포트제한이 적용되지 않은 경우, Telnet, FTP같은 보안에 취약한 네트워크 서비스를 통하여 불법적인 접근 및 시스템 침해사고가 발생할 수 있다.

진단 기준

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

진단 방법

■ All deny 적용 확인 및 접근 허용 IP 적절성 확인 또는 iptables에서 서버로 접속 하는 IP 설정 확인

1) /etc/hosts.deny, allow 설정 확인
   # cat /etc/hosts.deny
   # cat /etc/hosts.allow
2) iptables 설정 확인
   # iptables -nL
3) # firewall-cmd —list-all

※ 접근 통제 IP를 대역으로 설정하는 경우는 취약
※ TCP Wrapper, iptables, firewalld를 이용하여 IP 주소 및 포트를 제한하고 있지 않을 경우, 수동 점검을 통해 별도 방화벽 존재 및 IP 접근 통제 방식을 확인

조치 방법

■ /etc/hosts.deny 파일 수정

1) # vi /etc/hosts.deny
2) ALL deny 설정
   ALL:ALL

```
root@ubuntu:~# cat /etc/hosts.deny | grep ALL
# Example:    ALL: some.host.name, .some.domain
#             ALL EXCEPT in.fingerd: other.host.name, .other.domain
ALL:ALL
```

■ /etc/hosts.allow 파일 수정

1) # vi /etc/hosts.allow
2) 접속 허용 서비스 및 IP 설정 (예시)
   sshd : 192.168.0.148, 192.168.0.6

```
root@ubuntu:~# cat /etc/hosts.allow | grep sshd
sshd : 192.168.128.60
```

※ TCP Wrapper 접근제어 가능 서비스
SYSTAT, FINGER, FTP, TELNET, RLOGIN, RSH, TALK, EXEC, TFTP, SSH

비고

※ 허용되지 않는 IP는 서비스 사용이 불가함

cron 파일 소유자 및 권한 설정

항목설명

root 외 일반사용자에게도 crontab 명령어를 사용할 수 있도록 할 경우, 고의 또는 실수로 불법적인 예약 파일 실행으로 시스템 피해를 일으킬 수 있다.

진단 기준

양호

/etc/crontab 파일의 소유자가 root이고, 권한이 640(-rw-r-----) 이하인 경우

취약

/etc/crontab 파일의 소유자가 root가 아니거나, 권한이 640(-rw-r-----) 초과인 경우

진단 방법

■ /etc/cron.allow 및 /etc/cron.deny 파일 접근 권한 및 소유자 확인

1) # ls –l /etc/cron.allow

2) # ls –l /etc/cron.deny

※ cron.allow 파일이 존재하지 않는 경우, cron.deny 파일의 접근 권한만 확인하여 점검

조치 방법

■ /etc/cron.allow 및 /etc/cron.deny 파일의 소유자 및 권한 변경

1) # chown root /etc/cron.allow
   # chmod 640 /etc/cron.allow

2) # chown root /etc/cron.deny
   # chmod 640 /etc/cron.deny

Finger 서비스 비활성화

항목설명

비인가자에게 사용자 정보가 조회되어 패스워드 공격을 통한 시스템 권한 탈취 가능성이 있으므로 Finger 서비스를 사용하지 않는다면 해당 서비스를 중지하여야 한다.

진단 기준

양호

finger 서비스가 비활성화 되어 있는 경우

취약

finger 서비스가 활성화 되어 있는 경우

진단 방법

■ /etc/xinetd.d/finger 파일에서 서비스 비활성화 여부 확인 (xinetd)

1) # cat /etc/xinetd.d/finger | grep disable

```
[root@localhost ~]# cat /etc/xinetd.d/finger | grep disable
disable         = no
```

■ /etc/inetd.conf 파일에서 finger 서비스 라인 #처리(주석처리) 또는 삭제되어 있는지 확인 (inetd)

1) # cat /etc/inetd.conf | grep finger

조치 방법

■ /etc/xinetd.d/finger 파일에서 서비스 비활성화 설정

1) # vi /etc/xinetd.d/finger

```
disable         = no
```

Anonymous FTP 비활성화

항목설명

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 한다.

진단 기준

양호

Anonymous FTP (익명 ftp) 접속을 차단한 경우

취약

Anonymous FTP (익명 ftp) 접속을 차단하지 않은 경우

진단 방법

■ /etc/passwd 파일에 ftp 계정 존재 여부 확인 (일반 FTP)

1) # cat /etc/passwd | grep ftp

```
root@ubuntu:~# cat /etc/passwd | grep ftp
root@ubuntu:~#
```

■ proftpd.conf 파일에서 〈Anonymous ~ ftp〉 부분 확인 (ProFTP)

※ UserAlias 항목이 주석처리 되어있거나, 없으면 양호

1) # cat etc/proftpd/proftpd.conf

```
UserAlias        anonymous ftp
```

■ vsftpd.conf 파일에서 anonymous_enable 값이 No로 설정되어 있는지 확인

1) # cat /etc/vsftpd/vsftpd.conf (vsFTP)

```
anonymous_enable = Yes
```

조치 방법

■ Anonymous FTP 접속 제한 설정 방법 /etc/passwd 파일에서 ftp 또는, anonymous 계정 삭제 (일반 FTP)

1) # userdel ftp

```
root@ubuntu:~# userdel ftp
```

■ Anonymous FTP 접속 제한 설정 방법 (ProFTP)

/etc/passwd 파일에서 ftp 계정 삭제

1) # userdel ftp

■ Anonymous FTP 접속 제한 설정 방법 (vsFTP)

vsFTP 설정파일(/etc/vsftpd/vsftpd.conf 또는, /etc/vsftpd.conf)에서 anonymous_enable=NO 설정

비고

Anonymous FTP를 사용하지 않을 경우 영향 없음

r 계열 서비스 비활성화

항목설명

서비스 포트가 열려있을 경우, 비인가자에 의한 중요 정보 유출 및 시스템 장애 발생 등 사고의 원인이 될 수 있다.

진단 기준

양호

r 계열 서비스(rlogin, rsh, rexec)가 비활성화 되어 있는 경우

취약

r 계열 서비스(rlogin, rsh, rexec)가 활성화 되어 있는 경우

진단 방법

■ rsh, rlogin, rexec (shell, login, exec) 서비스 비활성화 여부 확인

1) # cat /etc/xinetd.d/rsh | grep disable
2) # cat /etc/xinetd.d/rlogin | grep disable
3) # cat /etc/xinetd.d/rexec | grep disable

조치 방법

■ vi 편집기를 이용하여 /etc/xinetd.d/ 디렉터리 내 rlogin, rsh, rexec 파일을 연 후,

■ 아래와 같이 설정 (disable = yes 설정)

1) /etc/xinetd.d/rlogin 파일
2) /etc/xinetd.d/rsh 파일
3) /etc/xinetd.d/rexec 파일

```
service       rlogin
{
...
disable         =  yes
}
```

비고

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

DoS 공격에 취약한 서비스 비활성화

항목설명

해당 서비스가 활성화되어 있는 경우 시스템 정보 유출 및 DoS(서비스 거부 공격)의 대상이 될 수 있다.

진단 기준

양호

Dos 공격에 취약한 echo, discard, daytime, chargen 서비스가 비활성화 된 경우

취약

Dos 공격에 취약한 echo, discard, daytime, chargen 서비스가 활성화 된 경우

진단 방법

■ /etc/xinetd.d/ 디렉터리 내 echo, discard, daytime, chargen 서비스 비활성화 여부 확인 (xinetd)

1) # cat /etc/xinetd.d/echo | grep disable
2) # cat /etc/xinetd.d/discard | grep disable
3) # cat /etc/xinetd.d/daytime | grep disable
4) # cat /etc/xinetd.d/chargen | grep disable

※ 각 서비스 설정 파일에서 disable=yes로 설정되어 있는지 확인 필요

조치 방법

■ /etc/xinetd.d/ 디렉터리 내 echo, discard, daytime, chargen 파일 열기

1) # vi /etc/xinetd.conf/...

2) 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)

3) disable=yes 확인
   service echo

```
{
disable      = yes
id           = echo-stream
type         = internal
wait         = no
socket—type          = stream
}
```

4) xinetd 서비스 재시작
   # service xinetd restart

NFS 서비스 비활성화

항목설명

NFS 서비스를 활성화 한 경우, 비인가자가 NFS 서비스를 악용하여 허가되지 않은 시스템 접근, 파일 위변조 등의 침해활동을 할 수 있는 가능성이 존재한다.

진단 기준

양호

NFS 서비스 관련 데몬이 비활성화 되어 있는 경우

취약

NFS 서비스 관련 데몬이 활성화 되어 있는 경우

진단 방법

■ NFS 데몬 구동 여부 확인

1) # ps -ef | grep nfsd

```
root@ubuntu:~# ps -ef | grep nfsd
root       41837   25472  0 21:40 pts/1    00:00:00 grep --color=auto nfsd
```

조치 방법

■ NFS 데몬(nfsd)을 중지

1) # kill -9 [NFS 데몬 PID]

비고

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

NFS 접근통제

항목설명

접근제한 설정이 적절하지 않을 경우 인증절차 없이 비인가자의 디렉터리나 파일의 접근이 가능하며, 해당 공유 시스템에 원격으로 마운트하여 중요 파일을 변조하거나 유출할 위험이 있다.

진단 기준

양호

NFS 서비스 사용 시 everyone 공유를 제한한 경우

취약

NFS 서비스 사용 시 everyone 공유를 제한하지 않은 경우

진단 방법

■ everyone으로 시스템이 마운트 되어 있는지 확인

1) # showmount -e hostname

■ /etc/exports 파일에서 접근 통제 설정 여부 확인

1) # cat /etc/exports

※ 취약한 설정 예 : /var/www/img *(ro,all_squash)
양호한 설정 예 : /data 172.27.0.0/16(rw,no_root_squash)

조치 방법

■ everyone 마운트 제거

1) # umount "파일시스템 이름"

■ /etc/exports 파일에서 접근 통제 설정 (예시)

1) # vi /etc/exports
/data 172.27.0.0/16(rw,no_root_squash)

비고

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

automountd 제거

항목설명

파일 시스템의 마운트 옵션을 변경하여 root 권한을 획득할 수 있으며, 로컬 공격자가 automountd 프로세스 권한으로 임의의 명령을 실행할 수 있다.

진단 기준

양호

automount 서비스가 비활성화 되어 있는 경우

취약

automount 서비스가 활성화 되어 있지 않은 경우

진단 방법

■ automountd 서비스 데몬 확인

1) # ps –ef | grep automountd

```
root@ubuntu:~# ps -ef | grep automountd
root       42929   25472  0 21:45 pts/1    00:00:00 grep --color=auto automountd
```

조치 방법

■ automountd 서비스 데몬 실행 중지

1) # ps –ef | grep automountd

2) # kill –9 [automountd 서비스 PID]

■ 시스템 재시작 시, automount 가 시작되지 않도록 설정

–1 부팅스크립트에서 automountd 제거
chkconfig ––level 0123456 autofs off

–2 아래와 같이 파일경로 확인 후 파일명 변경 (예시)
mv /etc/rc2.d/S28autofs /etc/rc2.d/S28autofs.orig

비고

※ 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)

참고) 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

RPC 서비스 확인

항목설명

버퍼 오버플로우(Buffer Overflow), Dos, 원격실행 등의 취약성이 존재하는 RPC 서비스를 통해 비인가자의 root 권한 획득 및 침해사고 발생 위험이 있으므로 서비스를 중지하여야 한다.

진단 기준

양호

불필요한 RPC 서비스가 비활성화 되어 있는 경우

취약

불필요한 RPC 서비스가 활성화 되어 있는 경우

진단 방법

■ /etc/xinetd.d/ 디렉터리 내 RPC 서비스 파일에서 비활성화 여부 확인 (xinetd)

1) # cat /etc/xinetd.d/rstatd

※ 각 서비스 설정 파일에서 disable=yes로 되어있는지 확인 필요

조치 방법

■ /etc/xinetd.d/ 디렉터리 내의 불필요한 RPC 서비스 파일 수정

1) disable=yes 설정

```
service  rstatd
{
    disable      =  yes
    … 이하 생략 …
}
```

NIS, NIS+ 점검

항목설명

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 권장한다.

진단 기준

양호

NIS, NIS+ 서비스가 구동 중이지 않을 경우

취약

NIS, NIS+ 서비스가 구동 중일 경우

진단 방법

■ NIS, NIS+ 서비스 구동 확인

ps –ef | egrep “ypserv|ypbind|ypxfrd|rpc.yppasswdd|rpc.ypupdated” | grep –v "grep“

```
root@ubuntu:~# ps -ef | egrep "ypserv|ypbind|ypxfrd|rpc.yppasswdd|rpc.ypupdated" | grep -v "grep"
root       44259       1  0 21:52 ?        00:00:00 rpc.yppasswdd
root@ubuntu:~#
```

조치 방법

■ NFS 서비스 데몬 중지

1) # kill –9 [NIS, NIS+ 서비스 PID]

```
root@ubuntu:~# kill -9 44259
root@ubuntu:~#
```

tftp, talk 서비스 비활성화

항목설명

사용하지 않는 서비스나 취약점이 발표된 서비스 운용 시 공격자의 공격 시도가 가능하다.

진단 기준

양호

tftp, talk 서비스가 비활성화 되어 있는 경우

취약

tftp, talk 서비스가 활성화 되어 있는 경우

진단 방법

■ /etc/xinetd.d/ 디렉터리 내 tftp, talk, ntalk서비스 파일에서 비활성화 여부 확인 (xinetd)

1) # cat /etc/xinetd.d/tftp

조치 방법

■ /etc/xinetd.d/ 디렉터리 내 tftp, talk, ntalk 파일 수정

1) disable=yes 설정
   /etc/xinetd.d/tftp 파일
   /etc/xinetd.d/talk 파일
   /etc/xinetd.d/ntalk 파일

```
service  tftp
{
    … 생략 …
    disable  =  yes
}
```

Sendmail 버전 점검

항목설명

취약점이 발견된 Sendmail, postfix 버전의 경우 버퍼 오버플로우(Buffer Overflow) 공격에 의한 시스템 권한 획득 및 주요 정보 유출 가능성이 있다.

진단 기준

양호

Sendmail, postfix 버전을 정기적으로 점검하고, 최신 버전 패치를 했을 경우

취약

Sendmail, postfix 버전을 점검하지 않고, 취약한 버전을 사용할 경우

진단 방법

■ Sendmail 프로세스 확인

1) # ps -ef | grep sendmail

```
root@ubuntu:~# ps -ef | grep sendmail
root       44515   25472  0 21:56 pts/1    00:00:00 grep --color=auto sendmail
root@ubuntu:~#
```

■ Sendmail 버전 확인

1) # cat /etc/mail/sendmail.cf | grep DZ

```
root@ubuntu:~# cat /etc/mail/sendmail.cf | grep DZ
cat: /etc/mail/sendmail.cf: 그 런  파 일 이 나  디 렉 터 리 가  없 습 니 다
```

※ Sendmail을 사용하지 않는 경우, 해당사항 없음(N/A)으로 처리함

■ Postfix 프로세스 확인

1) # systemctl status postfix

```
root@RR:~# systemctl status postfix
● postfix.service - Postfix Mail Transport Agent
     Loaded: loaded (/lib/systemd/system/postfix.service; enabled; vendor preset: en
     Active: active (exited) since Wed 2023-04-19 14:15:06 KST; 1h 13min ago
   Main PID: 1309 (code=exited, status=0/SUCCESS)
      Tasks: 0 (limit: 4580)
     Memory: 0B
     CGroup: /system.slice/postfix.service

 4월  19 14:15:06 RR systemd[1]: Starting Postfix Mail Transport Agent...
 4월  19 14:15:06 RR systemd[1]: Finished Postfix Mail Transport Agent.
```

2) postfix PID 확인
   # posftfix status

```
root@RR:~# postfix status
postfix/postfix-script: the Postfix mail system is running: PID: 1306
```

3) postfix 버전 확인
   # postconf -d | grep mail_version

```
root@RR:~# postconf -d | grep mail_version
mail_version = 3.4.13
milter_macro_v = $mail_name $mail_version
```

※ postfix를 사용하지 않는 경우 해당사항 없음(N/A)으로 처리함

조치 방법

- Sendmail 서비스 실행 여부 및 버전 점검 후, http://www.sendmail.org/ 또는, 각 OS 벤더사의 보안 패치 설치
- postfix 실행 여부 및 버전 점검 수, OS 벤더사의 보안 패치 설치

※ 최신 버전을 사용하도록 권고하고 있으나 시스템 운영상 적용이 어려운 경우 최신이 아닌 취약점이 존재하지 않는 버전도 허용하고 있음

비고

※ 보안 패치를 적용할 경우, 시스템 영향도를 파악하여 충분한 테스트 후 적용 권고

스팸 메일 릴레이 제한

항목설명

SMTP 서버의 릴레이 기능을 제한하지 않는 경우, 악의적인 사용목적을 가진 사용자들이 스팸메일 서버로 사용하거나 Dos공격의 대상이 될 수 있다.

진단 기준

양호

SMTP 서비스를 사용하지 않거나 릴레이 제한이 설정되어 있는 경우

취약

SMTP 서비스를 사용하며 릴레이 제한이 설정되어 있지 않은 경우

진단 방법

■ SMTP 서비스 사용 여부 및 릴레이 제한 옵션 확인 (Sendmail 사용 시)

1) # ps –ef | grep sendmail | grep –v "grep“

```
root@ubuntu:~# ps -ef | grep sendmail | grep -v "grep"
root@ubuntu:~#
```

※ SMTP 서비스가 비활성화되어 있는 경우, Sendmail 서비스가 미구동 상태이므로 해당사항 없음(N/A)으로 처리함

2) # cat /etc/mail/sendmail.cf | grep "R$ *" | grep "Relaying denied“

```
root@ubuntu:~# cat /etc/mail/sendmail.cf | grep "R$ \*" | grep "Relaying denied"
cat: /etc/mail/sendmail.cf: 그런 파일이나 디렉터리가 없습니다
```

■ 릴레이 제한 확인 (Postfix 사용 시)

1) # cat/etc/postfix/main.cf | grep ‘mynetworks =’

```
root@RR:~# cat /etc/postfix/main.cf | grep 'mynetworks = '
mynetworks = 127.0.0.0/8
```

2) # cat /etc/postfix/main.cf | grep ‘permit_mynetworks’

```
root@RR:~# cat /etc/postfix/main.cf | grep 'permit_mynetworks'
smtpd_relay_restrictions = permit_mynetworks,permit_sasl_authenticated,reject_unauth_destination
```

조치 방법

■ vi 편집기를 이용하여 sendmail.cf 설정파일을 연 후

■ 아래와 같이 주석 제거

(수정 전) #R$* $#error $@ 5.7.1 $: "550 Relaying denied"
(수정 후) R$* $#error $@ 5.7.1 $: "550 Relaying denied"

■ 특정 IP, domain, Email Address 및 네트워크에 대한 sendmail 접근 제한 확인

vi /etc/mail/access

■ postfix 사용 시, 파라미터를 이용한 릴레이 접근 제한 설정 (예시)

1) main.cf 파일 수정
(수정 전) mynetworks = localhost, 127.0.0.1 ::1/128 fe80::/10
(수정 후) mynetworks = 127.0.0.1/8 [::1]/128 192.168.0.0/24

```
root@RR:~# cat /etc/postfix/main.cf | grep 'mynetworks = '
mynetworks = 127.0.0.0/8 [::1]/128 192.168.0.0/24
```

비고

릴레이를 허용할 대상에 대한 정보를 입력한다면 영향 없음

일반 사용자의 Sendmail 실행 방지

항목설명

일반 사용자가 q 옵션을 이용해서 메일큐, Sendmail 설정을 보거나 메일큐를 강제적으로 drop 시킬 수 있어 악의적으로 SMTP 서버의 오류를 발생시킬 수 있다.

진단 기준

양호

SMTP 서비스 미사용 또는, 일반 사용자의 Sendmail 실행 방지가 설정된 경우

취약

SMTP 서비스 사용 또는, 일반 사용자의 Sendmail 실행 방지가 설정되지 않은 경우

진단 방법

■ sendmail.cf 파일에서 restrictqrun 옵션 설정 여부 확인 (Sendmail 사용)

1) # cat /etc/mail/sendmail.cf | grep PrivacyOptions
O PrivacyOptions=authwarnings, novrfy, noexpn

■ sendmail.cf 파일에서 restrictqrun 옵션 설정 여부 확인 (Postfix 사용)

1) postfix 파일 접근 권한 및 소유자 확인
/usr/sbin/postfix

```
root@RR:~# ls -l /usr/sbin/postfix
-rwxr-xr-x 1 root root 18664  9월   7  2021 /usr/sbin/postfix
```

2) postfix 그룹 사용자 목록 확인
getent group postfix

```
root@RR:~# getent group postfix
postfix:x:134:
```

조치 방법

■ sendmail.cf 설정 파일 수정

1) # vi /etc/mail/sendmail.cf

2) O PrivacyOptions= 설정 부분에 restrictqrun 옵션 추가
O PrivacyOptions=authwarnings, novrfy, noexpn (수정 전)
O PrivacyOptions=authwarnings, novrfy, noexpn, restrictqrun (수정 후)

■ postfix 파일 접근 권한 및 소유자 변경

1) # chown /usr/sbin/postfix

2) # chmod 750 /usr/sbin/postfix

```
root@RR:~# chown root /usr/sbin/postfix
root@RR:~# chmod 750 /usr/sbin/postfix
root@RR:~# ls -l /usr/sbin/postfix
-rwxr-x--- 1 root root 18664  9월   7  2021 /usr/sbin/postfix
```

3) postfix 그룹의 root 또는 관리자 계정 추가
gpasswd –a 〈user〉 postfix

```
root@RR:~# sudo gpasswd -a root postfix
Adding user root to group postfix
root@RR:~# getent group postfix
postfix:x:134:root
```

4) postfix 그룹의 일반 사용자 제거
gpasswd –d 〈user〉 postfix

DNS 보안 버전 패치

항목설명

최신 버전 이하의 버전에서는 Service Denial Attack, 버퍼 오버플로우(Buffer Overflow), DNS 서버 원격 침입 등의 취약성이 존재한다.

진단 기준

양호

DNS 서비스를 사용하지 않거나 주기적으로 보안 패치를 관리하고 있는 경우

취약

DNS 서비스를 사용하며, 주기적으로 보안 패치를 관리하고 있지 않은 경우

진단 방법

■ DNS 서비스 사용 및 BIND 버전 확인

1) # ps -ef | grep named

```
root@ubuntu:~# ps -ef | grep named
root       46313   25472  0 22:31 pts/1    00:00:00 grep --color=auto named
```

2) # named –v

조치 방법

■ DNS 서비스를 사용할 경우, 최신 보안 패치 적용

1) BIND 버전 확인 후, 최신 보안 패치 버전으로 업데이트

■ DNS 서비스를 사용하지 않는 경우, DNS 데몬 중지

1) 서비스 중지
   # kill –9 [DNS 프로세스 PID]

※ 최신 버전을 사용하도록 권고하고 있으나 시스템 운영상 적용이 어려운 경우 최신이 아닌 취약점이 존재하지 않는 버전도 허용하고 있음

비고

※ 최신 보안 패치를 적용 시, 시스템 영향도를 파악하여 충분한 테스트 후 보안 패치 적용 권고

DNS ZoneTransfer 설정

항목설명

비인가자 Zone Transfer를 이용해 Zone 정보를 전송받아 호스트 정보, 시스템 정보, 네트워크 구조 등 많은 정보를 파악할 수 있다.

진단 기준

양호

DNS 서비스 미사용 또는, Zone Transfer를 허가된 사용자에게만 허용한 경우

취약

DNS 서비스를 사용하며 Zone Transfer를 모든 사용자에게 허용한 경우

진단 방법

■ /etc/named.conf 설정 파일에서 zone transfer 설정 확인

1) # cat /etc/named.conf

```
Options {
      allow-transfer{10.10.10.10;};
};
```

※ DNS 서비스를 사용하지 않을 시, 해당사항 없음(N/A)으로 처리함

조치 방법

■ 특정 서버 Zone Transfer 지정

1) # vi /etc/named.conf

```
Options {
      allow-transfer{10.10.10.111; 10.10.10.112;};
};
```

■ 특정 도메인의 Zone에 대해서 제한할 경우에는 다음과 같이 설정

1) # vi /etc/named.conf

```
zone "xxx.co.kr" {
    Type master ;
    File "db.xxx.co.kr";
    allow-transfer{10.10.10.111; 10.10.10.112;};
}
```

비고

Zone 파일 전송을 허용할 대상을 정상적으로 등록할 경우 일반적으로 영향 없음

최신 보안패치 및 벤더 권고사항 적용

항목설명

최신 보안패치가 적용되지 않을 경우, 이미 알려진 취약점에 의해 해당 시스템의 침해사고 발생 가능성이 높아진다.

진단 기준

양호

패치 적용 정책을 수립하여 주기적으로 패치를 관리하고 있는 경우

취약

패치 적용 정책을 수립하여 주기적으로 패치를 관리하고 있지 않은 경우

진단 방법

■ Linux OS 버전 확인

1) # cat /etc/os-release

```
root@ubuntu:~# cat /etc/os-release
PRETTY_NAME="Ubuntu 22.04.3 LTS"
NAME="Ubuntu"
VERSION_ID="22.04"
VERSION="22.04.3 LTS (Jammy Jellyfish)"
VERSION_CODENAME=jammy
ID=ubuntu
ID_LIKE=debian
HOME_URL="https://www.ubuntu.com/"
SUPPORT_URL="https://help.ubuntu.com/"
BUG_REPORT_URL="https://bugs.launchpad.net/ubuntu/"
PRIVACY_POLICY_URL="https://www.ubuntu.com/legal/terms-and-policies/privacy-policy"
UBUNTU_CODENAME=jammy
root@ubuntu:~#
```

※ EOL 상태인 OS 버전을 사용하고 있다면 취약

■ Kernel 버전 확인

1) # uname –r

```
root@ubuntu:~# uname -r
6.2.0-37-generic
root@ubuntu:~#
```

조치 방법

■ 최신 보안 패치 적용

1) EOL 상태가 아닌 Linux OS 버전으로 업데이트

2) 최신 보안 패치 적용 Kernel 버전으로 업데이트

※ 최신 Kernel 버전을 사용하도록 권고하고 있으나 시스템 운영상 적용이 어려운 경우 최신이 아닌 취약점이 존재하지 않는 커널 버전도 허용하고 있음

비고

※ 보안 패치를 적용할 경우, 시스템 영향도를 파악하여 충분한 테스트 후 적용 권고

로그의 정기적 검토 및 백업

항목설명

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 어렵다.

진단 기준

양호

로그 기록의 검토, 분석 등이 정기적으로 이루어지고 있으며 로그 파일을 주기적으로 백업하고 있는 경우

취약

로그 기록의 검토, 분석 등이 정기적으로 이루어지고 있지 않거나 로그 파일을 주기적으로 백업하고 있지 않은 경우

진단 방법

■ 로그 정책 수립 여부 및 정책에 따른 로그 검토 여부 확인

1) 로그 정책 수립 여부 확인
2) 로그 파일 기록 주기 및 기록 방식 확인
3) 로그 파일 백업 주기 및 백업 방식 확인

조치 방법

■ 로그 기록 관리 및 백업

1) 로그 정책 수립

2) 로그 파일 주기적 기록 및 정기적인 백업

※ 아래의 로그를 검토해야 함
1) su 시도에 관한 로그
2) 반복적인 로그인 실패에 관한 로그
3) 로그인 거부 메시지에 관한 로그
4) /var/adm, /var/log

※ 커널과 시스템에 관련된 로그 메시지들은 syslogd와 klogd 두개의 데몬에 의해서 /var/log/messages에 기록하게 됨. 이 파일을 분석함으로써 시스템을 항상 점검 관리해야 함

2.6.

Server(Windows)

2.6. Server(Windows)

계정 관리(8개 항목), 서비스 관리(10개 항목), 패치 및 로그 관리(5개 항목), 보안 관리(9개 항목) 총 4개 영역에서 32개 항목으로 구성된다.

[표 6] Server(Windows) 진단 체크리스트

구분	진단 항목
가. 계정 관리	Administrator 계정 이름 바꾸기
	Guest 계정 상태
	불필요한 계정 제거
	계정 잠금 임계값 설정
	패스워드 최대 사용 기간 설정
	암호 사용 기간 제한없음 제거
	해독 가능한 암호화를 사용하여 암호 저장
	관리자 그룹에 최소한의 사용자 포함
나. 서비스 관리	공유 권한 및 사용자 그룹 설정
	하드디스크 기본 공유 제거
	불필요한 서비스 제거
	NetBIOS 바인딩 서비스 구동 점검
	FTP 서비스 구동 점검
	FTP 디렉터리 접근 권한 설정
	Anonymous FTP 금지
	FTP 접근 제어 설정
	DNS Zone Transfer 설정
	RDS(RemoteDataServices) 제거
다. 패치 및 로그 관리	최신 서비스팩 적용
	최신 Hot Fix 적용
	백신 프로그램 업데이트
	로그의 정기적 검토 및 보고
	원격으로 접근 할 수 있는 레지스트리 경로
라. 보안 관리	백신 프로그램 설치
	SAM 파일 접근 통제 설정
	화면보호기
	로그인하지 않고 시스템 종료 허용
	원격 시스템에서 강제로 시스템 종료
	보안 감사를 로그할 수 없는 경우 시스템 종료
	SAM 계정과 공유의 익명 열거 허용 안함
	Autologon기능 제어
	이동식 미디어 포맷 및 꺼내기 허용

Administrator 계정 이름 바꾸기

항목설명

일반적으로 관리자 계정을 Administrator로 설정한 경우 로그인 시도 실패 횟수의 제한이 없는 점을 이용해 악의적인 사용자가 패스워드 유추 공격을 끊임없이 시도할 수 있다. 공격자가 관리자 패스워드뿐만 아니라 계정 이름을 쉽게 유추하지 못하도록 Administrator 계정 이름을 변경해야 한다.

진단 기준

양호

Administrator 외의 다른 계정 이름으로 변경하여 사용하는 경우

취약

Administrator 계정 이름을 변경하지 않고 사용하는 경우

진단 방법

[CLI]

■ 명령 프롬프트에서 확인

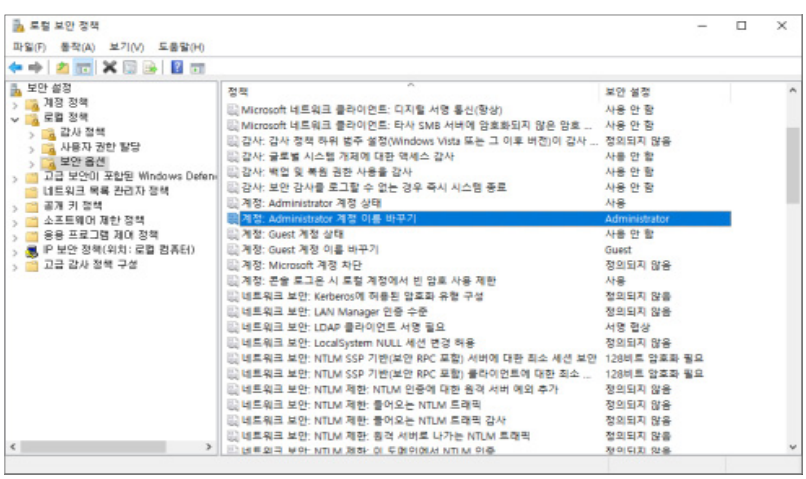
시작 → 실행 → cmd → net user 명령어 실행 후 Administrator 계정의 존재 유무 확인

```
C:\Users\Administrator>net user

User accounts for \\WIN-TUDGRKMVQCE

-------------------------------------------------------------------------------
Administrator            DefaultAccount           Guest
test                     WDAGUtilityAccount
The command completed successfully.
```

[GUI]

■ 로컬 보안 정책에서 확인

시작 → 프로그램 → 관리도구 → 로컬 보안 정책 → 로컬 정책 → 보안 옵션 → "계정: Administrator 계정 이름 바꾸기"의 값을 확인



조치 방법

[CLI]

■ 명령 프롬프트에서 변경

시작 → 실행 → cmd → wmic UserAccount where Name="administrator" call Rename Name="변경할 계정명" 명령어 입력

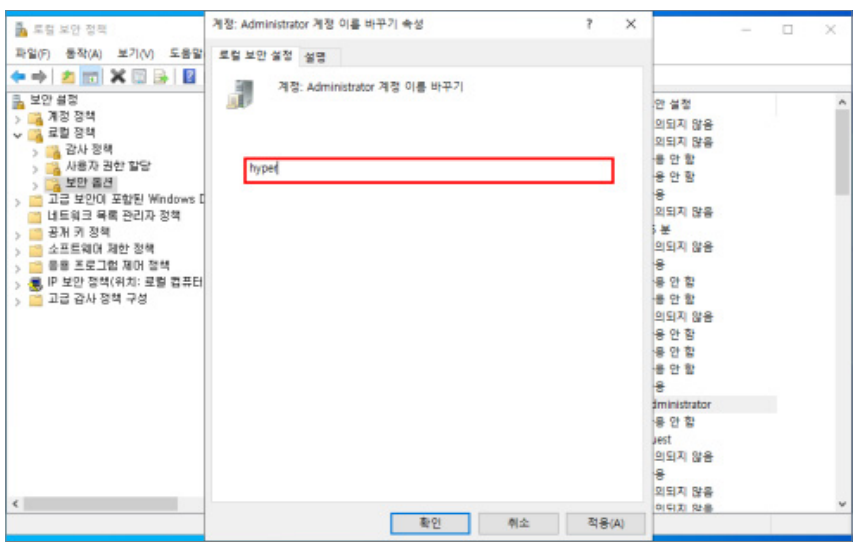
※ cmd를 관리자 권한으로 실행

```
C:\Users\Administrator>wmic UserAccount where Name="administrator" call Rename Name="hyper"
Executing (\\WIN-TUDGRKMVQCE\ROOT\CIMV2:Win32_UserAccount.Domain="WIN-TUDGRKMVQCE",Name="administrator")->Rename()
Method execution successful.
Out Parameters:
instance of __PARAMETERS
{
        ReturnValue = 0;
};

C:\Users\Administrator>
```

[GUI]

■ 로컬 보안 정책에서 변경

시작 → 프로그램 → 관리도구 → 로컬 보안 정책 → 로컬 정책 → 보안 옵션 → "계정: Administrator 계정 이름 바꾸기"에서 계정 이름 변경



Guest 계정 상태

항목설명

Guest 계정은 시스템 임시 접근을 허용하는 취약한 계정으로써, 사용을 제한해야한다. 불특정 다수의 접근이 필요할 경우 Guest 계정이 아닌 일반 사용자 계정을 생성해 사용하도록 해야한다.

진단 기준

양호

Guest 계정이 비활성화되어 있는 경우

취약

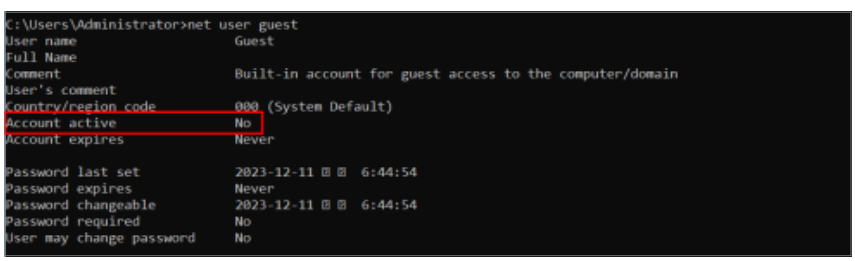
Guest 계정이 활성화되어 있는 경우

진단 방법

[CLI]

■ 명령 프롬프트에서 확인

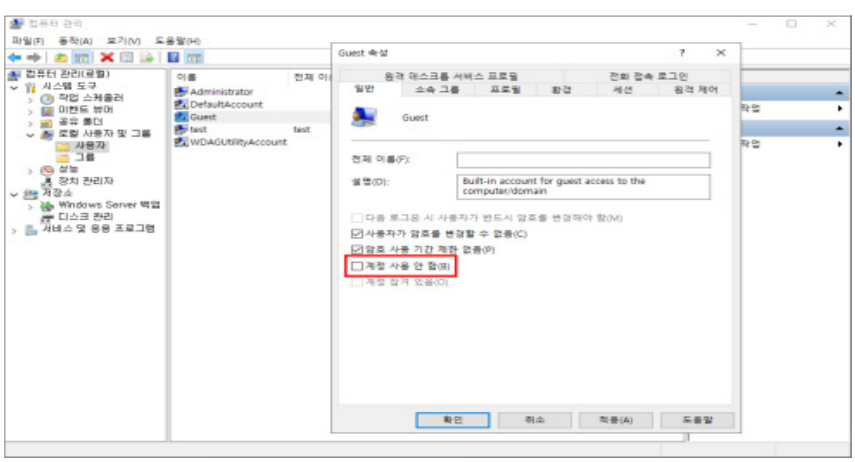
1. 시작 → 실행 → cmd → net user guest 명령어 실행 → “활성 계정” 상태 확인



[GUI]

■ 로컬 보안 정책에서 확인

1. 시작 → 프로그램 → 관리도구 → 컴퓨터 관리 → 로컬 사용자 및 그룹 → 사용자 → Guest 속성 → "계정 사용 안함" 체크 유무 확인



조치 방법

[CLI]

■ 명령 프롬프트에서 변경

시작 → 실행 → cmd → net user guest /active:no 명령어 실행

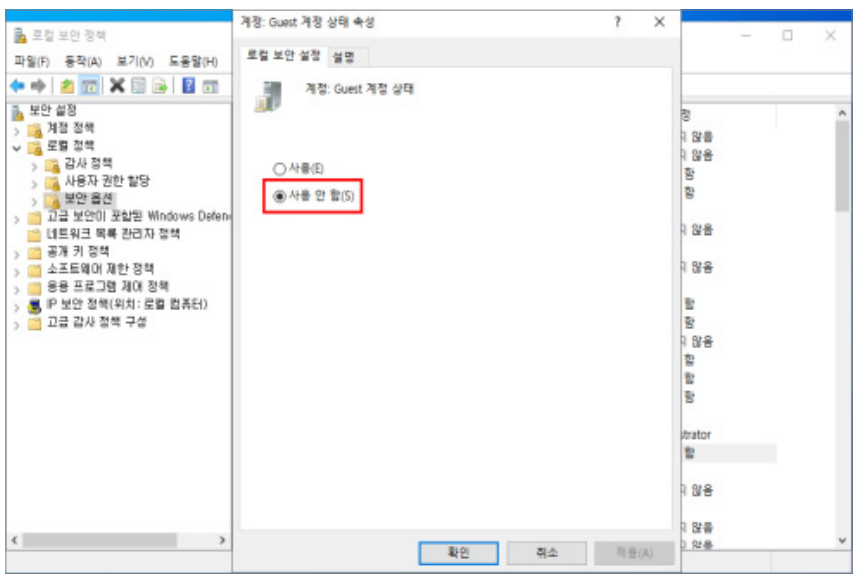
※ cmd를 관리자 권한으로 실행

```
C:\Users\Administrator>net user guest /active:no
The command completed successfully.
```

[GUI]

■ 로컬 보안 정책에서 변경

시작 → 프로그램 → 관리도구 → 로컬 보안 정책 → 로컬 정책 → 보안 옵션 →
"계정: Guest 계정 상태 속성"에서 "사용 안 함"



불필요한 계정 제거

항목설명

퇴직, 휴직 등의 이유로 사용하지 않는 계정, 불필요한 계정, 의심스러운 계정이 존재하는지 점검한다. 관리되지 않은 불필요한 계정은 장기간 패스워드가 변경되지 않아 *무작위 대입 공격(Brute Force Attack)이나 패스워드 추측 공격(Password Guessing)에 의해 계정 정보가 유출되어도 인지하기 어렵다.

진단 기준

양호
불필요한 계정이 존재하지 않을 경우

취약
불필요한 파일이 존재할 경우

진단 방법

[CLI]

■ 명령 프롬프트에서 확인

시작 → 실행 → cmd → net user 명령어 실행 후 사용자 계정 점검

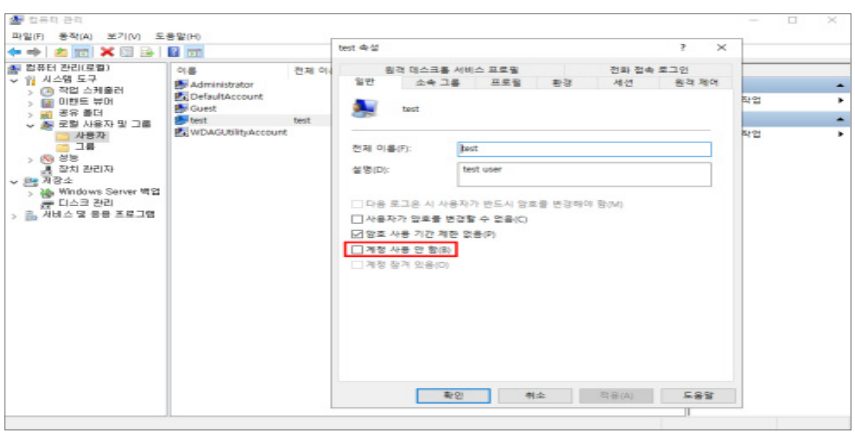
```
C:\Users\Administrator>net user

User accounts for \\WIN-TUDGRKMVQCE

-------------------------------------------------------------------------------
Administrator            DefaultAccount           Guest
test                     WDAGUtilityAccount
The command completed successfully.
```

※ 인터뷰를 통해 계정별 용도 확인이 필요함

[GUI]

■ 로컬 보안 정책에서 확인

시작 → 프로그램 → 관리도구 → 컴퓨터 관리 → 시스템 도구 → 로컬 사용자 및 그룹 → 사용자 → "계정 사용 안함" 체크 유무 확인



조치 방법

[CLI]

■ 명령 프롬프트에서 변경

시작 → 실행 → cmd → net user "제거할 계정명" /delete를 입력하여 삭제

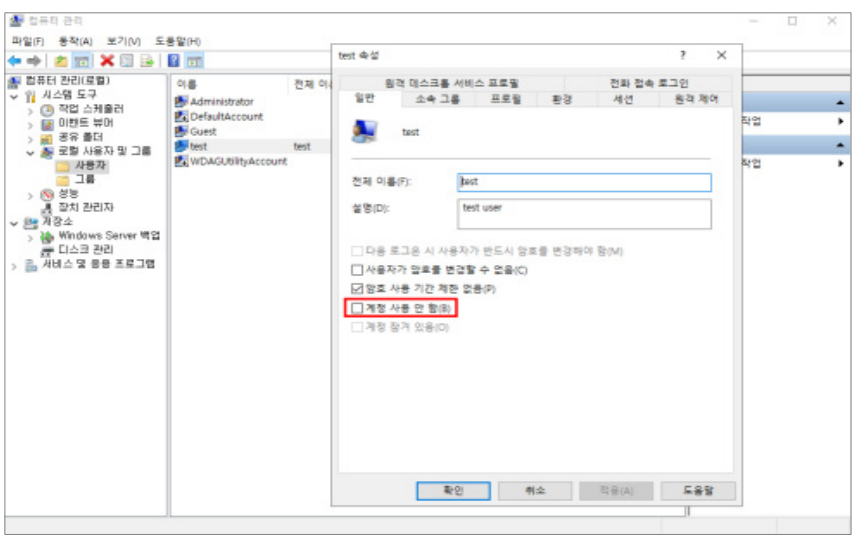
※ cmd를 관리자 권한으로 실행

```
C:\Users\Administrator>net user test-user /delete
The command completed successfully.


C:\Users\Administrator>net user

User accounts for \\WIN-TUDGRKMVQCE

-------------------------------------------------------------------------------
Administrator            DefaultAccount           Guest
test                     WDAGUtilityAccount
The command completed successfully.
```

[GUI]

■ 로컬 보안 정책에서 변경

시작 → 프로그램 → 관리도구 → 컴퓨터 관리 → 로컬 사용자 및 그룹 → 사용자 → 속성 → "계정 사용 안 함"에 체크 하거나 계정 삭제



※ 불필요한 계정은 삭제하는 것을 권고함

계정 잠금 임계값 설정

항목설명

계정 잠금 임계값을 설정하지 않을 경우, 무제한으로 로그인 시도가 가능하며 공격자는 계정을 탈취할 때까지 암호대입 공격을 지속적으로 시도할 수 있다.

진단 기준

양호

계정 잠금 임계값이 5번 이하로 설정되어 있는 경우

취약

계정 잠금 임계값이 5번 초과로 설정되어 있거나 설정되어 있지 않은 경우

진단 방법

[CLI]

■ 명령 프롬프트에서 확인

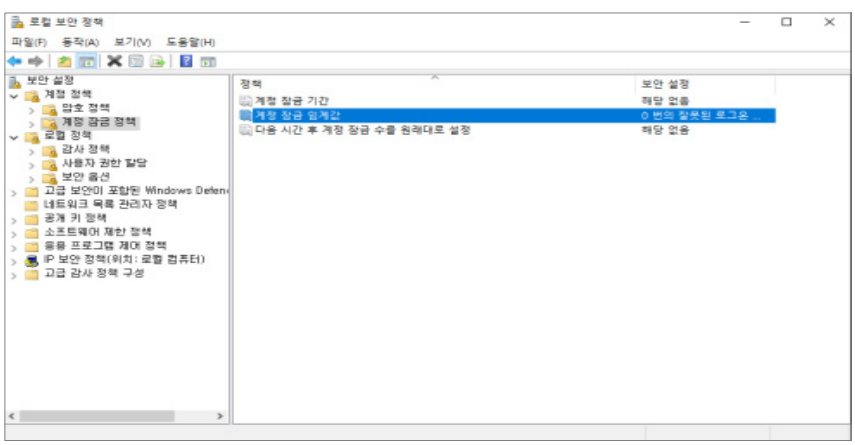
시작 → 실행 → cmd → net accounts 명령어 실행 후 계정 잠금 임계값 설정 확인

```
C:\Users\Administrator>net accounts
Force user logoff how long after time expires?:       Never
Minimum password age (days):                          0
Maximum password age (days):                          42
Minimum password length:                              0
Length of password history maintained:                None
Lockout threshold:                                    Never
Lockout duration (minutes):                           30
Lockout observation window (minutes):                 30
Computer role:                                        SERVER
The command completed successfully.
```

[GUI]

■ 로컬 보안 정책에서 확인

시작 → 프로그램 → 관리도구 → 로컬 보안 정책 → 계정 정책 → 계정 잠금 정책 → "계정 잠금 임계값" 설정 확인



조치 방법

[CLI]

■ 명령 프롬프트에서 변경

시작 → 실행 → cmd → net accounts /lockoutthreshold:5 명령어 실행

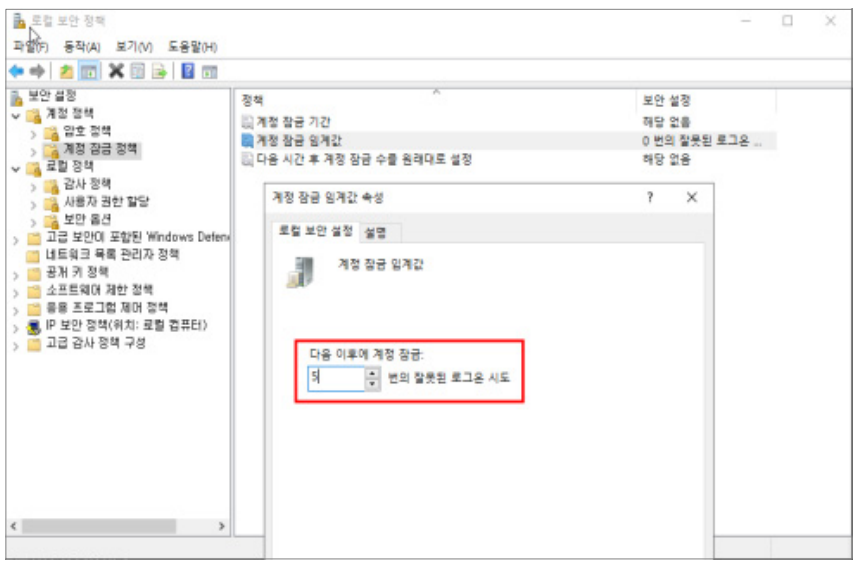
※ cmd를 관리자 권한으로 실행

```
C:₩>net accounts /lockoutthreshold:5
명령을 잘 실행했습니다.
```

[GUI]

■ 로컬 보안 정책에서 변경

시작 → 프로그램 → 관리도구 → 로컬 보안 정책 → 계정 정책 → 계정 잠금 정책 → "계정 잠금 임계값"을 5번 이하로 설정



패스워드 최대 사용 기간 설정

항목설명

모든 암호는 추측 공격으로 유출될 수 있으므로, 패스워드의 사용 기간이 길어질수록 패스워드 유출 및 계정 탈취 가능성이 높아진다. 패스워드를 주기적으로 바꾸도록 사용 기간을 설정하면 유출된 패스워드에 의한 보안사고 위험을 줄일 수 있다.

진단 기준

양호
최대 암호 사용 기간이 90일 이하일 경우

취약
최대 암호 사용 기간이 90일 초과일 경우

진단 방법

[CLI]

■ 명령 프롬프트에서 확인

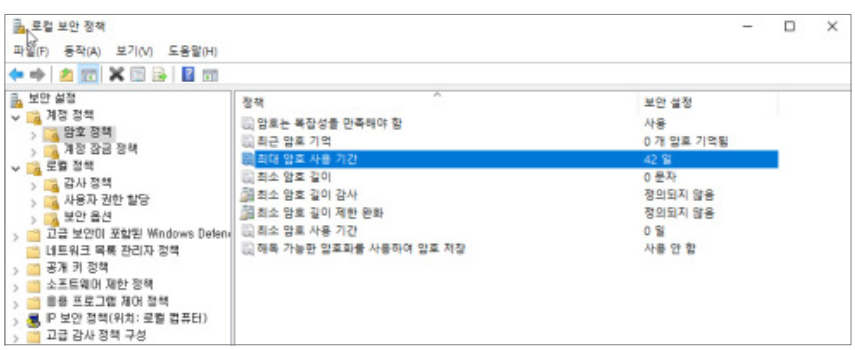
1. 시작 → 실행 → cmd → secedit /export /cfg /c:\cfg.txt 명령어 실행
2. 탐색기 → c:\cfg.txt 파일을 열어서 MaximumPasswordAge 설정값이 90일 이하로 설정되어 있는지 확인

```
1  [Unicode]
2  Unicode=yes
3  [System Access]
4  MinimumPasswordAge = 0
5  MaximumPasswordAge = 42
6  MinimumPasswordLength = 0
7  PasswordComplexity = 0
8  PasswordHistorySize = 0
9  LockoutBadCount = 0
```

[GUI]

■ 로컬 보안 정책에서 확인

시작 → 프로그램 → 로컬 보안 정책 → 계정 정책 → 암호 정책 → "최대 암호 사용 기간" 정책이 90일 이하로 설정되어 있는지 확인



조치 방법

[CLI]

■ 명령 프롬프트에서 변경

시작 → 실행 → cmd → net accounts /MAXPWAGE:90 명령어 실행

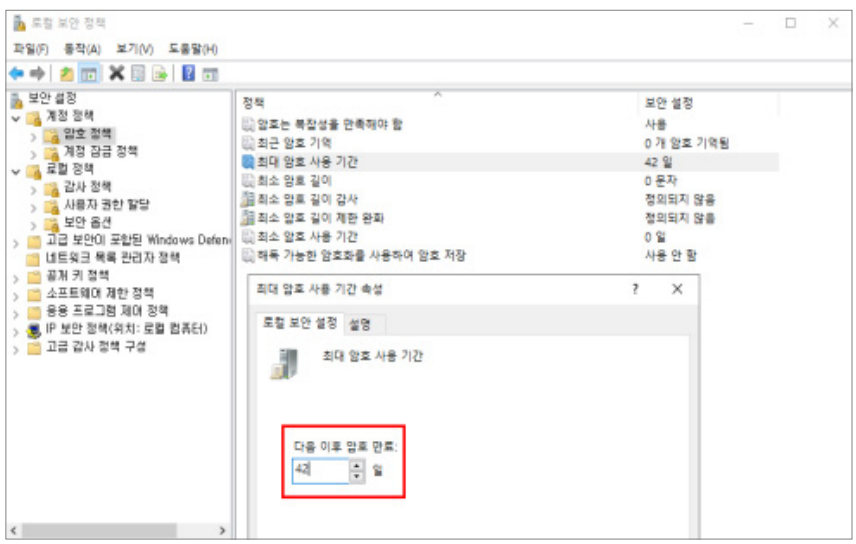
※ cmd를 관리자 권한으로 실행

```
C:₩test>net accounts /MAXPWAGE:90
명령을 잘 실행했습니다.
```

[GUI]

■ 로컬 보안 정책에서 변경

시작 → 프로그램 → 관리도구 → 로컬 보안 정책 → 계정 정책 → 암호 정책 → "최대 암호 사용 기간" 을 90일 이하로 설정



암호 사용 기간 제한없음 제거

항목설명

패스워드 최대 사용 기간을 설정하더라도, 패스워드 암호 사용 기간 제한없음 설정을 비활성화 시켜 주지 않으면 기능이 제대로 작동되지 않는다. 즉, 패스워드를 사용할 수 있는 기간에 대해 정책을 설정하면, 그 정책이 적용될 수 있도록 계정마다 암호 사용 기간 제한없음 설정을 비활성화 시켜주어야 한다.

진단 기준

양호

계정마다 암호 사용 기간 제한없음 설정이 비활성화되어 있는 경우

취약

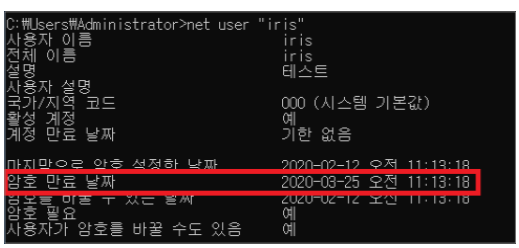
계정에 암호 사용 기간 제한없음 설정이 활성화되어 있는 경우

진단 방법

[CLI]

■ 명령 프롬프트에서 확인

시작 → 실행 → cmd → net user "계정명" 명령어를 입력하여 "암호 만료 날짜" 설정 확인

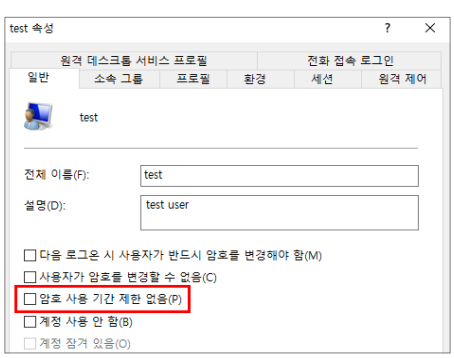


※ Windows Server에 존재하는 계정 중 '활성 계정' 여부를 먼저 확인한 후, 암호 만료 일자 설정을 파악해야 함

[GUI]

■ 컴퓨터 관리에서 확인

시작 → 프로그램 → 관리도구 → 컴퓨터 관리 → 로컬 사용자 및 그룹 → 사용자 → 설정할 계정 선택 → '속성'에서 "암호 사용 기간 제한 없음"이 해제되어 있는지 확인



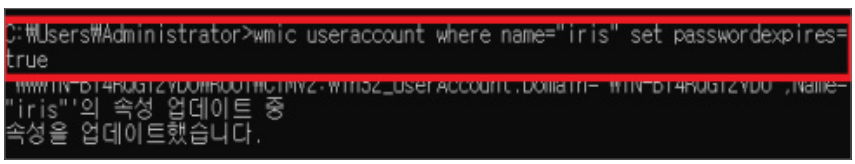
조치 방법

[CLI]

■ 명령 프롬프트에서 변경

시작 → 실행 → cmd → wmic useraccount where name="계정명" set passwordexpires=true 명령어 입력

※ cmd를 관리자 권한으로 실행



[GUI]

■ 로컬 보안 정책에서 변경

시작 → 프로그램 → 관리도구 → 컴퓨터 관리 → 로컬 사용자 및 그룹 → 사용자 → 설정할 계정 선택 → 속성에서 "암호 사용 기간 제한 없음" 해제

해독 가능한 암호화를 사용하여 암호 저장

항목설명

인증을 위해 사용자 암호를 알아야 하는 응용 프로그램 프로토콜이 지원될 경우 해독 가능한 방식으로 암호를 저장하기 때문에 암호공격을 이용한 공격자가 노출된 계정을 사용하여 네트워크 리소스에 로그인할 수 있다.

진단 기준

양호

"해독 가능한 암호화를 사용하여 암호 저장" 정책이 "사용 안 함"으로 설정되어 있을 경우

취약

"해독 가능한 암호화를 사용하여 암호 저장" 정책이 "사용"으로 설정되어 있을 경우

진단 방법

[CLI]

■ 명령 프롬프트에서 확인

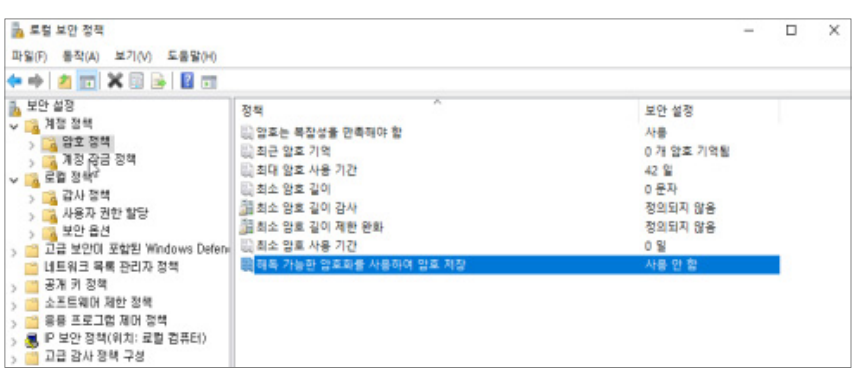
1. 시작 → 실행 → cmd → secedit /export /cfg c:\cfg.txt 명령어 실행
2. 탐색기 → cfg.txt 파일을 열어서 ClearTextPassword 설정값이 1로 되어있는지 확인 (0일 경우 양호, 1일 경우 취약)

```
[Unicode]
Unicode=yes
[System Access]
MinimumPasswordAge = 0
MaximumPasswordAge = 42
MinimumPasswordLength = 0
PasswordComplexity = 0
PasswordHistorySize = 0
LockoutBadCount = 0
RequireLogonToChangePassword = 0
ForceLogoffWhenHourExpire = 0
NewAdministratorName = "Admin"
NewGuestName = "Guest"
ClearTextPassword = 0
LSAAnonymousNameLookup = 0
```

[GUI]

■ 로컬 보안 정책에서 확인

시작 → 프로그램 → 관리도구 → 로컬 보안 정책 → 계정 정책 → 암호 정책 → "해독 가능한 암호화를 사용하여 암호 저장" 설정 확인



조치 방법

[CLI]

■ 명령 프롬프트에서 변경

1. 탐색기 → cfg.txt 파일을 열어서 ClearTextPassword 설정 값을 0으로 변경
2. 시작 → 실행 → cmd.exe → secedit /configure /db C:\cfg.sdb /cfg C:\cfg.txt 명령어 실행

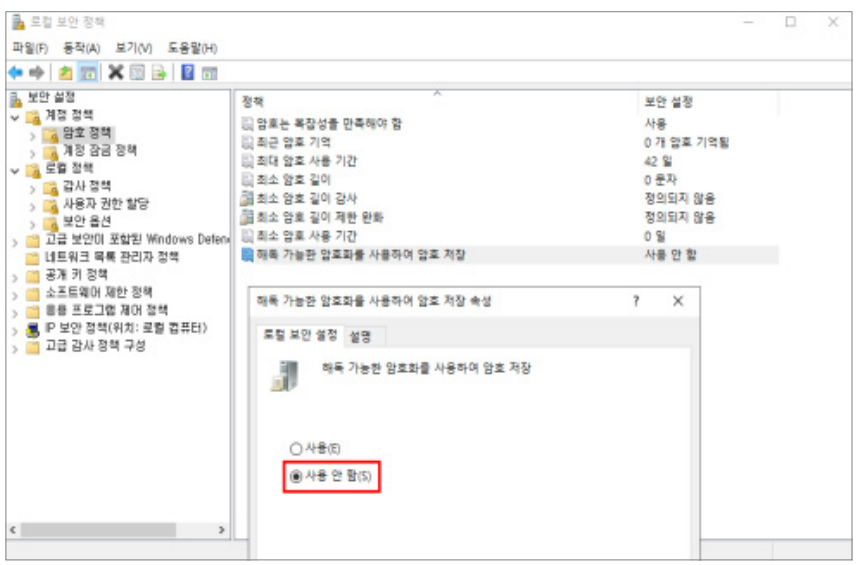
※ cmd를 관리자 권한으로 실행

```
c:₩>secedit /configure /db C:₩cfg.sdb /cfg C:₩cfg.txt

작업을 성공적으로 완료했습니다.
자세한 정보는 %windir%₩security₩logs₩scesrv.log를 참조하십시오.
```

[GUI]

■ 로컬 보안 정책에서 변경

시작 → 프로그램 → 관리도구 → 로컬 보안 정책 → 계정 정책 → 암호 정책 → "해독 가능한 암호화를 사용하여 암호 저장"을 "사용 안 함"으로 설정



관리자 그룹에 최소한의 사용자 포함

항목설명

일반 사용자에 의한 시스템 피해를 최소화하기 위해, 관리 업무를 위한 계정과 일반 업무를 위한 계정을 분리하여 사용해야 하며, 관리자 그룹에 최소한의 관리자만 포함하도록 한다.

진단 기준

양호

Administrators 그룹에 불필요한 관리자 계정이 존재하지 않은 경우

취약

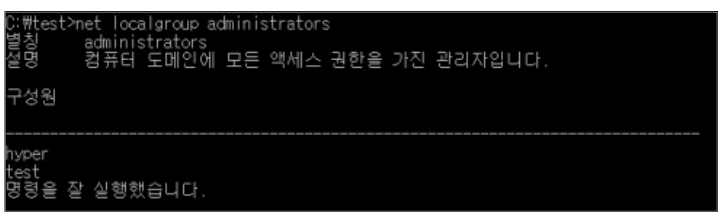
Administrators 그룹에 불필요한 관리자 계정이 존재하는 경우

진단 방법

[CLI]

■ 명령 프롬프트에서 확인

시작 → 실행 → cmd → net localgroup administrators 명령어 실행

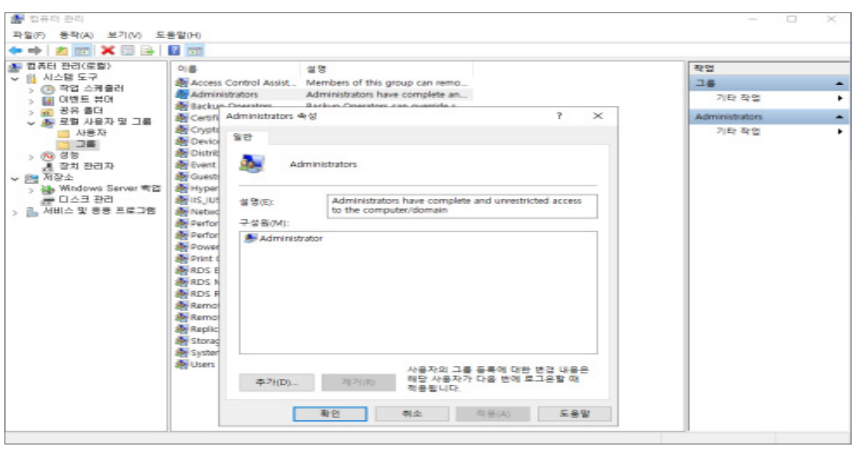


※ 인터뷰를 통해 존재하는 계정의 용도를 파악하고, 불필요한 계정이 있는 경우, 제거하도록 권고함

[GUI]

■ 컴퓨터 관리에서 확인

시작 → 프로그램 → 관리도구 → 컴퓨터 관리 → 로컬 사용자 및 그룹 → 그룹 → Administrators 선택 확인



조치 방법

[CLI]

■ 명령 프롬프트에서 변경

시작 → 실행 → cmd → net localgroup administrators 삭제할 계정명 /del 명령어 입력

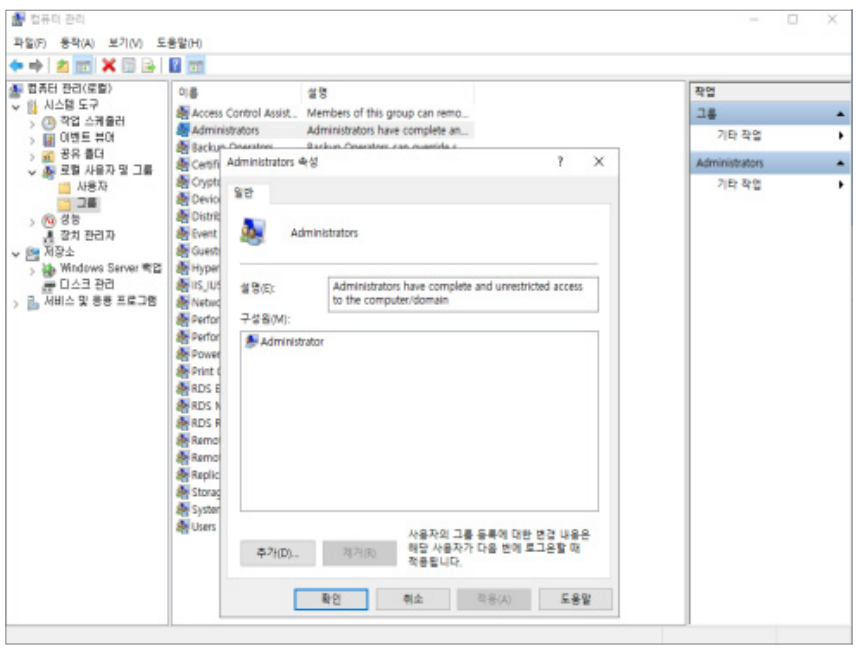
```
C:₩test>net localgroup administrators test /del
명령을 잘 실행했습니다.
```

※ cmd를 관리자 권한으로 실행

[GUI]

■ 컴퓨터 관리에서 변경

시작 → 프로그램 → 관리도구 → 컴퓨터 관리 → 로컬 사용자 및 그룹 → 그룹 → Administrators 선택 → 불필요한 계정 제거



공유 권한 및 사용자 그룹 설정

항목설명

Everyone이 공유계정에 포함되어 있을 경우, 익명 사용자의 접근이 가능함으로, 디폴트 공유인 C$, D$, Admin$, IPC$ 등을 제외한 공유 폴더에 everyone 그룹으로 공유 금지 여부를 점검한다.

진단 기준

양호

일반 공유 디렉터리가 없거나 공유 디렉터리 접근 권한에 Everyone이 없는 경우

취약

일반 공유 디렉터리의 공유 사용 권한에 Everyone이 있는 경우

진단 방법

[CLI]

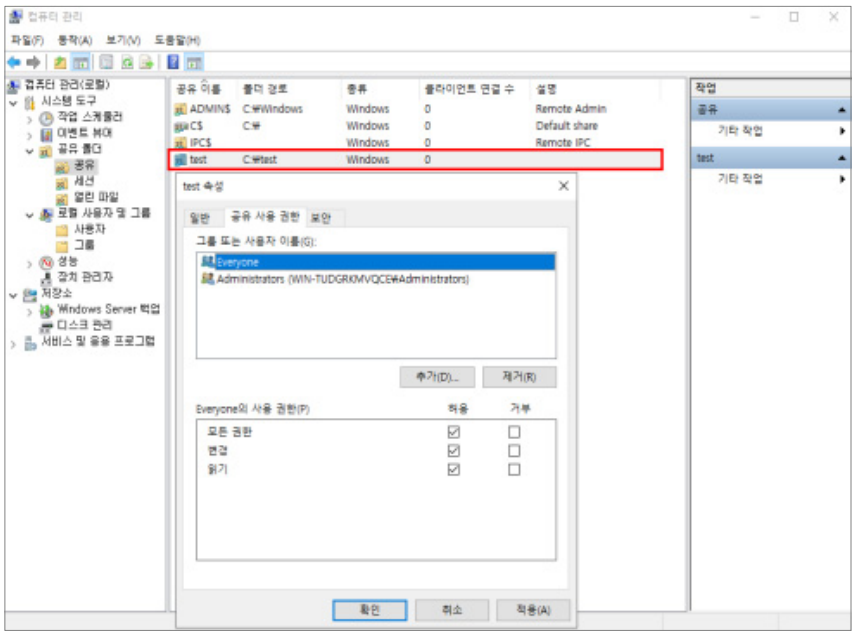
■ 명령 프롬프트에서 확인

1. 시작 → 실행 → cmd → net share 명령어 입력 (C$, D$, Admin$, IPC$ 등을 제외한 일반 공유 폴더가 존재하지 않으면 양호)
2. 위 1번 항목에서 C$, D$, Admin$, IPC$ 등을 제외한 일반 공유 폴더가 존재하는 경우 시작 → 실행 → cmd → net share 공유이름 명령어 입력 후 'Everyone으로 된 공유가 존재하는지 확인 (Everyone 공유가 존재하지 않으면 양호)

[GUI]

■ 컴퓨터 관리에서 확인

1. 시작 → 프로그램 → 관리도구 → 컴퓨터 관리 → 공유 폴더 → '공유'에서 일반 공유 폴더가 존재하는지 확인 (C$, D$, Admin$, IPC$ 등을 제외한 일반 공유 폴더가 존재하지 않으면 양호)
2. 위 1번 항목에서 C$, D$, Admin$, IPC$ 등을 제외한 일반 공유 폴더가 존재하는 경우. 일반 공유 폴더 → 속성 → 공유 사용 권한 탭에서 'Everyone'으로 된 공유가 존재하는지 확인 (Everyone 공유가 존재하지 않으면 양호)



조치 방법

[CLI]

■ 명령 프롬프트에서 변경

1. 시작 → 실행 → cmd → net share 공유이름 /delete 명령어 입력
2. cmd → net share 공유이름 = 드라이브 경로 /grant:계정명,권한 명령어 입력

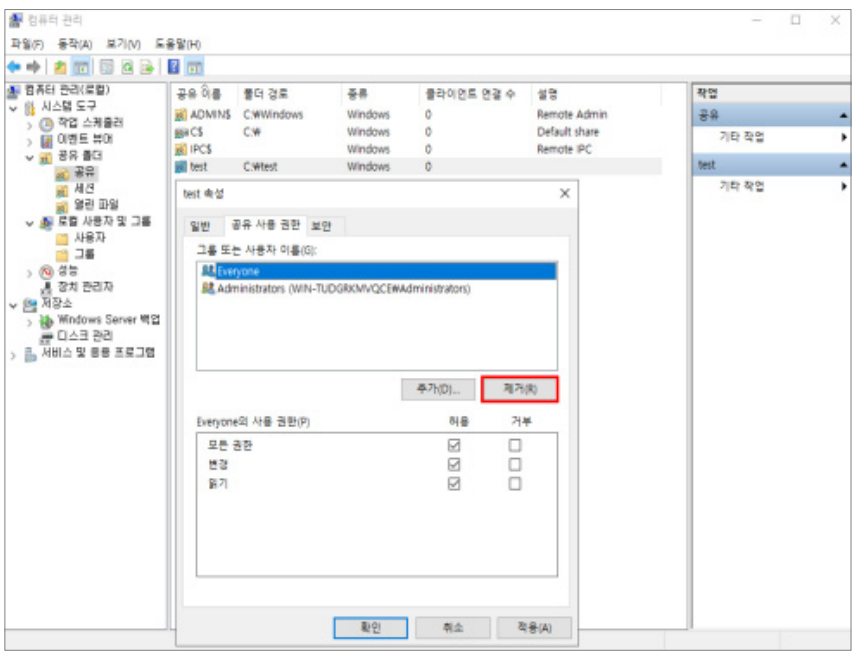
※ 권한의 종류는 READ(읽기), CHANGE(변경), FULL(읽기 및 변경)으로 권한에 따라 적절히 적용
※ 적용할 계정이 여러개 있을 시 /grant:계정명,권한을 여러개 붙여서 사용
EX) net share test=C:\test /grant:test1,read /grant:test2,full
※ cmd를 관리자 권한으로 실행

```
C:₩Users₩Administrator>net share everyone /delete
everyone이(가) 제거되었습니다.

C:₩Users₩Administrator>net share everyone=C:₩everyone /grant:test,full
everyone이(가) 공유되었습니다.

C:₩Users₩Administrator>net share everyone
공유 이름            everyone
경로                 C:₩everyone
설명
최대 사용자 수       제한 없음
사용자
캐싱                 문서의 수동 캐시
사용 권한            WIN-YC2UBF3UUVG₩test, FULL

명령을 잘 실행했습니다.
```

[GUI]

■ 컴퓨터 관리에서 변경

시작 → 프로그램 → 관리도구 → 컴퓨터 관리 → 공유 폴더 → 공유 → 일반 공유 폴더 선택 → 속성 → 공유 사용 권한 탭에서 Everyone으로 된 공유를 제거하고, 접근이 필요한 계정의 권한만 추가



하드디스크 기본 공유 제거

항목설명

시스템의 기본공유 항목이 제거되지 않게 되면 모든 시스템 자원에 접근할 수 있는 위험한 상황이 발생할 수 있다. 예전에 발생한 Nimda 바이러스도 여러 가지 방법 중에서 이러한 공유기능을 침투의 한 경로로 이용한 것으로 기본공유를 제거해야 한다.

진단 기준

양호

AutoShareServer 값이 0이며,
기본공유가 존재하지 않을 경우

취약

AutoShareServer 값이 1 이거나
기본공유가 존재하는 경우

진단 방법

[CLI]

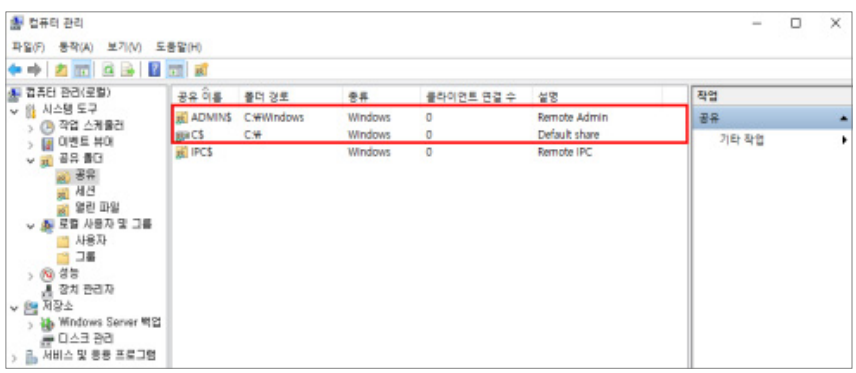
■ 명령 프롬프트에서 확인

시작 → 실행 → cmd → net share 명령어 실행 후 기본 공유가 존재하는지 확인

[GUI]

■ 컴퓨터 관리에서 확인

시작 → 프로그램 → 관리도구 → 컴퓨터 관리 → 공유 폴더 → 공유에서 기본 공유 확인



조치 방법

[CLI]

■ 명령 프롬프트에서 변경

시작 → 실행 → cmd → net share 삭제할 공유 이름 /del 명령어 실행

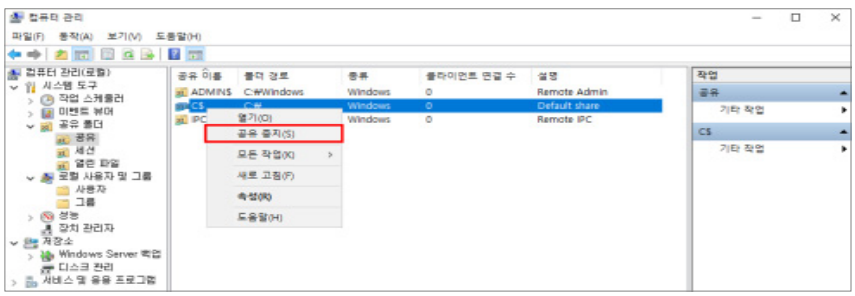
※ cmd를 관리자 권한으로 실행
※ cmd에서 설정을 변경할 경우 프로그램 재시작 후 기본공유가 다시 생성되므로 영구적인 제거가 불가능함

```
C:₩Users₩Administrator>net share C$ /del
C$이(가) 제거되었습니다.
```

[GUI]

■ 컴퓨터 관리에서 변경

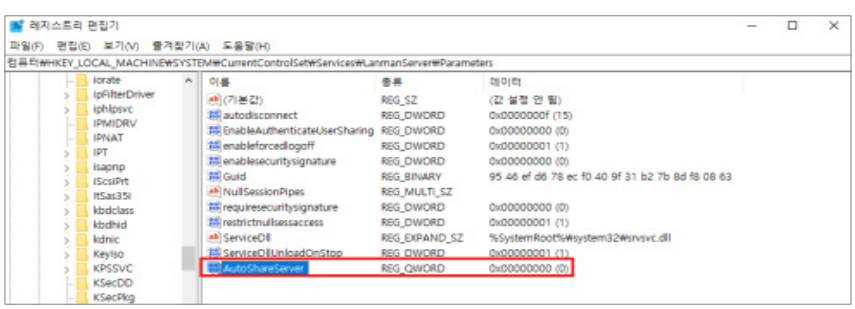
시작 → 프로그램 → 관리도구 → 컴퓨터 관리 → 공유 폴더 → '공유'에서 불필요한 기본공유에 대해 "공유 중지" 설정



[레지스트리]

■ 레지스트리에서 변경

시작 → 실행 → regedit → HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\lanmanserver\parameters 에서 AutoShareServer 의 값을 0으로 수정
(AutoShareServer 설정이 존재하지 않을 경우 DWORD로 새로 만들기)



※ 레지스트리 값을 수정해야만 영구적인 기본공유 중지 적용이 가능함
※ IPC$는 중지할 경우, 네트워크 서비스에 문제가 발생할 가능성이 존재하므로 제거를 권고하지 않음
※ IPC$를 제외한 나머지 기본공유는 제거해야 함

불필요한 서비스 제거

항목설명

일반적으로 시스템에는 필요하지 않고 취약한 서비스들이 디폴트로 설치되어 실행되고 있으며, 해당 서비스 또는 응용 프로그램은 공격 목표가 될 수 있으므로, 불필요한 서비스는 사용하지 않거나 제거해야한다.

진단 기준

양호

아래 서비스가 중지되어있는 경우

취약

아래 서비스가 구동 중인 경우
- Alerter(서버에서 클라이언트로 경고 메시지를 보냄)
- Clipbook(서버 내 Clipbook을 다른 클라이언트와 공유)
- Messenger(net send 명령어를 이용하여 클라이언트에 메시지 보냄)
- Simple TCP/IP Services(Echo, Discard, Character Generator, Daytime, Quote of the Day)

진단 방법

[CLI]

■ 명령 프롬프트에서 확인

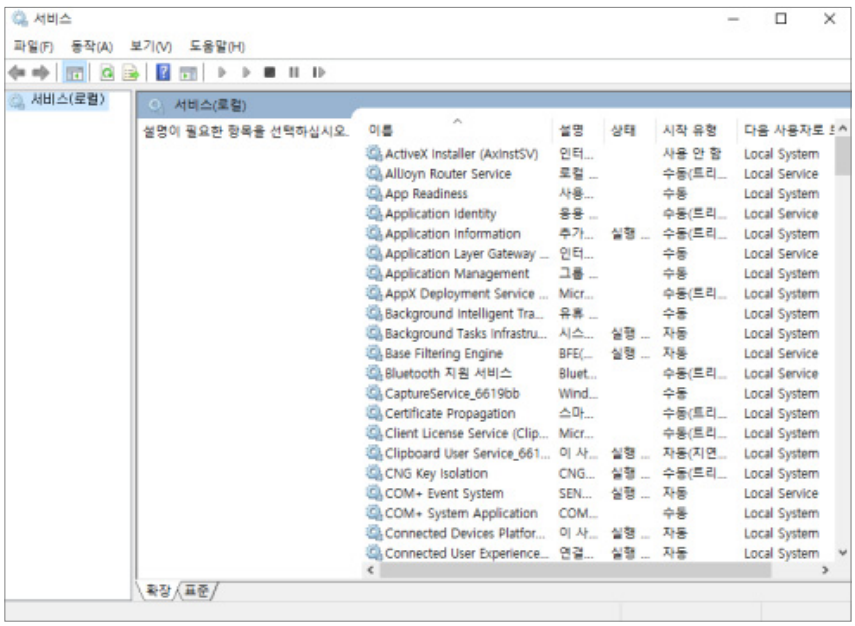
시작 → 실행 → cmd → net start 명령어 실행 후 확인

```
C:\Users\Administrator>net start
These Windows services are started:

   Application Information
   Background Tasks Infrastructure Service
   Base Filtering Engine
   Clipboard User Service_6619bb
   CNG Key Isolation
   COM+ Event System
   Connected Devices Platform User Service_6619bb
   Connected User Experiences and Telemetry
   CoreMessaging
   Credential Manager
   Cryptographic Services
   DCOM Server Process Launcher
   Device Install Service
   DHCP Client
   Diagnostic Policy Service
   Diagnostic System Host
   Distributed Link Tracking Client
   Distributed Transaction Coordinator
```

[GUI]

■ 서비스에서 확인

시작 → 관리도구 → 서비스에서 확인



조치 방법

[CLI]

■ 명령 프롬프트에서 변경

1. 시작 → 실행 → cmd → net stop 서비스명 명령어 실행
2. cmd → sc config 서비스명 start= disabled 명령어 실행

※ cmd를 관리자 권한으로 실행

[GUI]

■ 컴퓨터 관리에서 변경

1. 시작 → 관리도구 → 서비스 → 해당 서비스 더블 클릭
2. 일반 → 시작 유형 → "사용 안 함"으로 설정

NetBIOS 바인딩 서비스 구동 점검

항목설명

NetBIOS(Network Basic Input/Output System)은 IBM PC를 위한 네트워크 인터페이스 체계로 네임, 세션 데이터그램의 세가지 서비스를 제공하고 있다. 윈도우 NT 시스템이 인터넷에 직접 연결되어 있는 경우, 공격자가 쉽게 파일 시스템을 사용할 수 있으므로 NetBIOS에 대한 접근 통제가 필요하다.

진단 기준

양호

TCP/IP와 NetBIOS 간의 바인딩이 제거되어 있는 경우

취약

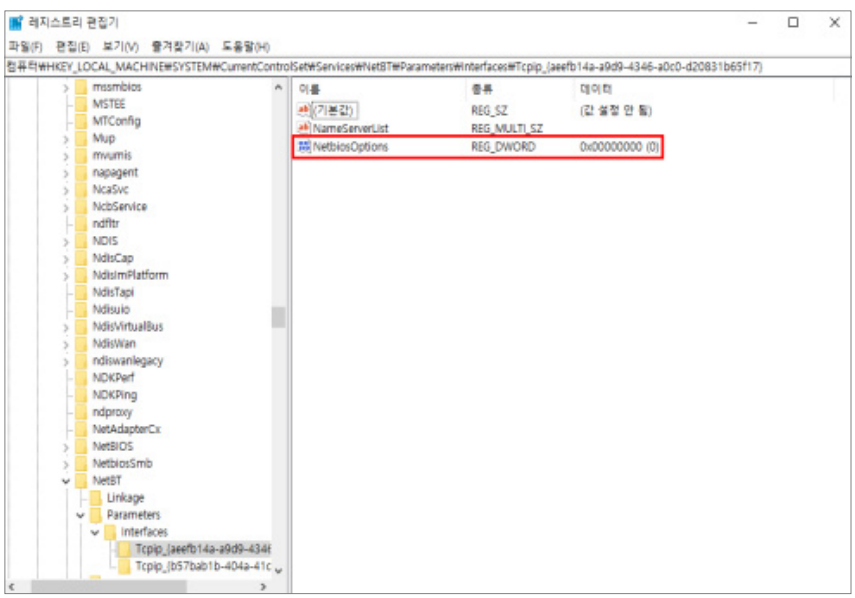
TCP/IP와 NetBIOS 간의 바인딩이 제거되어 있지 않은 경우

진단 방법

[레지스티리]

■ 레지스트리에서 확인

1. 시작 → 실행 → regedit → HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\NetBT\Parameters\Interfaces
2. Interfaces 폴더 마우스 우클릭 → 찾기 → NetbiosOptions 를 검색하여 해당 데이터 값이 2로 설정되어 있는지 확인 (값이 2로 설정되어 있을 경우 양호)

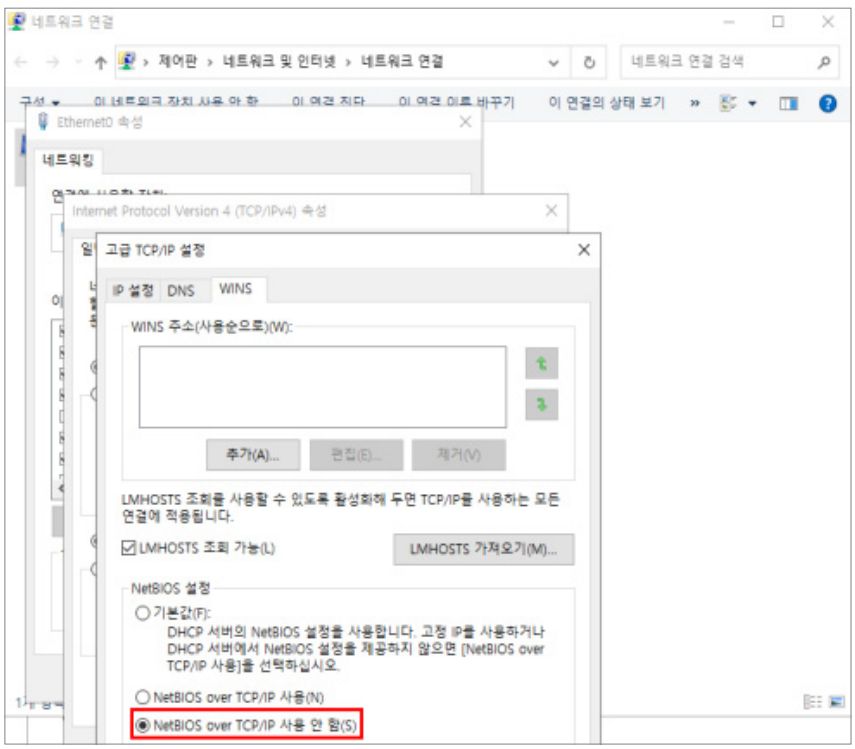


※ NetbiosOptions 옵션 값
NetbiosOptions = 0 : 기본 값 (DHCP 서버의 NetBIOS 사용)
NetbiosOptions = 1 : NetBIOS over TCP/IP 사용
NetbiosOptions = 2 : NetBIOS over TCP/IP 사용 안 함

[GUI]

■ 네트워크 및 공유 센터에서 확인

시작 → 제어판 → 네트워크 및 공유 센터 → 어댑터 설정 변경 → 해당 네트워크 어댑터 선택 후 마우스 오른쪽 버튼을 클릭하여 “속성” 선택 → 목록에서 "Internet Protocol Version 4 (TCP/IPv4)" 또는 "Internet Protocol Version 6 (TCP/IPv6)"를 찾아 선택한 다음 "속성" 선택 → 속성 창에서 “고급” 선택 → “WINS” 탭에서 NetBIOS 설정 확인
(설정이 "NetBIOS over TCP/IP 사용 안 함"으로 설정되어 있을 경우 양호)

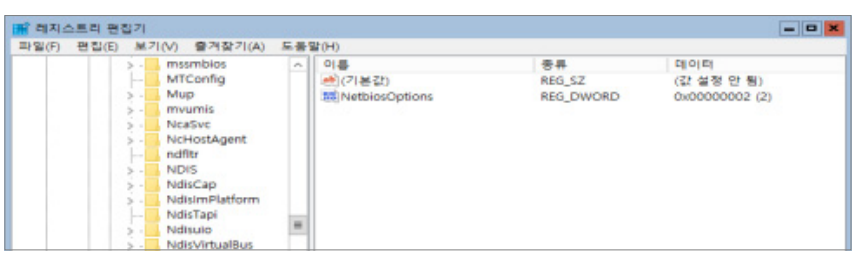


조치 방법

[레지스트리]

■ 레지스트리에서 변경

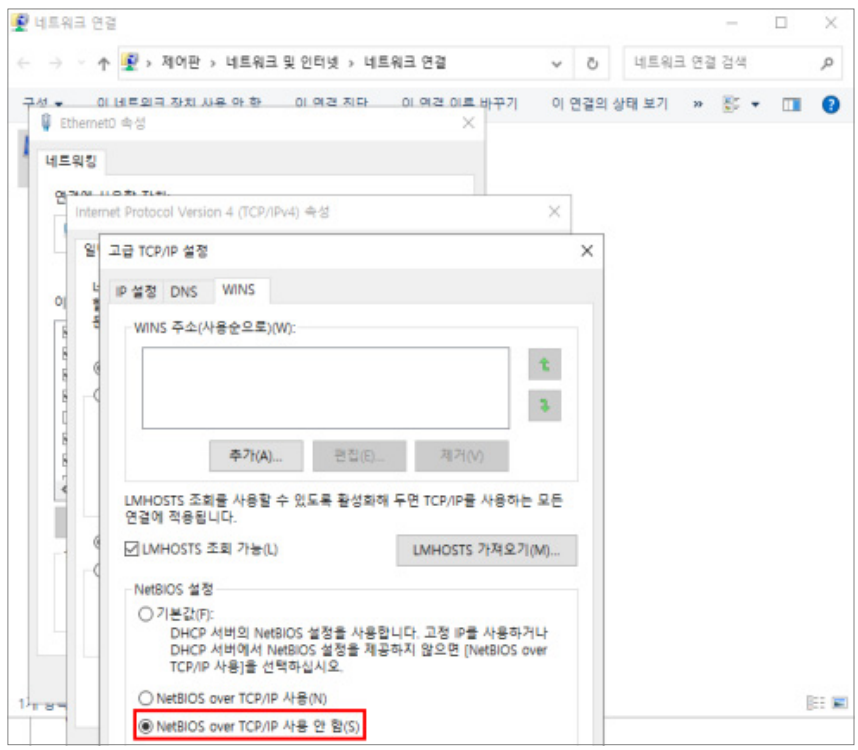
시작 → 실행 → regedit → HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\NetBT\Parameters\Interfaces에서 NetbiosOptions 데이터 값을 2로 변경



[GUI]

■ 네트워크 및 공유 센터에서 변경

시작 → 제어판 → 네트워크 및 공유 센터 → 어댑터 설정 변경 → 해당 네트워크 어댑터 선택 후 마우스 오른쪽 버튼을 클릭하여 “속성” 선택 → 목록에서 "Internet Protocol Version 4 (TCP/IPv4)" 또는 "Internet Protocol Version 6 (TCP/IPv6)"를 찾아 선택한 다음 "속성" 선택 → 속성 창에서 “고급” 선택 → “WINS” 탭에서 NetBIOS 설정을 “사용 안 함”으로 변경



FTP 서비스 구동 점검

항목설명

기본적인 FTP 서비스는 계정과 패스워드가 암호화되지 않은 채로 전송되므로 간단한 Sniffer에 의해서도 스니핑이 가능하기 때문에 보안이 취약한 FTP 서비스 사용을 지양한다.

진단 기준

양호
FTP 서비스가 구동 중이지 않은 경우

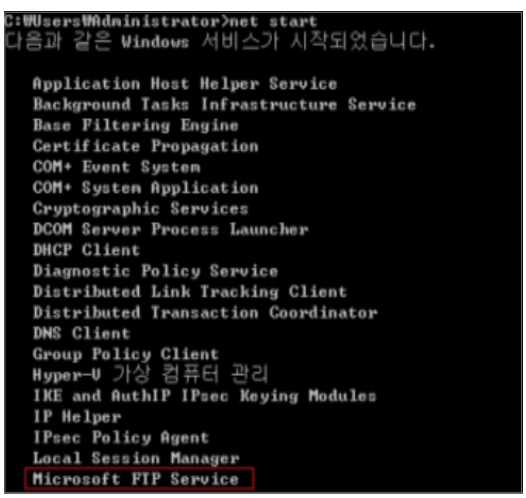
취약
FTP 서비스가 구동 중인 경우

진단 방법

[CLI]

■ 명령 프롬프트에서 확인

1. 시작 → 실행 → cmd → net start 명령어를 통해 FTP 서비스 구동 확인



[GUI]

■ 서비스에서 확인

시작 → 프로그램 → 관리도구 → 서비스 에서 FTP 서비스 구동 확인

조치 방법

[CLI]

■ 명령 프롬프트에서 변경

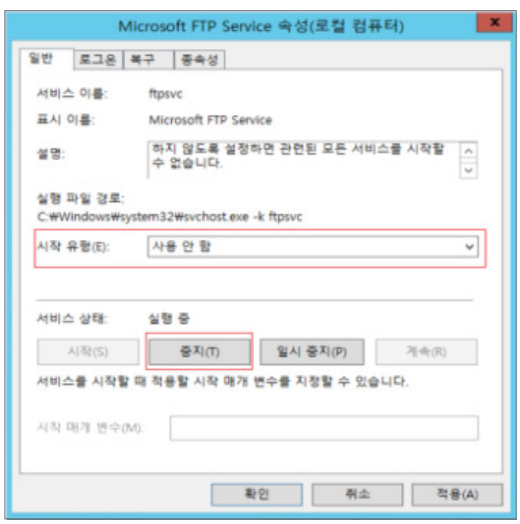
1. 시작 → 실행 → cmd → net stop ftpsvc 명령어 실행
2. cmd → sc config ftpsvc start= disabled 명령어 실행

※ cmd를 관리자 권한으로 실행

[GUI]

■ 서비스에서 변경

시작 → 프로그램 → 관리도구 → '서비스'에서 'Microsoft FTP Service'를 중지하고, 시작유형을 "사용 안 함"으로 설정



FTP 디렉터리 접근 권한 설정

항목설명

홈 디렉터리에 쓰기 권한이 주어진 경우, 임의의 사용자가 쓰기, 수정이 가능하므로 정보 유출, 파일 위・변조로 인한 피해가 발생할 수 있다.

진단 기준

양호

FTP 홈 디렉터리에 Everyone 권한이 없는 경우

취약

FTP 홈 디렉터리에 Everyone 권한이 있는 경우

진단 방법

[GUI]

■ 인터넷 정보 서비스(IIS) 관리에서 확인

1. 시작 → 프로그램 → 관리도구 → 인터넷 정보 서비스(IIS) 관리 → FTP 사이트→ 해당 FTP 사이트→ 기본 설정에서 FTP 홈 디렉터리 확인
2. 탐색기 → 홈 디렉터리 → 속성→ [보안] 탭에서 Everyone 권한 확인

조치 방법

[GUI]

■ 인터넷 정보 서비스(IIS) 관리에서 변경

1. 시작 → 프로그램 → 관리도구 → 인터넷 정보 서비스(IIS) 관리 → FTP 사이트 → 해당 FTP 사이트 → 기본 설정에서 FTP 홈 디렉터리 확인
2. 탐색기 → 홈 디렉터리 → 속성 → [보안] 탭에서 Everyone 권한 제거

Anonymous FTP 금지

항목설명

FTP 서비스를 이용해야 하는 경우 Default 설정으로 되어 있는 익명 연결 허용을 금지하고, FTP를 위한 계정을 따로 만들어서 사용해야 한다.
또한 Password는 복잡도를 높이고 권한은 해당 디렉터리에 대한 읽기 권한만 부여한다. Home Directory는 Default로 설정하지 말고, 임의의 폴더를 생성하여 설정하는 것이 바람직하다.

진단 기준

양호

FTP를 사용하지 않거나 "익명 연결 허용" 이 체크되어 있지 않은 경우

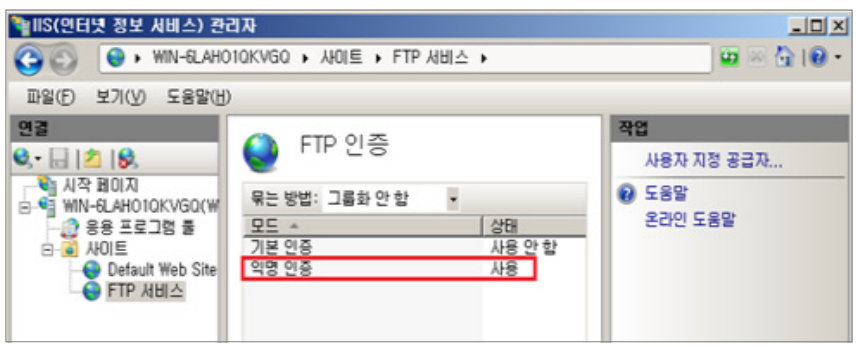
취약

FTP를 사용하거나 "익명 연결 허용" 이 체크되어 있는 경우

진단 방법

■ 인터넷 정보 서비스(IIS) 관리에서 확인

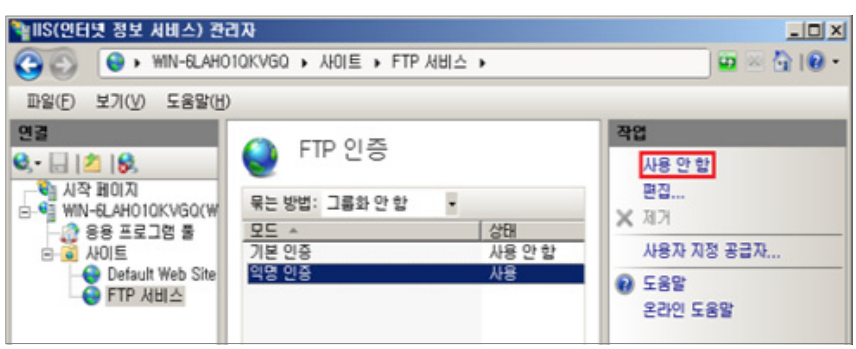
시작 → 프로그램 → 관리도구 → IIS(인터넷 정보 서비스) 관리자 → 사용중인 FTP 서비스 → FTP 인증 에서 "익명 인증" 이 "사용 안 함" 으로 되어 있는지 확인한다.
(익명 인증이 "사용 안 함" 으로 되어 있으면 양호)



조치 방법

■ 인터넷 정보 서비스(IIS) 관리에서 변경

시작 → 프로그램 → 관리도구 → IIS(인터넷 정보 서비스) 관리자 → 사용중인 FTP 서비스 → FTP 인증 에서 "익명 인증" 을 "사용 안 함" 으로 설정



FTP 접근 제어 설정

항목설명

FTP 서비스를 사용할 경우 허가되지 않은 네트워크에 대해 FTP 접속을 차단하는 접근 통제를 설정해야 한다.

진단 기준

양호

FTP 서비스에 접근 가능한 IP 제한 설정을 적용한 경우

취약

FTP 서비스에 접근 가능한 IP 제한 설정을 적용하지 않은 경우

진단 방법

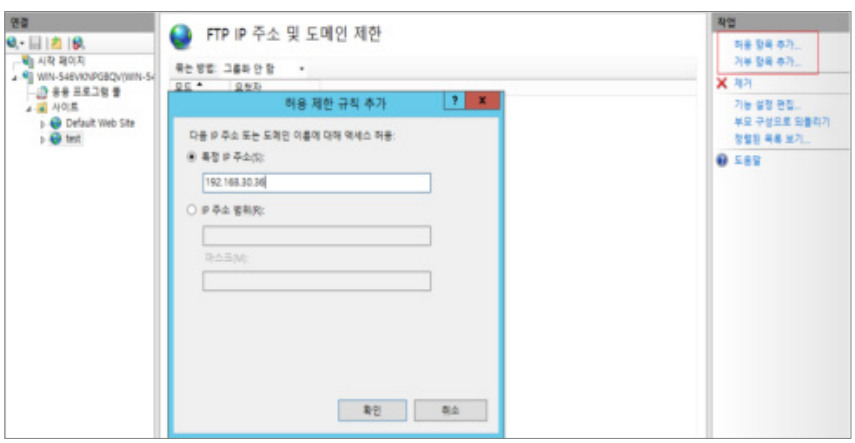
■ 인터넷 정보 서비스(IIS) 관리에서 확인

[Win2012, Win2016]
시작 → 프로그램 → 관리도구 → IIS(인터넷 정보 서비스) 관리자 → 사용중인 FTP 사이트 → FTP IP 주소 및 도메인 제한에서 허용 및 거부 IP 설정 확인

조치 방법

■ 인터넷 정보 서비스(IIS) 관리에서 변경

시작 → 프로그램 → 관리도구 → IIS(인터넷 정보 서비스) 관리자 → 사용중인 FTP 서비스 → FTP IP 주소 및 도메인 제한에서 허용 및 거부 IP를 추가하여 설정



DNS Zone Transfer 설정

항목설명

DNS 서버에 저장되어 있는 도메인 정보를 승인된 DNS서버가 아닌 다른 외부로 유출하는 것은 보안상 바람직하지 않다. 만약, DNS 도메인 정보가 외부로 노출될 경우 악의적인 사용자가 해당 정보를 이용하여 홈페이지 및 하위 URL 정보를 입수하여 웹 애플리케이션 구조를 예측할 수 있다.

진단 기준

양호

아래 기준에 해당될 경우
1. DNS 서비스를 사용하지 않는 경우
2. 영역 전송 허용을 하지 않는 경우
3. 특정 서버로만 설정이 되어 있는 경우

취약

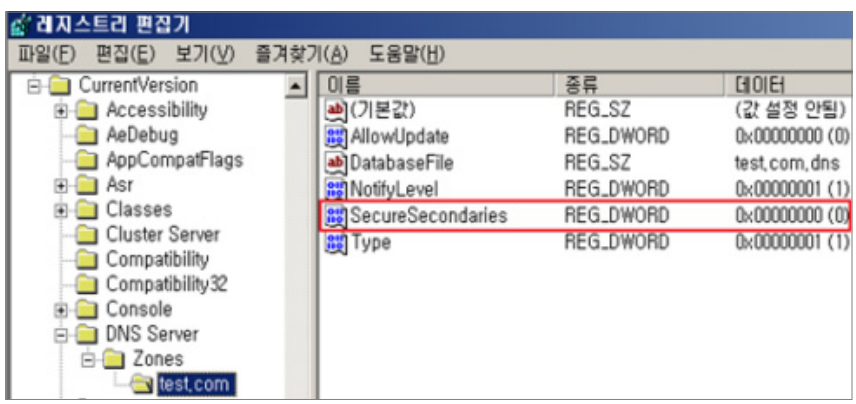
위 3개 기준 중 하나라도 해당되지 않는 경우

진단 방법

[레지스트리]

■ 레지스트리에서 확인

시작 → 실행 → regedit → HKEY_LOCAL_MACHINE\ SOFTWARE\Microsoft\WindowsNT\ CurrentVersion\DNS Server\Zones\운영중인 DNS 영역 에서 SecureSecondaries 값이 2로 설정되어 있는지 확인 (해당 값이 2일 경우 양호)

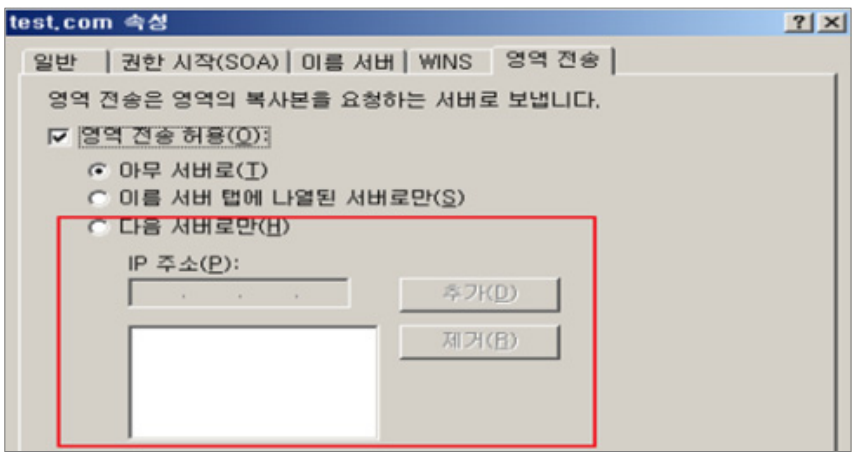


※ SecureSecondaries = 0 : 아무 서버로 영역 전송
SecureSecondaries = 1 : 이름 서버 탭에 나열된 서버로만 영역 전송
SecureSecondaries = 2 : 다음 서버로만 영역 전송

[GUI]

■ DNS 관리자에서 확인

시작 → 프로그램 → 관리도구 → DNS → 정방향 조회 영역 → 사용중인 DNS → 속성 → 영역 전송 에서 특정 서버로만 영역 전송이 이루어는지 확인
("영역 전송 허용" 설정이 제한되어 있거나, 허용 시, "다음 서버로만" 으로 설정되어 있을 경우 양호)

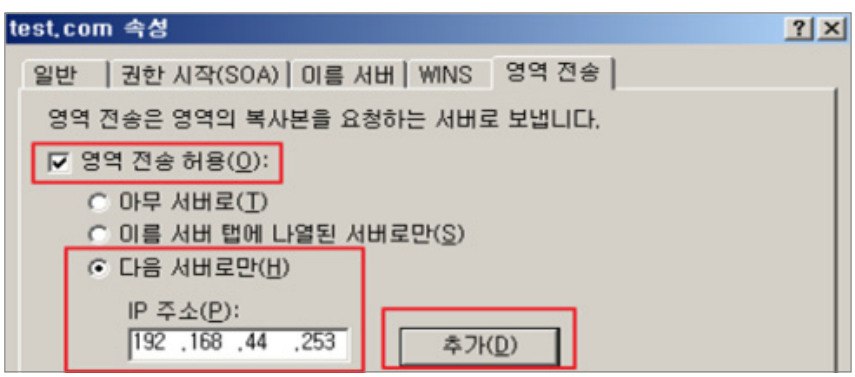


조치 방법

[GUI]

■ DNS 관리자에서 설정

시작 → 프로그램 → 관리도구 → DNS → 정방향 조회 영역 → 사용중인 DNS → 속성 → 영역 전송 에서 "영역 전송 허용"을 제한하거나, 사용 시 특정 서버로만 영역 전송이 이루어지도록 IP 등록



RDS(RemoteDataServices) 제거

항목설명

RDS는 MDAC(Microsoft Data Access Components)의 한 컴포넌트로 RDS(RemoteData Services)가 잘못 설정되어 있으면 서비스거부 공격이나 원격에서 관리자 권한으로 임의의 명령을 실행할 수 있는 취약점이 존재한다. MDAC 2.7 미만의 버전에서 웹 서버와 웹 클라이언트는 모두 이 취약점으로 인해 위험해질 수 있으므로 RDS가 불필요할 경우 제거하는 것이 안전하다.

진단 기준

양호

다음 중 한 가지라도 해당되는 경우(2008 이상 양호)
1. IIS를 사용하지 않는 경우
2. Windows 2000 서비스팩 4, Windows 2003 서비스팩 2 이상 설치되어 있는 경우
3. 디폴트 웹 사이트에 MSADC 가상 디렉터리가 존재하지 않는 경우
4. 해당 레지스트리 값이 존재하지 않는 경우

취약

양호 기준에 한 가지도 해당되지 않는 경우

진단 방법

[Win 2003]

■ 인터넷 정보 서비스(IIS) 관리 및 레지스트리에서 확인

1. 웹 사이트로부터 "/msadc" 가상 디렉터리 확인
   시작 → 실행 → INETMGR → 웹 사이트 선택 후 오른쪽 디렉터리에서 msadc 확인
2. 다음의 레지스트리 키/디렉터리 확인
   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

※ Windows Server 2008 이상 버전을 사용하는 경우 양호함

조치 방법

[Win 2003]

■ 인터넷 정보 서비스(IIS) 관리 및 레지스트리에서 변경

1. 웹 사이트로부터 "/msadc" 가상 디렉터리 제거
   시작 → 실행 → INETMGR → 웹 사이트 선택 후 오른쪽 디렉터리에서 msadc 제거
2. 다음의 레지스트리 키/디렉터리 제거
   HKEY_LOCAL_MACHINE \SYSTEM \CurrentControlSet \Services \W3SVC \Parameters \ADCLaunch\RDSServer.DataFactory
   HKEY_LOCAL_MACHINE \SYSTEM \CurrentControlSet \Services \W3SVC \Parameters \ADCLaunch\AdvancedDataFactory
   HKEY_LOCAL_MACHINE \SYSTEM \CurrentControlSet \Services \W3SVC \Parameters \ADCLaunch\VbBusObj.VbBusObjCls

※ Windows Server 2008 이상 버전을 사용하는 경우 양호함

최신 서비스팩 적용

항목설명

서비스 팩은 Windows의 안정성을 높이기 위해 응용 프로그램, 서비스, 실행파일 등 여러 수정 파일들을 모아 놓은 프로그램으로 최신 보안패치가 적용된 버전을 유지해야 한다.

진단 기준

양호

최신 보안패치가 적용된 서비스 팩이 설치되어 있는 경우

취약

최신 보안패치가 적용된 서비스 팩이 설치되어 있지 않은 경우

진단 방법

[CLI]

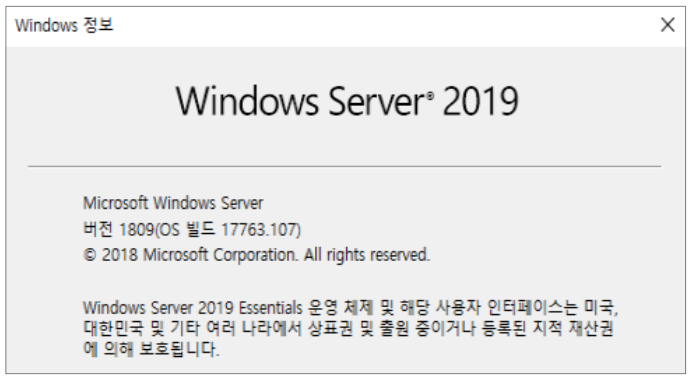
■ 명령프롬프트에서 확인

시작 → 실행 → cmd → winver 또는 systeminfo 명령어를 실행하여 버전 확인

[Win2012 서비스팩 버전 확인]

[Win2016 서비스팩 버전 확인]

[Win2019 서비스팩 버전 확인]



※ 서비스팩이 존재하는 경우, 최신 서비스팩 적용 여부 확인
※ 서비스팩이 존재하지 않는 경우, 최신 빌드 버전 적용 여부 확인

조치 방법

[Win2012]

■ Microsoft 2012 보안 패치 사이트(Windows 2012 R2, 2020년 12월 기준)

https://support.microsoft.com/ko-kr/help/4009470

※ 일반 지원 종료일 : 2018년 10월 09일
연장 지원 종료일 : 2023년 10월 10일

참고) https://docs.microsoft.com/ko-kr/lifecycle/products/windows-server-2012-r2

[Win2016]

■ Microsoft 2016 보안 패치 사이트(Windows 2016, 2020년 12월 현재)

https://support.microsoft.com/ko-kr/help/4043454

※ 일반 지원 종료일 : 2022년 01월 11일
연장 지원 종료일 : 2027년 01월 12일

참고) https://docs.microsoft.com/ko-kr/lifecycle/products/windows-server-2016

[Win2019]

■ Microsoft 2019 보안 패치 사이트(Windows 2019, 2020년 12월 기준)

https://support.microsoft.com/ko-kr/help/4581839

※ 일반 지원 종료일 : 2024년 01월 09일
연장 지원 종료일 : 2029년 01월 09일

참고) https://support.microsoft.com/ko-kr/lifecycle/search/1163

비고

※ 보안 패치 적용 시, 시스템 영향도를 파악하여 충분한 테스트 후 적용 권고

최신 Hot Fix 적용

항목설명

Hot Fix는 즉시 교정되어야만 하는 주요한 취약점(주로 보안과 관련된)을 패치하기 위해 배포되는 프로그램이다. Hot Fix는 각각의 Service Pack 이 발표된 이후 패치가 추가될 필요가 있을 때 별도로 발표되며, Hot Fix 보다 취약성을 이용한 공격 도구가 먼저 나올 수 있으므로 Hot Fix는 배포 후 가능한 빨리 설치 할 것을 권장한다.

진단 기준

양호
최신 Hot Fix가 설치되어 있을 경우

취약
최신 Hot Fix가 설치되어 있지 않은 경우

진단 방법

[CLI]

■ 명령 프롬프트에서 확인

시작 → 실행 → cmd → wmic QFE Get HotFixID,InstalledOn,Description 명령어를 실행하여 보안 패치 업데이트 날짜 확인

```
C:\Windows\system32>wmic QFE Get HotFixID,InstalledOn,Description
Description      HotFixID   InstalledOn
Update           KB3192137  9/17/2016
Update           KB3193190  9/17/2016
Update           KB3211320  2/28/2017
Security Update  KB3213986  2/28/2017
```

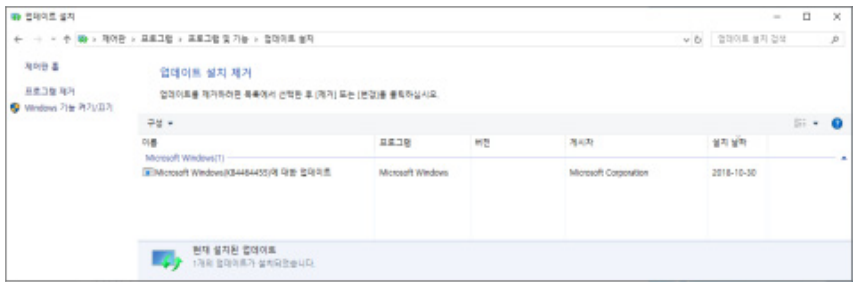
[GUI]

■ 프로그램 및 기능에서 확인

[Win2012]
시작 → 제어판 → 프로그램 및 기능 → 설치된 업데이트 보기 → 보안 패치 업데이트 날짜 확인
※ Windows 정기 보안 업데이트 릴리즈 날짜는 매월 둘째 주 수요일 (한국시간)

[Win2016]
시작 → 설정 →업데이트 및 복구 → Windows 업데이트 → 업데이트 기록을 통하여 보안 패치 업데이트 날짜 확인
※ Windows 정기 보안 업데이트 릴리즈 날짜는 매월 둘째 주 수요일 (한국시간)

[Win2019]
시작 → 업데이트 및 보안 → Windows 업데이트 → 업데이트 기록을 통하여 보안 패치 업데이트 날짜 확인
또는 시작 → 제어판 → 프로그램 및 기능 → 설치된 업데이트 보기 → 보안 패치 업데이트 날짜 확인
※ Windows 정기 보안 업데이트 릴리즈 날짜는 매월 둘째 주 수요일 (한국시간)



조치 방법

■ Hot Fix 수동 설치

아래의 패치 리스트를 조회하여, 서버에 필요한 패치 선별 후, 수동으로 설치
http://technet.microsoft.com/ko-kr/security/

■ Winodws 자동 업데이트를 통한 설치

[Win2012]
시작 → 제어판 → Windows 업데이트에서 자동 업데이트 사용을 클릭하면 자동으로 시스템에 필요한 Hot Fix 및 소프트웨어 업그레이드를 보여주고 설치를 쉽게 할 수 있다.

[Win2016]
시작 → 설정 →업데이트 및 복구 → Windows 업데이트 → 업데이트 확인을 클릭하면 자동으로 시스템에 필요한 Hot Fix 및 소프트웨어 업그레이드를 보여주고 설치를 쉽게 할 수 있다

[Win2019]
시작 → 설정 → 업데이트 및 보안 → Windows 업데이트 → 업데이트 확인을 클릭하면 자동으로 시스템에 필요한 Hot Fix 및 소프트웨어 업그레이드를 보여주고 설치를 쉽게 할 수 있다

■ PMS(Patch Management System) Agent를 통한 설치

[Win2003, Win2008, Win2012, Win2016, Win2019]
PMS Agent를 통한 보안 패치 및 Hot Fix의 경우는 적용 후 시스템 재시작을 요구하는 경우가 대부분이므로, 관리자는 서비스에 지장이 없는 시간대에 적용하는 것을 권장한다.

백신 프로그램 업데이트

항목설명

지속적인 신종 바이러스의 출현으로 인해 백신 프로그램을 설치 후 주기적으로 업데이트를 하지 않을 경우 백신의 성능이 미비할 수 있다. 바이러스 정보에 대한 주기적인 업데이트를 통해 신규 바이러스를 탐지 및 차단할 수 있도록 최신 업데이트를 적용해야 한다.

진단 기준

양호

바이러스 백신 프로그램의 최신 엔진 업데이트가 설치되어 있을 경우

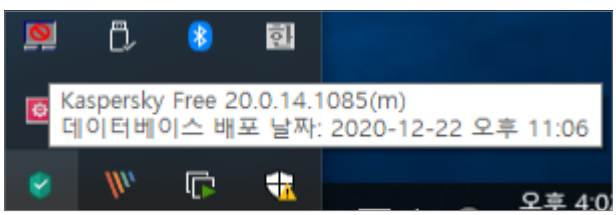
취약

바이러스 백신 프로그램의 최신 엔진 업데이트가 설치되어 있지 않은 경우

진단 방법

■ 바이러스 백신 프로그램의 최신 엔진 업데이트 설치 유무를 수동으로 확인

※ 수동 점검을 통해 백신 프로그램의 최신 업데이트 일자 확인이 필요함



조치 방법

■ 담당자를 통해 바이러스 백신 설치 후 엔진 업데이트를 설정

백신회사 마다 다소 차이는 있으나 매주 업데이트가 이뤄지고, 긴급한 경우 수시로 업데이트를 하기도 한다. 따라서 정기적인 업데이트를 통해 검색엔진을 최신 버전으로 유지하고, 백신회사에서 발표하는 경보를 주시해야 한다.

또한, 백신 프로그램의 자동업데이트 기능을 이용하면 인터넷에 연결되어 있을 때 변동사항을 자동으로 업데이트 되도록 설정할 수 있다.

※ 시스템 설정상, 자동업데이트 기능을 사용할 수 없는 경우, 수동으로 업데이트를 할 수 있도록 업데이트 주기 정책 설정이 필요함

로그의 정기적 검토 및 보고

항목설명

로그를 정기적으로 분석하여 침입 유무를 파악하고, 침입 시도 의심 사례를 분석하여 사전에 해당 장비에 대한 접근을 차단하는 등 체계적인 로그 관리 작업이 이루어져야 한다.

진단 기준

양호

로그 기록에 대해 정기적으로 검토, 분석, 리포트 작성 및 보고 등의 조치가 이루어지는 경우

취약

로그 기록에 대해 정기적으로 검토, 분석, 리포트 작성 및 보고 등의 조치가 이루어지지 않는 경우

진단 방법

■ 로그 기록에 대한 정기적 검토 및 분석 증적, 보고서 확인

※ 수동 점검을 통해, 로그 기록, 검토 및 보고의 주기 확인이 필요함

조치 방법

■ 로그 기록에 대한 정기적 검토 및 분석 실시

(1) 시작 → 제어판 → 관리 도구 → 이벤트 뷰어
(2) 응용 프로그램 로그, 보안 로그, 시스템 로그 분석
(3) OS 구성에 따라 디렉터리 서비스 로그, 파일 복제 서비스 로그, DNS 서버 로그 등 분석

※ 이벤트 로그를 확인하기 위해서 Windows 서버의 이벤트 뷰어를 사용하여 진행함

■ 로그 기록에 대한 정기적 검토 및 분석 실시 후 분석 결과에 대한 일일·월간 보고서 작성 및 보고

비고

■ 로컬 보안 정책 감사 설정의 기본값

정책	서버 버전 기본 값	데스크탑 버전 기본 값
개체 액세스 감사	감사 안함	감사 안함
계정 관리 감사	사용자 계정 관리 : 성공 컴퓨터 계정 관리 : 성공 보안 그룹 관리 : 성공	사용자 계정 관리 : 성공 보안 그룹 관리 : 성공
계정 로그인 이벤트 감사	Kerberos 서비스 티켓 작업 : 성공 Kerberos 인증 서비스 : 성공	감사 안함
권한 사용 감사	감사 안함	감사 안함
디렉터리 서비스 액세스 감사	디렉터리 서비스 액세스 : 성공 로그인 : 성공, 실패 로그오프 : 성공	로그인 : 성공 로그오프 : 성공
로그인 이벤트 감사	계정 잠금 : 성공 특수 로그인 : 성공 네트워크 정책 서버 : 성공, 실패 보안 상태 변경 : 성공	계정 잠금 : 성공 특수 로그인 : 성공 네트워크 정책 서버 : 성공, 실패 보안 상태 변경 : 성공
시스템 이벤트 감사	시스템 무결성 : 성공, 실패 기타 시스템 이벤트 : 성공, 실패	시스템 무결성 : 성공, 실패 기타 시스템 이벤트 : 성공, 실패
정책 변경 감사	감사 정책 변경 : 성공 인증 정책 변경: 성공	감사 정책 변경 : 성공 인증 정책 변경: 성공
프로세스 추적 감사	감사 안함	감사 안함

원격으로 접근 할 수 있는 레지스트리 경로

항목설명

Windows에 의해 사용되는 모든 초기화와 환경설정 정보는 레지스트리에 저장되므로 레지스트리에 대한 철저한 보안이 요구된다. 레지스트리 편집기는 원격접속으로도 그 키를 바꿀 수 있는데 이는 대단히 위험한 것으로 네트워크를 통한 레지스트리 접속을 차단해야 한다. 원격에서 레지스트리로 접근을 위해서는 관리자의 권한 또는 원격에서 접근을 위한 특별한 계정이 필요하다. 윈도우에서는 원격에서 레지스트리 접근에 대한 요구를 다루기 위해 원격 레지스트리 서비스를 제공하고 있는데 이 서비스를 중지시키면 레지스트리에 대한 어떠한 원격 접근도 막을 수 있다.

진단 기준

양호

Remote Registry Service가 중지되어 있는 경우

취약

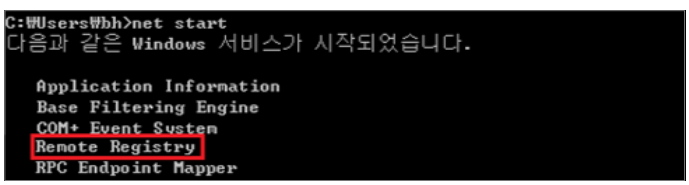
Remote Registry Service가 사용 중일 경우

진단 방법

[CLI]

■ 명령 프롬프트에서 확인

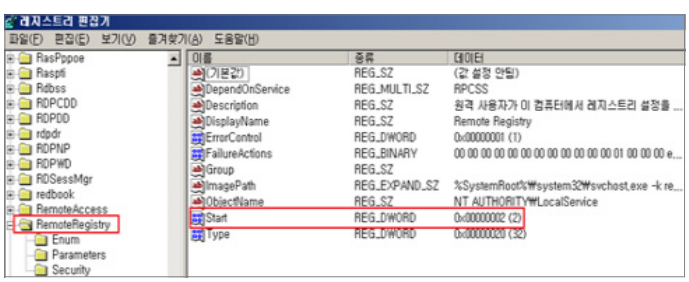
시작 → 실행 → cmd → net start 명령어를 실행하여 원격 레지스트리 서비스가 구동 중인지 확인



[레지스트리]

■ 레지스트리에서 확인

시작 → 실행 → regedit → HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\RemoteRegistry에서 Start 값이 4로 되어 있는지 확인

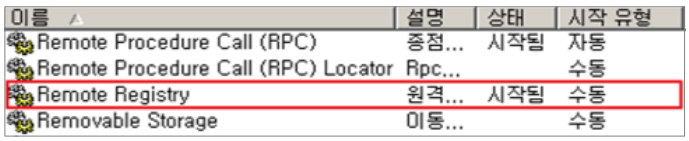


- Start = 2 : 자동(재부팅시에도 자동으로 시작됨)
- Start = 3 : 수동(재부팅시 수동으로 시작해야 함)
- Start = 4 : 사용안함(재부팅시 서비스 시작되지 않음)

[GUI]

■ 서비스에서 확인

시작 → 프로그램 → 관리도구 → 서비스 → Remote Registry 서비스 구동 여부 확인

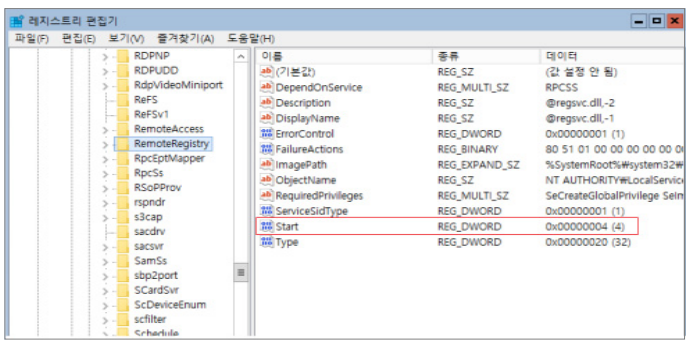


조치 방법

[레지스트리]

■ 레지스트리에서 변경

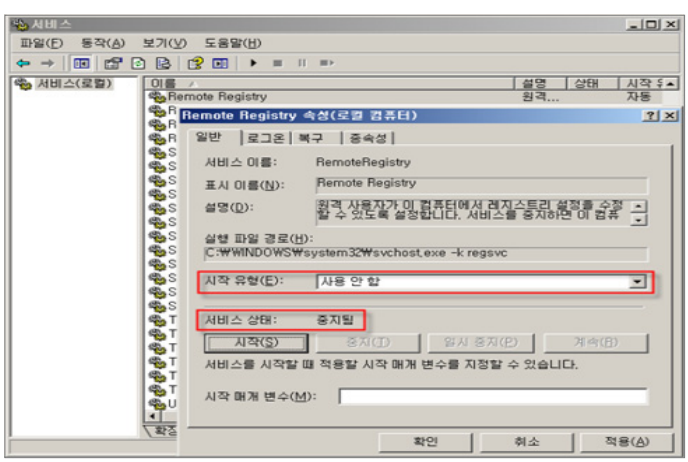
시작 → 실행 → regedit → HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\RemoteRegistry 에서 Start 값을 4로 변경



[GUI]

■ 서비스에서 변경

시작 → 프로그램 → 관리도구 → 서비스 → Remote Registry → 속성 에서 시작 유형을 "사용 안 함" 으로 설정하고, 서비스를 중지



백신 프로그램 설치

항목설명

웜, 트로이목마 등의 악성 바이러스로 인한 피해규모가 커지고 있으며 이에 대한 피해를 최소화하기 위해 반드시 바이러스 백신 프로그램을 설치해야 한다. 바이러스 백신 프로그램은 바이러스 감염 여부 진단 및 치료, 파일 보호가 가능하며 예방도 가능하다.

진단 기준

양호

바이러스 백신 프로그램이 설치되어 있는 경우

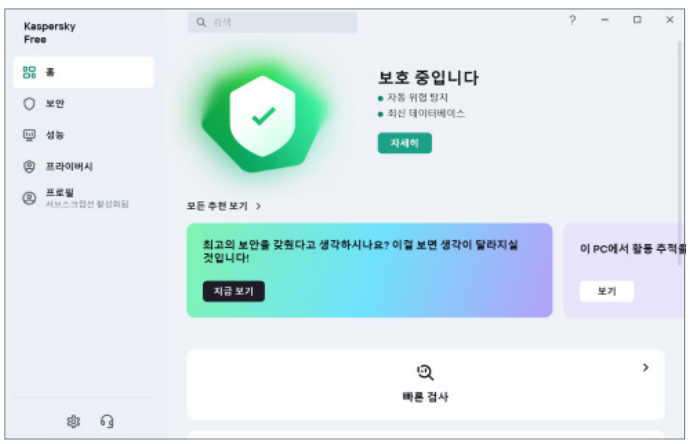
취약

바이러스 백신 프로그램이 설치되어 있지 않은 경우

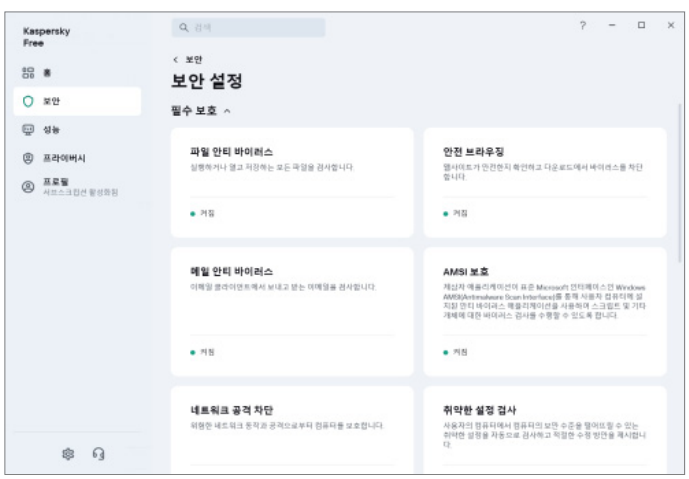
진단 방법

■ 다음 항목들을 수동으로 점검

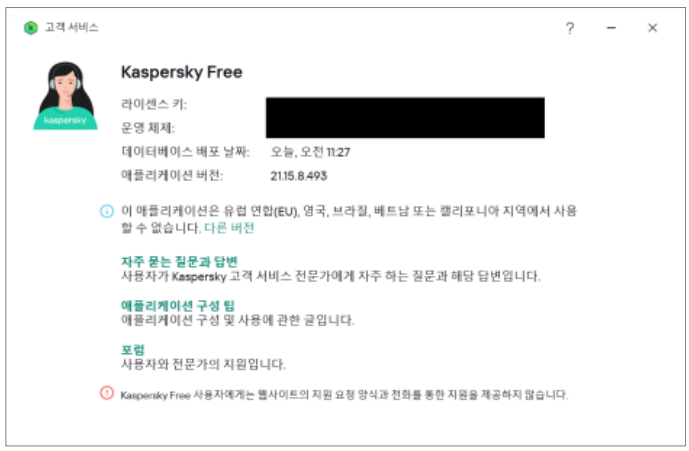
1. 바이러스 백신 프로그램 설치 여부



2. 실시간 감시 기능 설정 여부



3. 최신 Update 여부



조치 방법

■ 담당자를 통하여 바리어스 백신을 설치하도록 권고하며, 최신 보안패치를 확인하고, 실시간 감시를 설정

- 안철수 연구소 : http://www.ahnlab.com
- 하우리 : http://www.hauri.co.kr
- 시만텍코리아 : http://www.symantec.co.kr
- 한국트렌드마이크로: http://www.trendmicro.co.kr/

SAM 파일 접근 통제 설정

항목설명

SAM(Security Account Manager) 파일은 사용자와 그룹 계정의 패스워드를 관리하고, LSA(Local Security Authority)를 통한 인증을 제공한다. 따라서 SAM 파일에 대한 패스워드 공격 시도로 인해 패스워드 데이터베이스 정보가 노출될 수 있으므로 Administrator 및 System 그룹 외에는 SAM 파일에 대한 접근을 제한해야 한다.

진단 기준

양호

SAM 파일 접근 권한에 Administrator, System 그룹만 모든 권한으로 등록되어 있는 경우

취약

SAM 파일에 Administrator, System 그룹 외 다른 그룹에 권한이 설정 되어 있는 경우

진단 방법

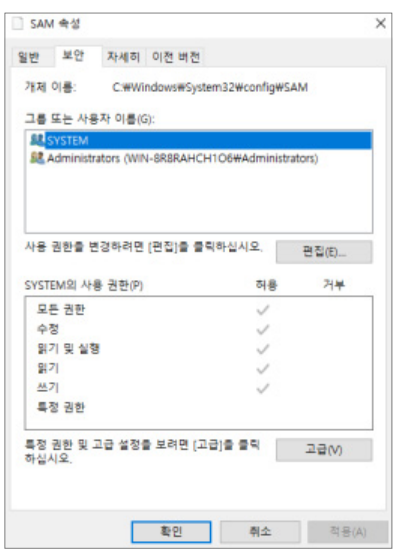
■ 명령 프롬프트에서 확인

시작 → 실행 → cmd → cacls %systemroot%\system32\config\SAM 명령어를 통해 SAM 파일 접근권한에 Administrator, System 그룹만 모든 권한으로 등록되어 있는지 확인

```
C:\Users\Administrator>cacls %systemroot%\system32\config\SAM
C:\Windows\system32\config\SAM NT AUTHORITY\SYSTEM:F
                               BUILTIN\Administrators:F


C:\Users\Administrator>_
```

※ 명령 프롬프트를 관리자 권한으로 실행

■ 탐색기에서 확인



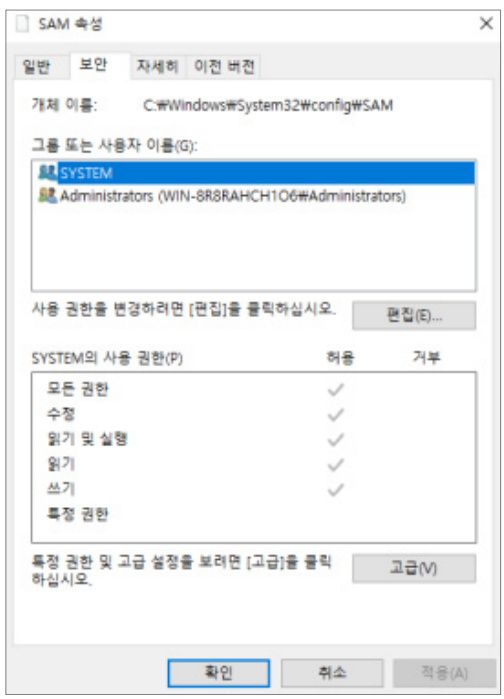
조치 방법

■ 명령 프롬프트에서 확인

시작 → 실행 → cmd → cacls %systemroot%\system32\config\SAM /remove:g 삭제할 그룹 또는 계정명 명령어를 통해 SAM 파일 접근권한에 Administrator, System 그룹 외 나머지 계정 및 그룹 권한 제거

■ 탐색기에서 확인

탐색기 → C:\Windows\system32\config\SAM → 속성 → 보안 탭에서 Administrator, System 그룹 외 다른 사용자 및 그룹 권한 제거



로그온하지 않고 시스템 종료 허용

항목설명

로그인 창에 “시스템 종료” 버튼이 활성화되어 있으면 로그인을 하지 않고도 불법적인 시스템 종료가 가능하여 정상적인 서비스 운영이 불가능할 수 있다. 시스템 종료 버튼을 비활성화함으로 허가되지 않은 사용자가 시스템 종료를 하는 위협을 방지할 수 있다.

진단 기준

양호

"로그인하지 않고 시스템 종료 허용"이
"사용 안 함"으로 설정되어 있는 경우

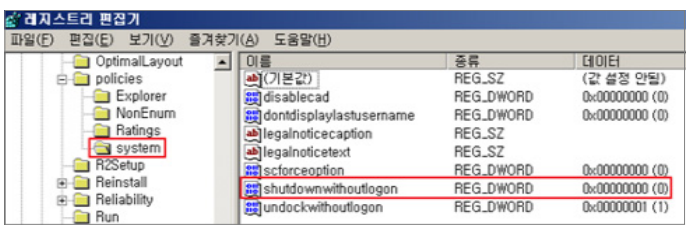
취약

"로그인하지 않고 시스템 종료 허용"이
"사용"으로 설정되어 있는 경우

진단 방법

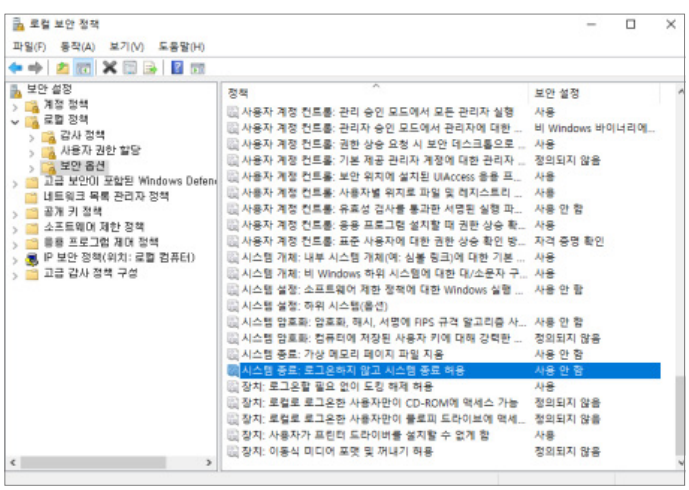
■ 레지스트리에서 확인

[Win2003, Win2008, Win2012, Win2016]
CurrentVersion\policies\system 에서 ShutdownWithoutLogon 값이 "0" (사용안함)으로 설정되어 있는지 확인 (값이 0 으로 설정되어 있는 경우 양호)



■ 로컬 보안 정책에서 확인

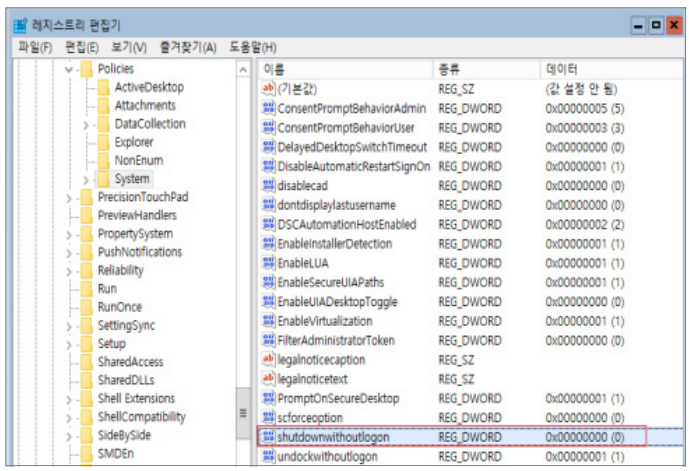
[Win2003, Win2008, Win2012, Win2016]
시작 → 프로그램 → 관리도구 → 로컬 보안 정책 → 로컬 정책 → 보안 옵션 → "시스템 종료 : 로그인하지 않고 시스템 종료 허용” 정책이 “사용 안 함”으로 되어 있는지 확인



조치 방법

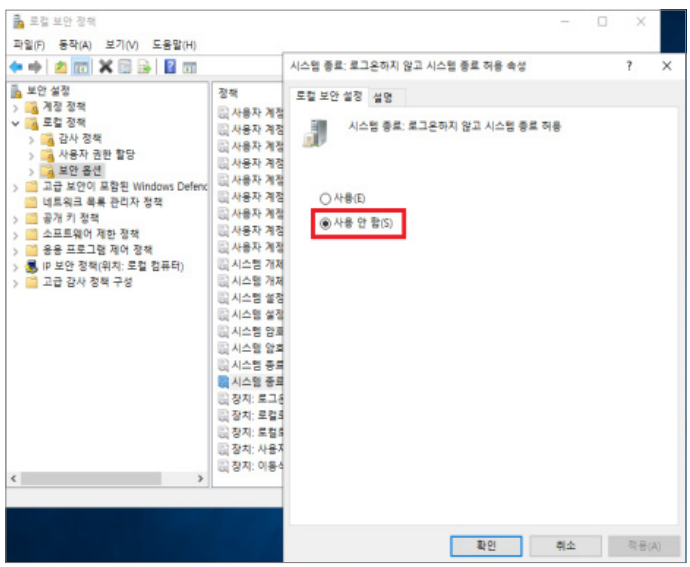
■ 레지스트리에서 변경

[Win2003, Win2008, Win2012, Win2016]
CurrentVersion\policies\system 에서 ShutdownWithoutLogon 값이 "0" (사용안함)으로 설정되어 있는지 확인 (값이 0 으로 설정되어 있는 경우 양호)



■ 로컬 보안 정책에서 확인

시작 → 프로그램 → 관리도구 → 로컬 보안 정책 → 보안 옵션 → " 시스템 종료: 로그인하지 않고 시스템 종료 허용" 정책을 "사용 안 함" 으로 적용



원격 시스템에서 강제로 시스템 종료

항목설명

이 보안 설정은 원격에서 네트워크를 사용하여 운영체제를 종료할 수 있는 사용자 및 그룹을 결정하며, 특정 사용자만 제어할 수 있도록 설정해야한다. 만약 해당 권한 부여가 부적절할 경우 서비스 거부 공격에 이용될 수 있다.

진단 기준

양호

원격 시스템에서 강제로 시스템 종료" 정책에 "Administrators" 만 존재할 경우

취약

"원격 시스템에서 강제로 시스템 종료" 정책에 "Administrators" 외 다른 계정 및 그룹이 존재할 경우

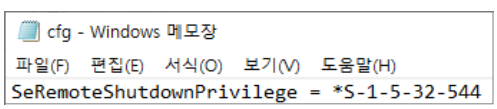
진단 방법

■ 명령 프롬프트에서 확인

1. 시작 → 실행 → cmd.exe → secedit /export /cfg c:\cfg.txt 명령어 실행

```
C:\Users\Administrator>secedit /export /cfg C:\cfg.txt

The task has completed successfully.
See log %windir%\security\logs\scesrv.log for detail info.

C:\Users\Administrator>
```

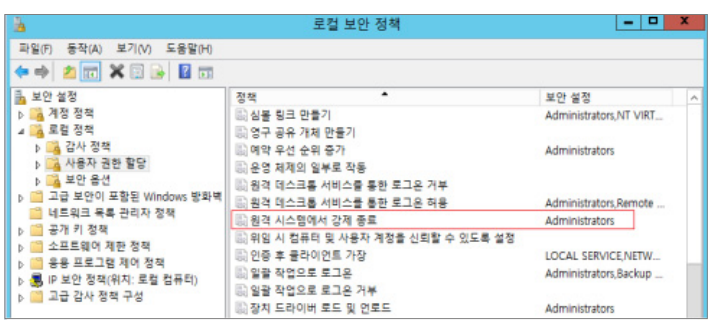
2. 탐색기 → cfg.txt 파일을 열어서 SeRemoteShutdownPrivilege 설정 값에 S-1-5-32-544만 적용되어 있는지 확인



※ 잘 알려진 보안 식별자
- Administrators = S-1-5-32-544
- Power Users = S-1-5-32-547
- Backup operators = S-1-5-32-551
- Users = S-1-5-32-545

■ 로컬 보안 정책에서 확인

시작 → 프로그램 → 관리도구 → 로컬 보안 정책 → 로컬 정책 → 사용자 권한 할당 → "원격 시스템에서 강제로 시스템 종료" 정책에 "Administrators" 그룹만 존재하는지 확인



조치 방법

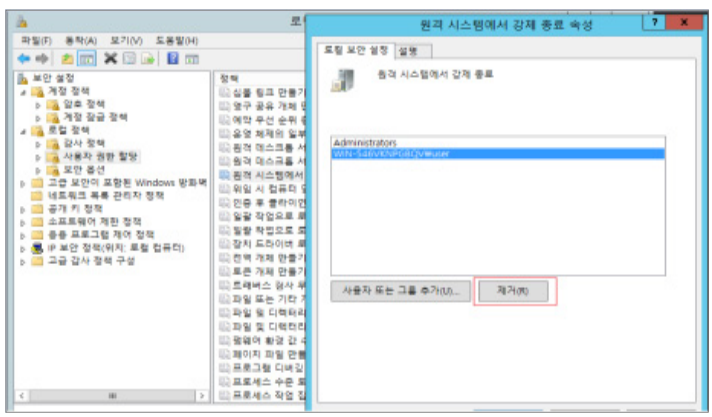
■ 명령 프롬프트에서 변경

1. 탐색기 → cfg.txt 파일을 열어서 SeRemoteShutdownPrivilege 설정 값을 S-1-5-32-544로 변경
2. 시작 → 실행 → cmd.exe → secedit /configure /db C:\cfg.sdb /cfg C:\cfg.txt 명령어 실행

```
c:₩>secedit /configure /db C:₩cfg.sdb /cfg C:₩cfg.txt

작업을 성공적으로 완료했습니다.
자세한 정보는 %windir%₩security₩logs₩scesrv.log를 참조하십시오.
```

■ 로컬 보안 정책에서 변경

시작 → 프로그램 → 관리도구 → 로컬 보안 정책 → 로컬 정책 → 사용자 권한 할당 → "원격 시스템에서 강제 종료" 정책에 "Administrators" 그룹만 존재하도록 다른 사용자 및 그룹 제거



보안 감사를 로그할 수 없는 경우 시스템 종료

항목설명

보안 감사 로그를 기록할 수 없는 경우 시스템을 종료할 것인지를 결정하는 설정이며, 해당 설정을 통해 서비스 거부 공격 또는 비정상적인 시스템 종료로 인한 시스템 및 데이터 손상이 발생할 수 있다.

진단 기준

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

진단 방법

■ 명령 프롬프트에서 확인

1. 시작 → 실행 → cmd.exe → secedit /export /cfg c:\cfg.txt 명령어 실행
2. 탐색기 → cfg.txt 파일을 열어서 CrashOnAuditFail 설정 값이 4, 1로 되어 있는지 확인

```
C:\Users\Administrator>secedit /export /cfg c:\cfg.txt

The task has completed successfully.
See log %windir%\security\logs\scesrv.log for detail info.

C:\Users\Administrator>_
```

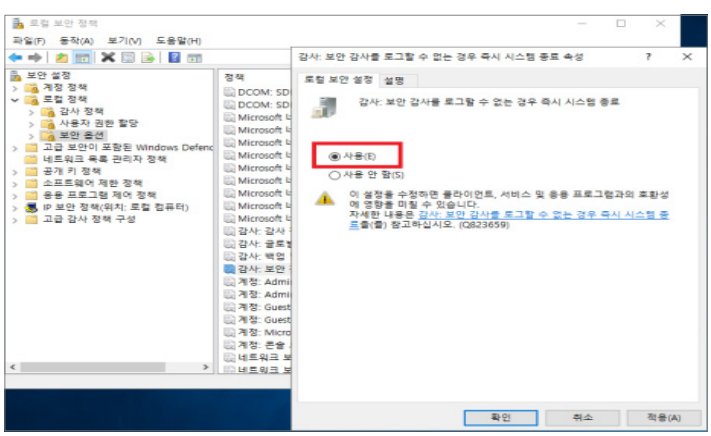
```
MACHINE\System\CurrentControlSet\Control\Lsa\CrashOnAuditFail=4,0
```

- CrashOnAuditFail = 4,0 (보안 감사를 로그할 수 없을 때 즉시 종료 안 함)
- CrashOnAuditFail = 4,1 (보안 감사를 로그할 수 없을 때 즉시 종료됨)

※ default 옵션
CrashOnAuditFail = 4,0

■ 로컬 보안 정책에서 확인

시작 → 제어판 → 관리도구 → 로컬 보안 정책 → 로컬 정책 → 보안 옵션 → "감사: 보안 감사를 기록할 수 없는 경우 즉시 시스템 종료" 정책이 "사용 안함"으로 되어 있는지 확인



조치 방법

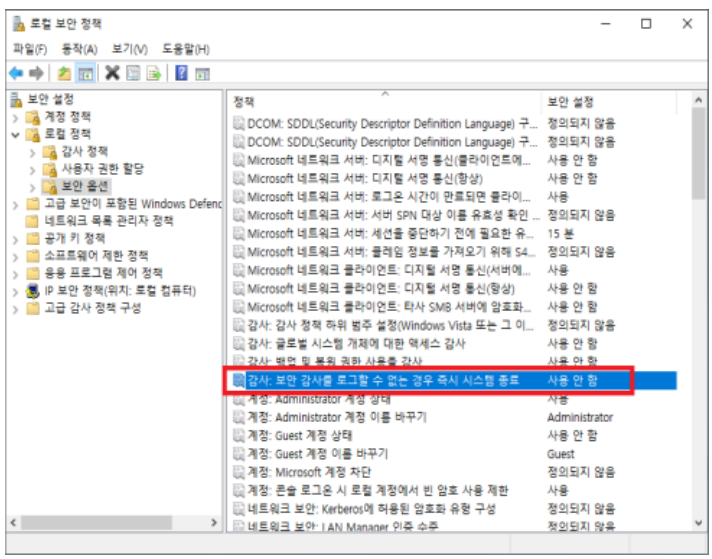
■ 명령 프롬프트에서 확인

1. 탐색기 → cfg.txt 파일을 열어서 CrashOnAuditFail 설정 값을 4, 0로 변경
2. 시작 → 실행 → cmd.exe → secedit /configure /db C:\cfg.sdb /cfg C:\cfg.txt 명령어 실행

```
c:₩>secedit /configure /db C:₩cfg.sdb /cfg C:₩cfg.txt

작업을 성공적으로 완료했습니다.
자세한 정보는 %windir%₩security₩logs₩scesrv.log를 참조하십시오.
```

■ 로컬 보안 정책에서 확인

시작 → 제어판 → 관리도구 → 로컬 보안 정책 → 로컬 정책 → 보안 옵션 → "감사: 보안 감사를 기록할 수 없는 경우 즉시 시스템 종료" 정책이 "사용 안함" 으로 변경



SAM 계정과 공유의 익명 열거 허용 안함

항목설명

SAM(보안 계정 관리자) 계정과 공유의 익명 열거 설정이 허용될 경우, Windows에서는 익명 사용자가 도메인 계정(사용자, 컴퓨터 및 그룹)과 네트워크 공유의 이름 열거를 통해 악의적인 사용자가 계정 이름 목록을 익명으로 표시할 수 있다. 이 정보를 사용하여 암호를 추측하거나 사회 공학적 기술 공격을 수행 할 수 있다.

진단 기준

양호

아래의 보안옵션을 모두 사용하고 있을 경우

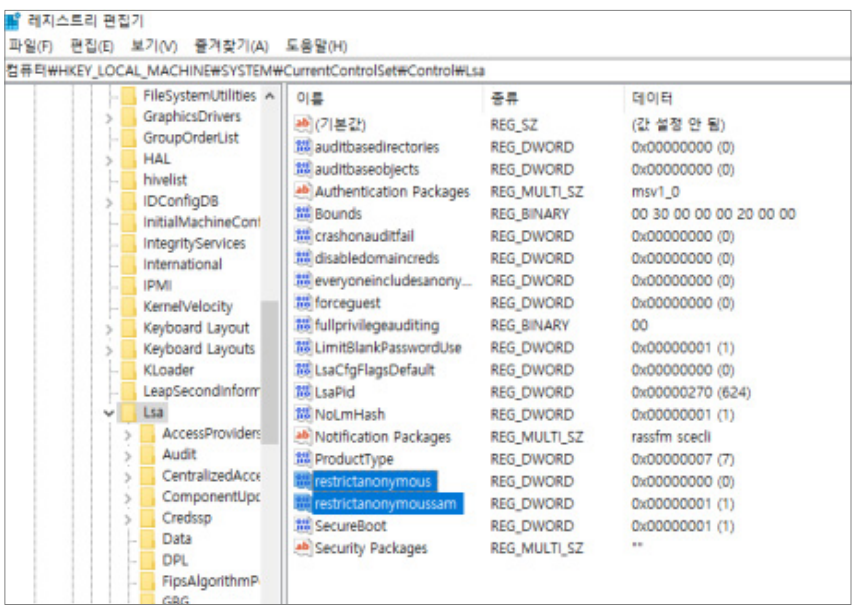
취약

아래의 보안옵션 중 어느 하나라도 사용하고 있지 않을 경우
1. 네트워크 액세스: SAM 계정의 익명 열거 허용 안 함
2. 네트워크 액세스: SAM 계정과 공유의 익명 열거 허용 안함

진단 방법

■ 레지스트리에서 확인

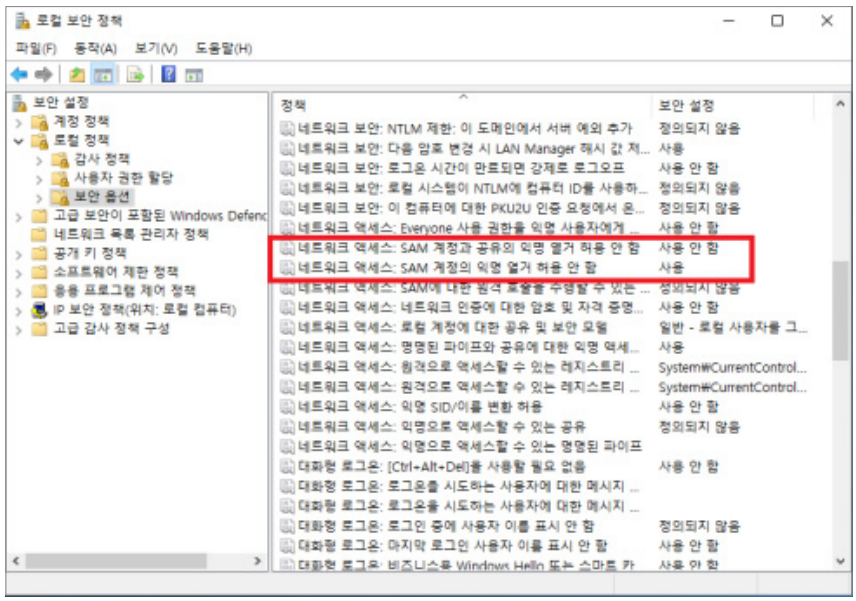
1. 시작 → 실행 → regedit
2. HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa
3. restrictanonymous과 restrictanonymoussam의 값이 1로 되어 있는지 확인



※ default 옵션
restrictanonymous : 0
restrictanonymoussam : 1

■ 로컬보안정책에서 확인

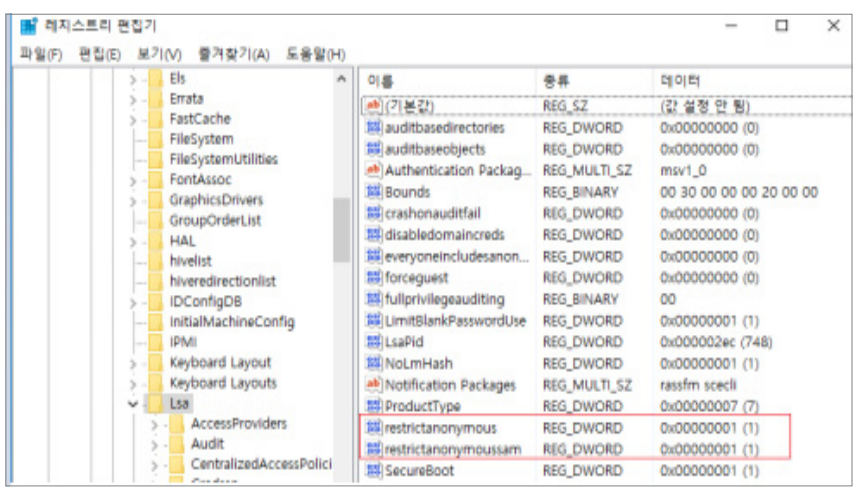
시작 → 제어판 → 관리도구 → 로컬 보안 정책 → 보안 옵션에서 “네트워크 액세스: SAM 계정과 공유의 익명 열거 허용 안 함” 정책과 “네트워크 액세스: SAM 계정의 익명 열거 허용 안 함” 정책이 모두 “사용”으로 되어 있는지 확인



조치 방법

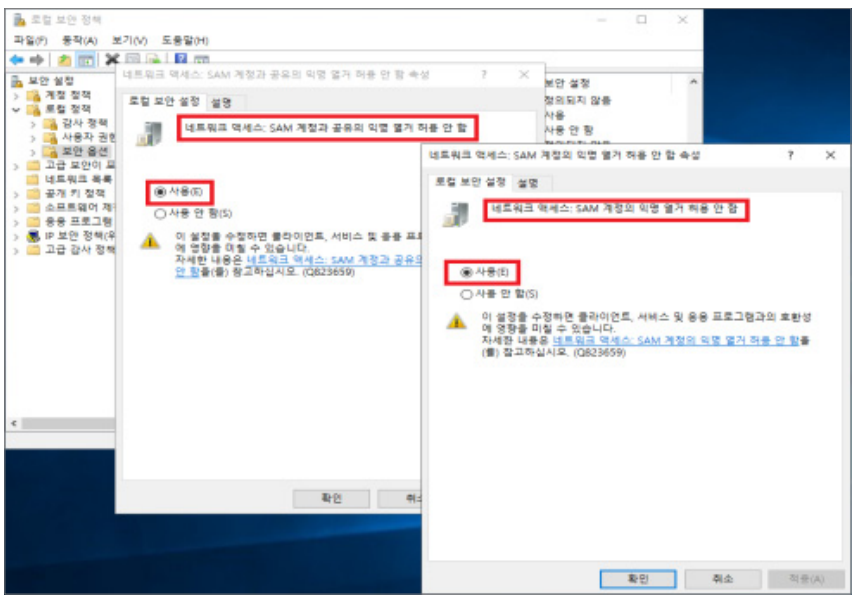
■ 레지스트리에서 변경

1. 시작 → 실행 → regedit
2. HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa
3. restrictanonymous과 restrictanonymoussam의 값을 1로 변경



■ 로컬 보안 정책에서 변경

시작 → 프로그램 → 관리도구 → 로컬 보안 정책 → 보안 옵션에서 “네트워크 액세스: SAM 계정과 공유의 익명 열거 허용 안 함” 정책과 “네트워크 액세스: SAM 계정의 익명 열거 허용 안 함” 정책을 모두 “사용”으로 설정



Autologon 기능 제어

항목설명

Autologon 기능을 사용하면 침입자가 해킹 도구를 이용하여 레지스트리에서 로그인 계정 및 암호를 확인할 수 있으므로 Autologon 기능을 사용하지 않아야 한다.
사용 시 비인가자가 시스템이 물리적으로 접근할 수 있으며, 시스템 정보 유출 및 손상될 수 있다.

진단 기준

양호

AutoAdminLogon 값이 없거나 0으로 설정되어 있는 경우

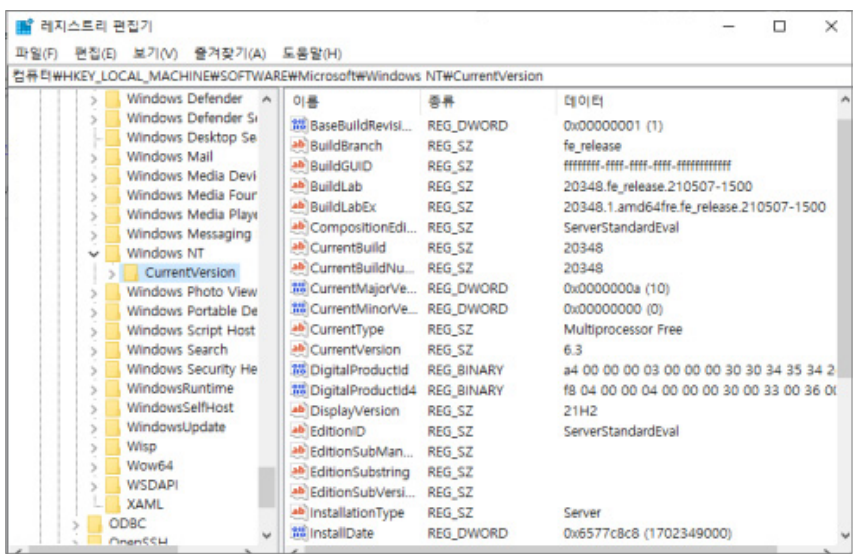
취약

AutoAdminLogon 값이 1로 설정되어 있는 경우

진단 방법

■ 레지스트리에서 확인

시작 → 실행 → regedit → HKEY_LOCAL_MACHINE\ Software\Microsoft\Windows NT\CurrentVersion\Winlogon 에서 AutoAdminLogon 가 존재하지 않거나 "0" 으로 설정되어 있는지 확인
(AutoAdminLogon가 존재하지 않거나, 0으로 설정되어 있을 경우 양호)

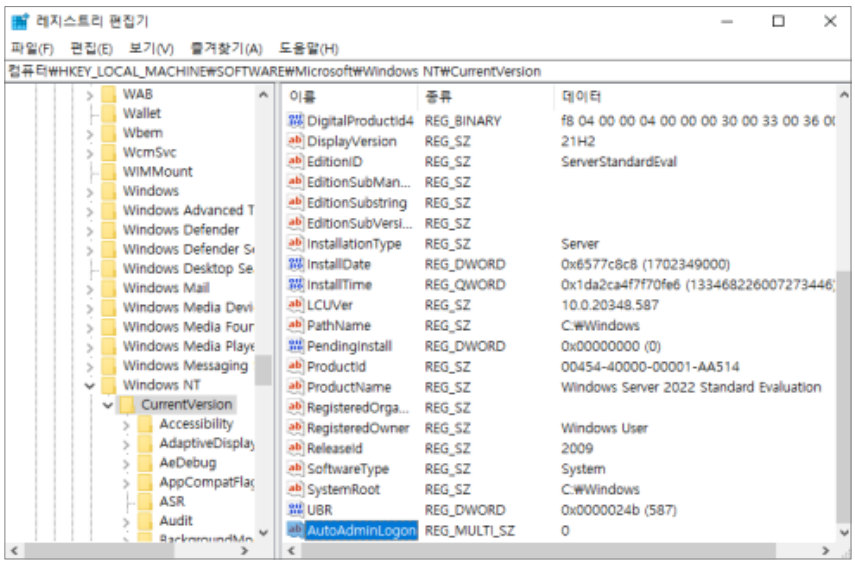


※ default 옵션 : AutoAdminLogon 값이 없음

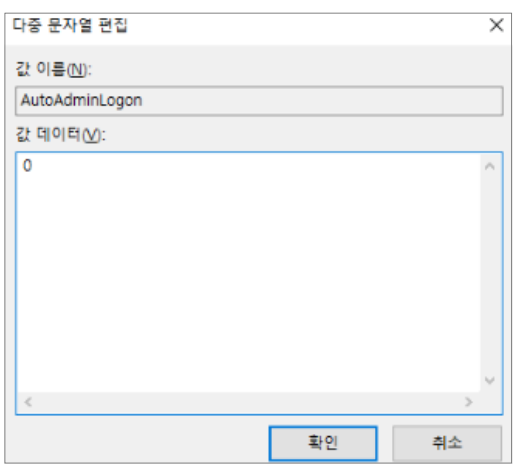
조치 방법

■ 레지스트리에서 변경

시작 → 실행 → regedit → HKEY_LOCAL_MACHINE\ Software\Microsoft\ Windows NT\CurrentVersion\Winlogon에서 AutoAdminLogon 값을 0 으로 설정



※ AutoAdminLogon 값이 없을 경우
새로 만들기 → 다중 문자열 값 → AutoAdminLogon으로 이름 바꾸기 → 값 데이터 “0” 입력



이동식 미디어 포맷 및 꺼내기 허용

항목설명

이동식 미디어의 NTFS 포맷 및 꺼내기가 허용되는 사용자를 제한함으로, 사용자가 관리 권한을 가진 다른 컴퓨터로 이동식 디스크의 데이터를 이동하여 파일에 대한 소유권을 얻고 자신에게 모든 권한을 부여하여 파일을 보거나 수정할 수 있다.

진단 기준

양호

"이동식 미디어 포맷 및 꺼내기 허용" 정책이 "Administrators"로 되어있는 경우

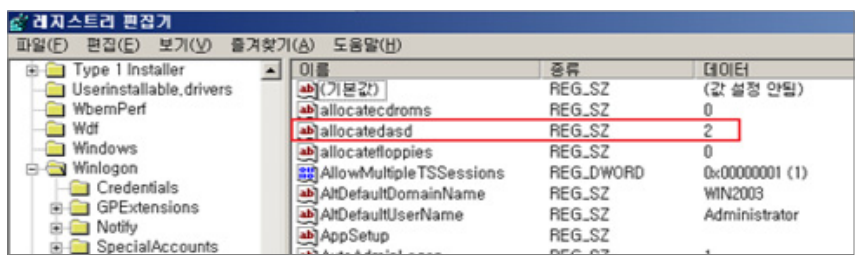
취약

"이동식 미디어 포맷 및 꺼내기 허용" 정책이 "Administrators"로 되어있지 않은 경우

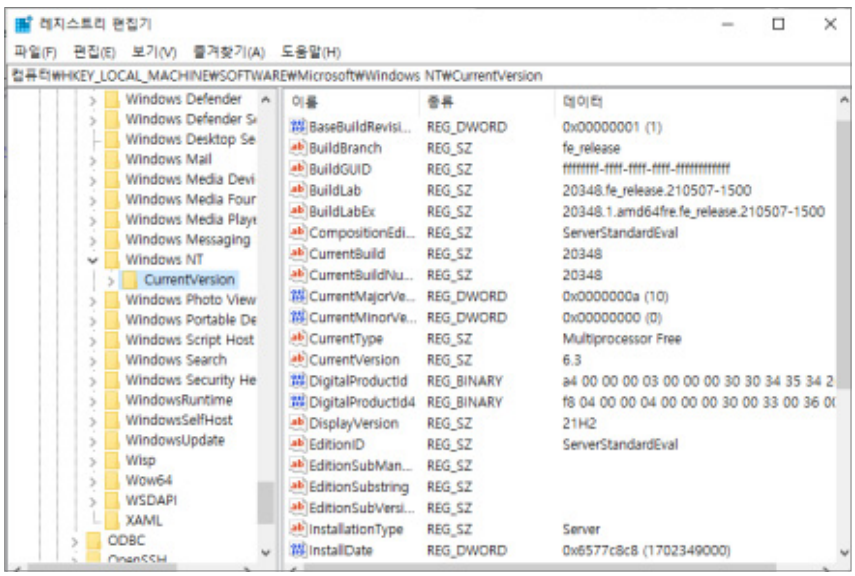
진단 방법

■ 레지스트리에서 확인

시작 → 실행 → regedit → HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon 에서 allocatedasd 값이 "0"으로 되어있는지 확인



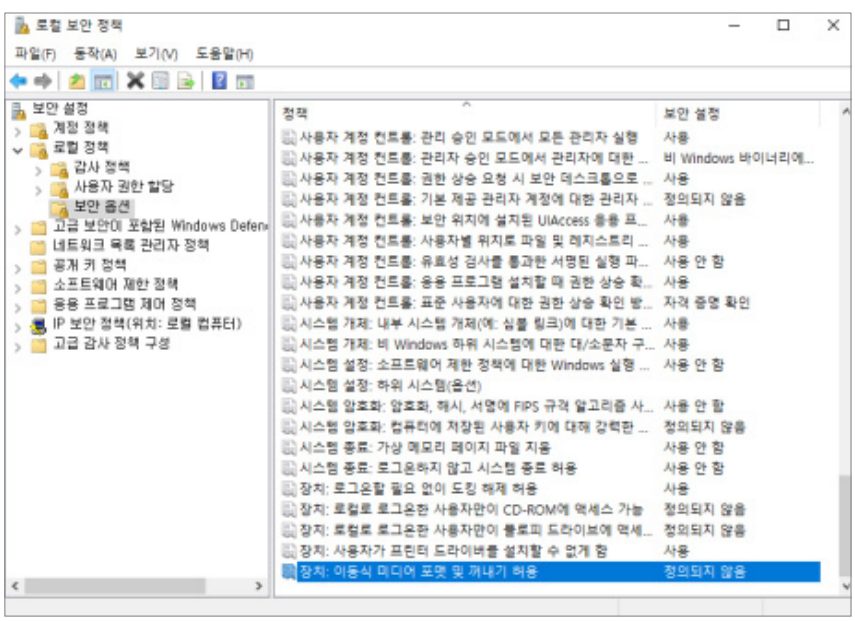
※ allocatedasd = 0 : Administrators
allocatedasd = 1 : Administrators 및 Power Users
allocatedasd = 2 : Administrators 및 Interactive Users



※ Windows Server 2022에서는 default 옵션 : allocatedasd 값이 없음

■ 로컬 보안 정책에서 확인

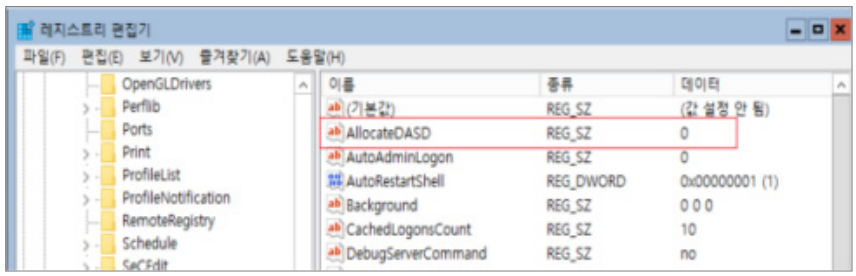
시작 → 프로그램 → 관리도구 → 로컬 보안 정책 → 로컬 정책 → 보안 옵션 → "장치 : 이동식 미디어 포맷 및 꺼내기 허용" 정책이 "Administrators"로 되어 있는지 확인



조치 방법

■ 레지스트리에서 변경

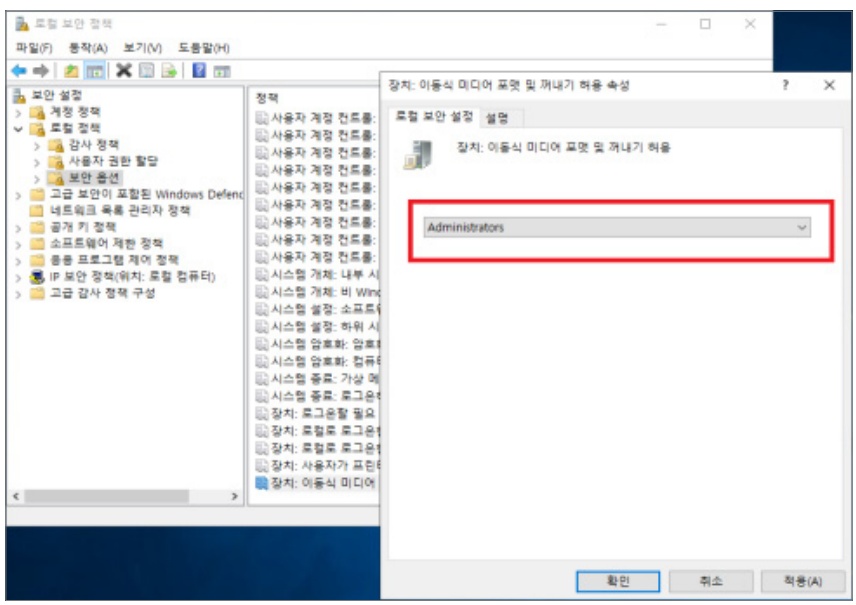
시작 → 실행 → regedit → HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon 에서 AllocateDASD 값을 "0" 으로 변경



※ Windows Server 2022의 경우 default 설정이 allocatedasd 값이 없으므로 신규로 생성하여 데이터 값을 0으로 지정

■ 로컬 보안 정책에서 변경

시작 → 프로그램 → 관리도구 → 로컬 보안 정책 → 로컬 정책 → 보안 옵션 → "장치 : 이동식 미디어 포맷 및 꺼내기 허용" 정책을 "Administrators" 으로 설정



2.7.

PC(Windows)

2.7. PC(Windows)

계정 관리(2개 항목), 파일 시스템(3개 항목), 패치 관리(2개 항목), 보안관리(4개 항목) 총 4개 영역에서 11개 항목으로 구성된다.

[표 7] PC(Windows) 진단 체크리스트

구분	진단 항목
가. 계정 관리	패스워드의 주기적 변경
	기관 보안 정책과 패스워드 정책 일치
나. 파일 시스템	공유 폴더 제거
	불필요한 서비스 제거
	Windows Messenger(MSN, ,NET 메신저 등)와 같은 상용 메신저의 사용 금지
다. 패치 관리	HOT FIX 등 최신 보안패치
	최신 서비스팩 적용
라. 보안 관리	OS에서 제공하는 침입차단 기능 활성화
	화면 보호기 대기 시간 설정 및 재시작 시 암호 보호 설정
	CD, DVD, USB 메모리 등과 같은 미디어의 자동실행 방지 등 이동식 미디어에 대한 보안 대책 수립
	비인가 무선랜 사용 제한

패스워드의 주기적 변경

항목설명

계정의 패스워드를 주기적으로 변경하지 않고 오랫동안 사용할 경우 계정 패스워드가 외부에 유출될 수 있으며, 관리자 계정의 패스워드가 유출될 시 자료 유출 등 심각한 사고 발생 가능성이 존재한다.

진단 기준

양호

최대 암호 사용 기간이 “90일” 이하로 설정되어 있는 경우

취약

암호 사용 기간이 “90일” 초과 또는 “제한 없음”으로 설정되어 있는 경우

진단 방법

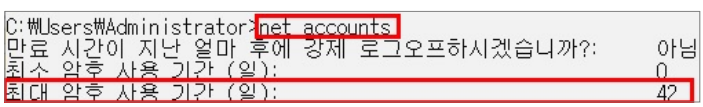
※ 최대 암호 사용 기간이 “90일”로 설정되어 있는지 확인한다.

■ 명령 프롬프트에서 확인

[Win10, Win11]

1) 시작 → 실행 → cmd → net accounts 명령어

2) 실행하여 “최대 암호 사용 기간(일)”이 “90일” 이하로 설정되어 있는지 확인

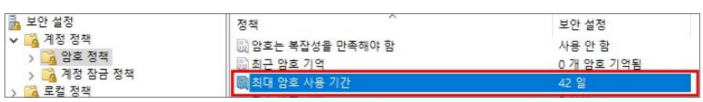


■ 로컬 보안 정책에서 확인

[Win10, Win11]

1) 제어판 → windows Tools(관리도구(큰 아이콘, 작은 아이콘)) → 로컬 보안 정책 → 보안 설정 → 계정 정책 → 암호 정책(실행(Win+r) → secpol.msc → 계정 정책 → 암호 정책)

2) “최대 암호 사용 기간”이 “90일” 이하로 설정되어 있는지 확인



조치 방법

■ 최대 암호 사용 기간 설정

1) 제어판 → windows Tools(관리도구(큰 아이콘, 작은 아이콘)) → 로컬 보안 정책 → 보안 설정 → 계정 정책 → 암호 정책

2) “최대 암호 사용 기간”을 “90일”로 설정

■ 암호 사용 기간 제한 없음 비활성화 여부 확인

1) 명령 프롬프트에서 확인

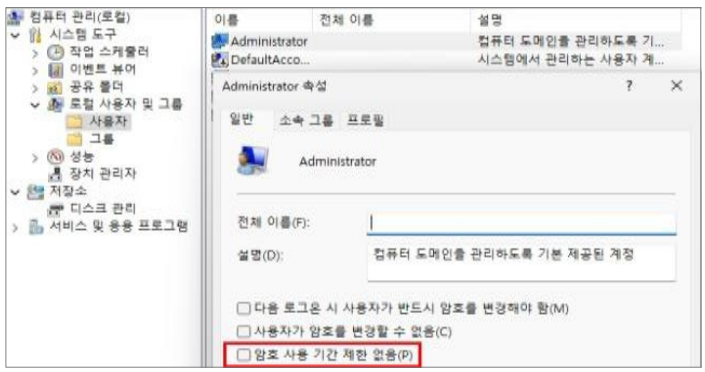
〉 wmic useraccount where Disabled=FALSE get Name, PasswordExpires

2) 조치방법

- “암호 사용 기간 제한 없음” 해제(제어판 → Windows Tools(관리도구(큰 아이콘, 작은 아이콘)) → 컴퓨터 관리 → 로컬 사용자 및 그룹 → 사용자)

■ 컴퓨터 관리에서 사용 계정 암호 사용 기간 제한 없음 해제

- 위 2) 조치 방법과 동일



■ 명령 프롬프트에서 암호 사용 기간 제한 없음 해제

〉 wmic useraccount where Name='계정명' set PasswordExpires=TRUE

■ 명령 프롬프트에서 최대 암호 사용 기간 설정

[Win10, Win11]

시작 → 실행(Win+r) → cmd → net accounts /MAXPWAGE:90 명령어를 입력

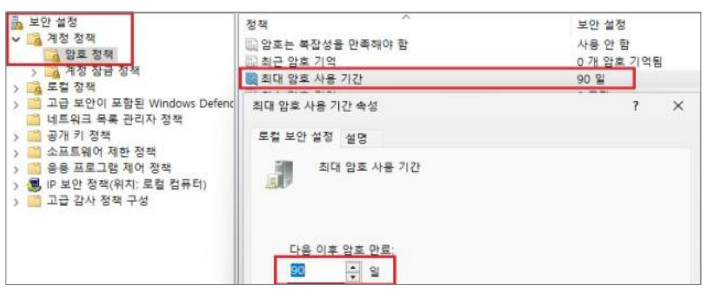
```
C:₩Users₩Administrator>net accounts /MAXPWAGE:90
명령을 잘 실행했습니다.
```

■ 로컬 보안 정책에서 최대 암호 사용 기간 설정

[Win10, Win11]

1) 제어판 → windows Tools(관리도구(큰아이콘, 작은 아이콘)) → 로컬 보안 정책 → 보안 설정 → 계정 정책 → 암호 정책

2) "최대 암호 사용 기간" 정책의 속성 → "다음 이후 암호 만료" 값을 "90일"로 설정



비고

※ 최대 암호 사용 기간을 "90일" 이하로 설정하고, 이 정책이 활성화되기 위해 우선적으로 암호 사용 기간 제한 없음을 해제해야 함

※ 환경에 따라 30에서 90일마다(기본 값: 42) 암호가 만료되도록 설정하는 것이 보안을 위해 가장 좋으며, 이 방법을 사용하면 침입자가 사용자의 암호를 도용하여 네트워크 리소스에 무단으로 액세스하는 횟수가 제한되어야 함

※ 명령 프롬프트(cmd)는 관리자 권한으로 실행해야 함

기관 보안 정책과 패스워드 정책 일치

항목설명

패스워드 복잡도 설정을 점검하여 해당 기관의 보안 정책에 적합하게 패스워드 정책이 설정되어 있는지 확인하고, 비인가자의 패스워드 추측 공격(무작위 대입 공격, 사전 대입 공격 등)에 대한 대비가 되어있는지 확인한다.

진단 기준

양호

기관 정책에 맞게 패스워드 복잡도 설정이 적용되어 있는 경우

취약

기관 정책에 맞게 패스워드 복잡도 설정이 적용되어 있지 않은 경우

진단 방법

※ 최소 암호 길이가 해당 기관의 보안 정책에 적합하게 설정되어 있는지 확인

■ 명령 프롬프트에서 “최소 암호 길이”와 “패스워드 복잡도 설정” 확인

[Win10, Win11]

1) 시작 → 실행(Win+r) → cmd → net accounts 명령어를 실행하여 “최소 암호 길이” 확인

```
C:₩Users₩Administrator>net accounts
만료 시간이 지난 얼마 후에 강제 로그오프하시겠습니까?:      아님
최소 암호 사용 기간 (일):                                  0
최대 암호 사용 기간 (일):                                  90
최소 암호 길이:                                            0
```

2) secedit /export /cfg LocalSecurityPolicy.txt
type LocalSecurityPolicy.txt | find /i “PasswordComplexity”

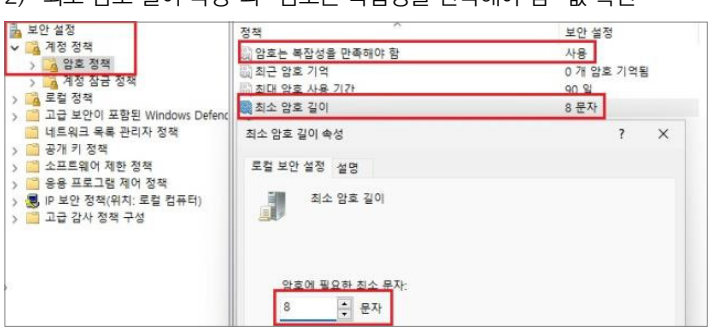
```
C:₩Users₩Administrator>secedit /export /cfg LocalSecurityPolicy.txt

작업을 성공적으로 완료했습니다.
자세한 정보는 %windir%₩security₩logs₩scesrv.log를 참조하십시오.

C:₩Users₩Administrator>type LocalSecurityPolicy.txt | find /i "PasswordComplexity"
PasswordComplexity = 1
```

■ 로컬 보안 정책에서 “최소 암호 길이”와 “암호는 복잡성을 만족해야 함” 값 확인

[Win10, Win11]

1) 제어판 → windows Tools(관리도구(큰 아이콘, 작은 아이콘)) → 로컬 보안 정책 → 보안 설정 → 계정 정책 → 암호 정책

2) “최소 암호 길이 속성”과 “암호는 복잡성을 만족해야 함” 값 확인



조치 방법

※ 최소 암호 길이를 해당 기관의 보안 정책에 적합하게 설정
※ 명령 프롬프트(cmd)는 관리자 권한으로 실행해야 함

■ 명령 프롬프트에서 “최소 암호 길이” 설정

[Win10, Win11]

1) 시작 → 실행(Win+r) → cmd → net accounts /MINPWLEN:8 명령어를 입력

■ 로컬 보안 정책에서 “최소 암호 길이”와 “암호는 복잡성을 만족해야 함” 설정

[Win10, Win11]

1) 제어판 → windows Tools(관리도구(큰 아이콘, 작은 아이콘)) → 로컬 보안 정책 → 보안 설정 → 계정 정책 → 암호 정책

2) “최소 암호 길이” 정책의 속성 → “암호에 필요한 최소 문자” 값을 “8문자”로 설정하고 “암호는 복잡성을 만족해야 함” 설정값을 “사용”으로 설정

비고

■ 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)
- 영문 대문자(26개)
- 영문 소문자(26개)
- 숫자(10개)
- 특수문자(32개)

2) 패스워드는 비인가자에 의한 추측이 어렵도록 다음의 사항을 반영하여 설계
- Null(공백) 패스워드 사용 금지
- 문자 또는 숫자만으로 구성 금지
- 사용자 ID와 동일하거나 유사한 패스워드 금지
- 연속적인 문자나 숫자 사용 (EX. 1111, 1234, abcd) 사용 금지
- 주기성 패스워드 재사용 금지
- 전화번호, 생일과 같이 추측하기 쉬운 개인정보를 패스워드로 사용 금지

3) SAM 파일에 암호를 저장하기 위해 사용되는 LANMan 알고리즘은 8자 단위로 글자를 나누어 암호화하기 때문에 8의 배수가 되는 암호 사용을 권장(8자로 이루어진 암호 사용 권장)

4) 아래와 같은 암호 설정 지양
Null, 계정과 동일하거나 유사한 스트링, 지역명, 부서명, 담당자명, 대표 업무명
예) root, rootroot, root123, 123root, admin, admin123, 123admin, osadmin, adminos

공유 폴더 제거

항목설명

시스템의 기본 공유 항목이 제거되지 않으면 모든 시스템 자원에 접근할 수 있는 위험한 상황이 발생할 수 있다. 불필요한 공유라고 판단되면 공유를 해제해야 하며, 공유를 해제한 후에 레지스트리 AutoShareServer 값 설정을 통해 재부팅 시 기본 공유 폴더의 자동 공유 설정을 방지할 수 있다. (하드디스크 기본 공유 폴더 예: C$, D$, Admin$, IPC$ 등) 또한, 기본 공유 폴더를 제외한 일반 공유 폴더의 권한이 Everyone으로 설정되었는지 확인하고, 공유 금지 설정을 통해 익명 사용자에 의한 접근을 차단해야 한다.

진단 기준

양호
불필요한 공유 폴더가 존재하지 않는 경우

취약
불필요한 공유 폴더가 존재하는 경우

진단 방법

※ 불필요한 기본 공유 폴더 및 일반 공유 폴더가 존재하는지 확인

■ 명령 프롬프트에서 공유 폴더 확인

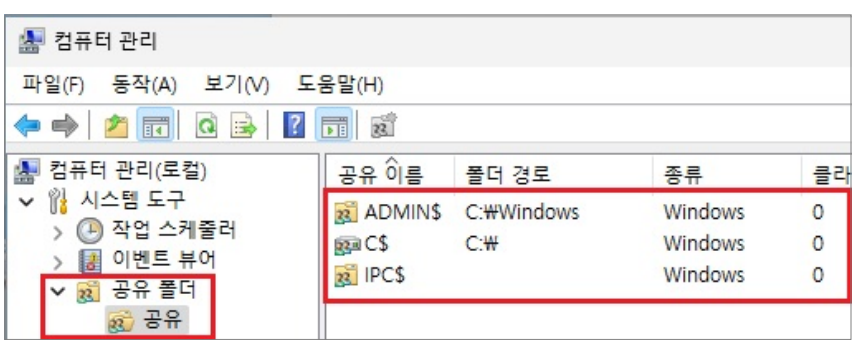
[Win10, Win11]

1) 시작 → 실행(Win+r) → cmd → net share 명령어를 입력하여 불필요한 공유 폴더 확인

```
C:₩Users₩Administrator>net share

공유 이름    리소스                         설명

-------------------------------------------------------------------------------
IPC$                                        원격 IPC
C$           C:₩                            기본 공유
ADMIN$       C:₩Windows                     원격 관리
C            C:₩
Users        C:₩Users
명령을 잘 실행했습니다.
```

■ 컴퓨터 관리에서 공유 폴더 확인

1) 제어판 → Windows Tools(관리도구(큰 아이콘, 작은 아이콘)) → 컴퓨터 관리 → 공유 폴더 → 공유에서 불필요한 공유 폴더 확인(시작 → 실행(Win+r) → "fsmgmt.msc" 입력 → 공유)



조치 방법

※ 기본 공유 폴더 및 일반 공유 폴더 존재 시 제거하고, 재부팅 후 자동 공유 되지 않도록 설정
※ 기본 공유에 대한 조치 시 반드시 [기본 공유 삭제], [비활성화 레지스트리 값]을 모두 설정해야 함

■ 명령 프롬프트에서 기본 공유 중지

[Win10, Win11]

1) 시작 → 실행(Win+r) → cmd → net share “삭제할 공유 폴더명” /delete 명령을 통해 공유 디렉터리 삭제

```
C:₩Users₩Administrator>net share C$ /delete
C$이(가) 제거되었습니다.
```

■ 컴퓨터 관리에서 기본 공유 중지

[Win10, Win11]

1) 제어판 → Windows Tools(관리도구(큰 아이콘, 작은 아이콘)) → 컴퓨터 관리 → 공유 폴더 → 공유 → 불필요한 공유 폴더 우클릭

2) 공유 중지 (하드디스크 기본 공유 폴더는 C$, D$, Admin$, IPC$가 있으며 C$,D$, Admin$ 폴더의 공유 제거)

■ 시스템 재부팅 시 기본 공유 폴더 자동 공유 방지 설정

1) 시작 → 실행(Win+r) → regedit 입력

2) HKLM\System\CurrentControlSet\Services\LanmanServer\Parameters

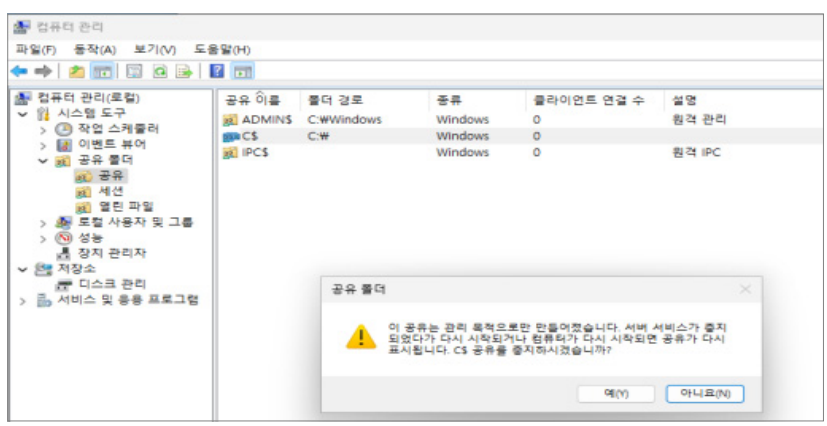
3) AutoShareWks 의 데이터 값을 0으로 설정

4) 값이 없는 경우, “DWORD 값” 선택하고 AutoShareWks를 추가하여 값을 “0”으로 입력

■ 일반 공유 폴더 사용 시 접근 권한 설정, 사용 권한, 암호 설정

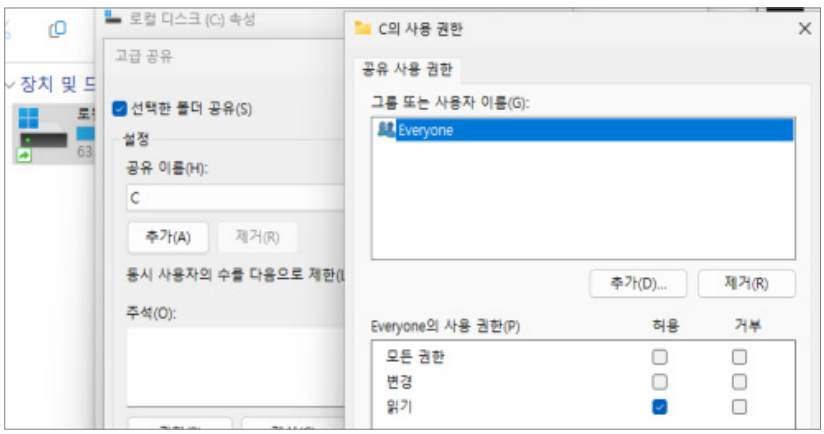
1) 일반 공유 폴더에 Everyone 공유 제거

① 제어판 → Windows Tools(관리도구(큰 아이콘, 작은 아이콘)) → 컴퓨터 관리 → 공유 폴더 → 공유 → 사용할 공유 폴더



우클릭 → 공유 중지

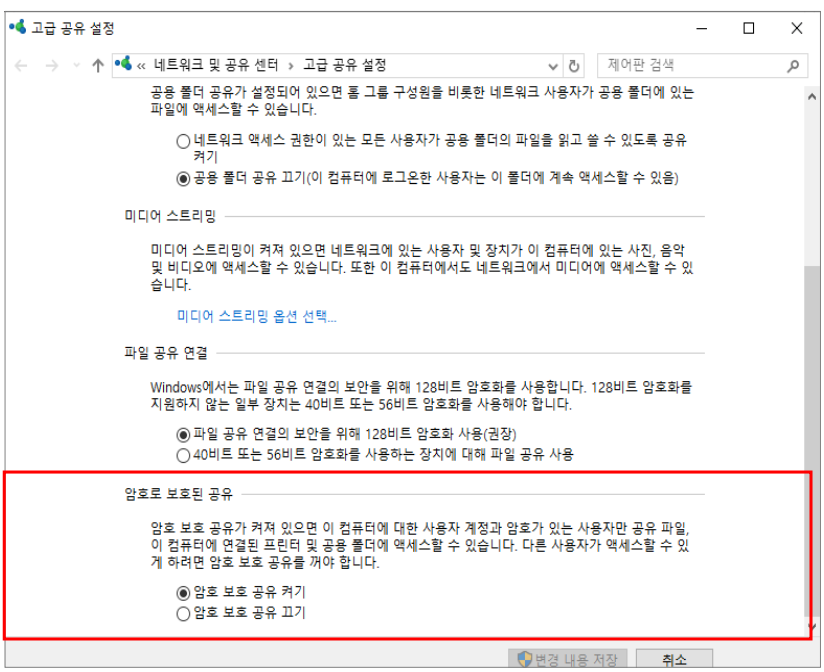
② 공유 파일 생성 시 “Everyone”으로 된 공유 제거, 접근이 필요한 계정만 권한 추가
(해당 공유 파일 → 우클릭 → 속성 → 공유 → 고급 공유 → 권한)



2) 공유 폴더의 접근 암호 설정

[Win10]

① 제어판 → 네트워크 및 공유 센터 → 고급 공유 설정에서 “암호 보호 공유 켜기” 설정

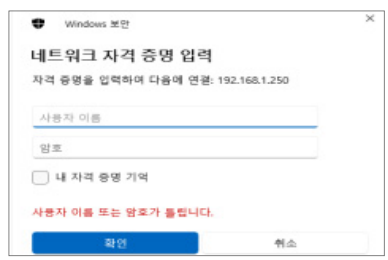


[Win11]

② 제어판 → 네트워크 및 공유 센터(관리도구(큰 아이콘, 작은 아이콘)) → 고급 공유 설정 변경 → 모든 네트워크에서 “암호로 보호된 공유” 켜기 설정

3) 공유 폴더 접근 가능 여부 확인

① 시작 → 실행(Win+r) → 공유 폴더 PC 계정명 또는 IP 주소 입력 (Ex. \\192.168.0.0) 후 패스워드 입력 팝업 확인



비고

■ 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

※ 업무에 필요한 공유 폴더 사용 시 사용자별 권한 부여 필요
※ 방화벽과 라우터에서 135, 139(TCP/UDP) 포트를 차단하여 외부로부터 위험을 제거함으로써 보안성을 높일 수 있음

불필요한 서비스 제거

항목설명

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 한다. 시스템 관리자는 대상 시스템의 용도를 파악한 후 특별한 목적으로 사용하는 업무 서비스를 제외한 서비스는 제거해야 한다.

진단 기준

양호

업무에 필요한 서비스만 실행되고 있는 경우

취약

디폴트로 설치된 서비스가 실행되고 있는 경우

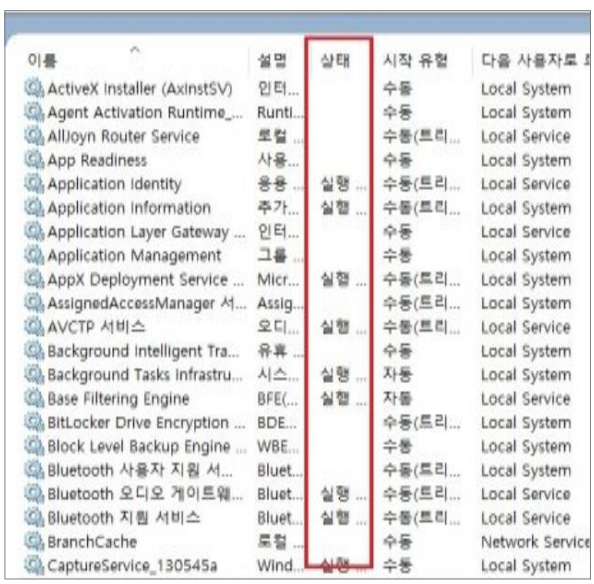
진단 방법

※ 업무에 불필요한 서비스가 실행되고 있는지 확인한다.

■ 서비스에서 확인

[Win10, Win11]

1) 제어판 → Windows Tool(관리도구(큰 아이콘, 작은 아이콘)) → 서비스 → 서비스 상태를 확인하여 불필요한 서비스가 실행 중인지 확인



조치 방법

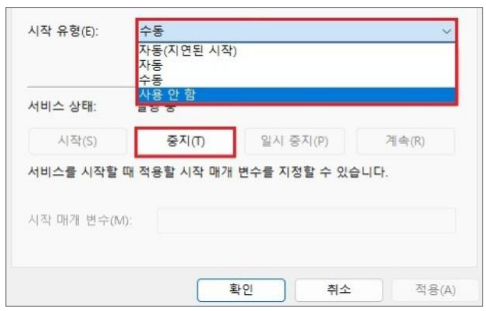
※ 업무에 불필요한 서비스를 중지시키고 시작 유형을 “사용 안 함”으로 설정한다.

■ 서비스에서 설정

[Win10, Win11]

1) 제어판 → Windows Tool(관리도구(큰 아이콘, 작은 아이콘)) → 서비스 → 해당 서비스 선택 → 속성 → [일반] 탭

2) 불필요한 서비스 → 서비스 상태 중지, 시작 유형 → 사용 안 함



비고

※ 해당 서비스의 속성에서 “시작 유형” 선택 및 “시작 시 로그온 계정” 별도 설정이 가능

서비스 시작 유형	설명
사용 안 함	설치되어 있으나 실행되지 않음
수동	다른 서비스나 응용 프로그램에서 당 기능을 필요 할 때만 시작됨
자동	부팅 시에 해당 장치 드라이버가 로드된 후에 운영체제에 의해 시작됨

※ 서비스 리스트

불필요한 서비스 리스트	windows 운영을 위한 최소한의 서비스
- Alerter - Clipbook Computer Browser DHCP client TerminalService Print spooler Messenger NetLogon Network DDE Network DDE DSDM FTP Publishing Service InternetConnectionSharingService IndexingService InfaredMonitorService NetMeetingRemoteDesktopSharingService RemoteRegistryService RoutingandRemoteAccessService SimpleTCP/IPService SMTPService TaskSchedulerService TCPIP NetBIOS Helper	Logical Logging Manager Network Connections NTLM Security Support Provider Plug and Play Server Workstation Removeable Storage Security Accounts Manager Windows Management Instrumentation Windows Management Instrumentation driver extensions WWDM PMSP Service Application Management

Windows Messenger(MSN, .NET 메신저 등)와 같은 상용 메신저의 사용 금지

항목설명

일반 사용자 PC에서 Windows Messenger를 사용할 경우, 메신저를 통해서 주요 정보가 유출될 수 있을 뿐만 아니라 악성코드가 유입될 수 있다.

진단 기준

양호

Windows Messenger가 실행되고 있지 않거나 상용 메신저가 설치되지 않은 경우

취약

Windows Messenger가 실행되고 있거나 상용 메신저가 설치되어 있는 경우

진단 방법

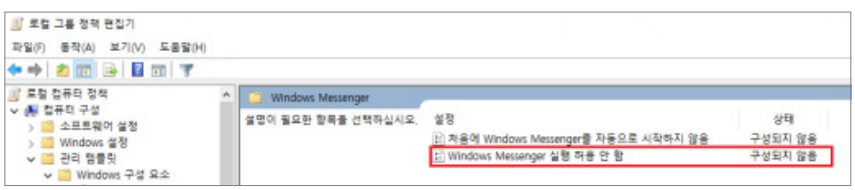
※ Windows Messenger가 실행되고 있는지 확인

■ 로컬 그룹 정책 편집기에서 Windows Messenger 실행 여부 확인

[Win10, Win11]

1) 시작 → 실행 → gpedit.msc 입력 → 컴퓨터 구성 → 관리 템플릿 → Windows 구성 요소 → Windows Messenger

2) "Windows Messenger 실행 허용 안 함" 설정 확인



■ 레지스트리에서 Windows Messenger 실행 여부 확인

[Win10, Win11]

1) 시작 → 실행(Win+r) → regedit

2) HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Messenger\Client 경로의 PreventRun 데이터 값 확인(PreventRun 데이터 값이 1로 설정되어 있는지 확인, 구성되지 않음으로 설정되어 있는 경우 레지스트리 경로 존재하지 않음)

■ 프로그램 및 기능에서 상용 메신저 설치 여부 확인

1) 제어판 → 프로그램 → 프로그램 및 기능

2) 상용 메신저 설치 여부 확인

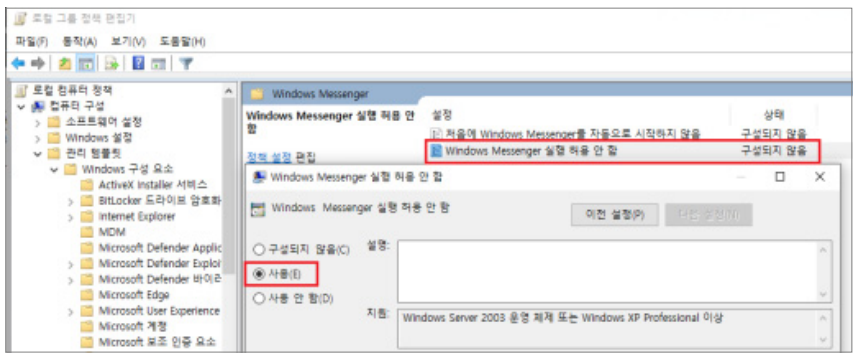
조치 방법

■ 로컬 그룹 정책 편집기에서 Windows Messenger 설정

[Win10, Win11]

1) 시작 → 실행 → gpedit.msc 입력 → 컴퓨터 구성 → 관리 템플릿 → Windows 구성 요소 → Windows Messenger

2) “Windows Messenger 실행 허용 안 함” 정책 마우스 우클릭 → 편집 → “사용”으로 설정



■ 레지스트리에서 Windows Messenger 설정

[Win11]

1) 시작 → 실행(Win+r) → regedit

2) HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Messenger\Client 경로의 PreventRun 데이터 마우스 우클릭 → 수정 → 값 데이터 1로 설정

■ 프로그램 및 기능에서 상용 메신저 삭제

1) 제어판 → 프로그램 → 프로그램 및 기능

2) 설치된 상용 메신저 삭제

비고

Windows Messenger 사용 불가
원격 지원에서도 Windows Messenger를 사용할 수 없음

HOT FIX 등 최신 보안패치

항목설명

Hot FIX 설치 및 자동 업데이트가 설정되어 있지 않은 경우 취약점으로 인한 공격이 발생할 수 있으므로 Hot FIX 출시 즉시 신속하게 설치하고 항상 최신의 보안 업데이트가 이루어져야 한다.

진단 기준

양호

최근 한 달 이내 HOT FIX 설치 및 자동 업데이트 설정이 되어 있는 경우

취약

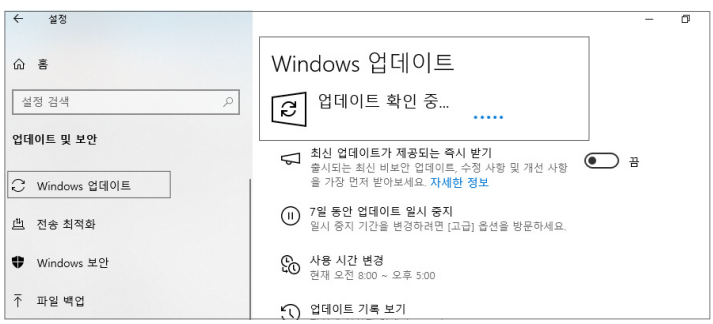
최근 한 달 이내 HOT FIX가 설치되어 있지 않은 경우

진단 방법

※ 시스템의 최신 패치 여부를 확인

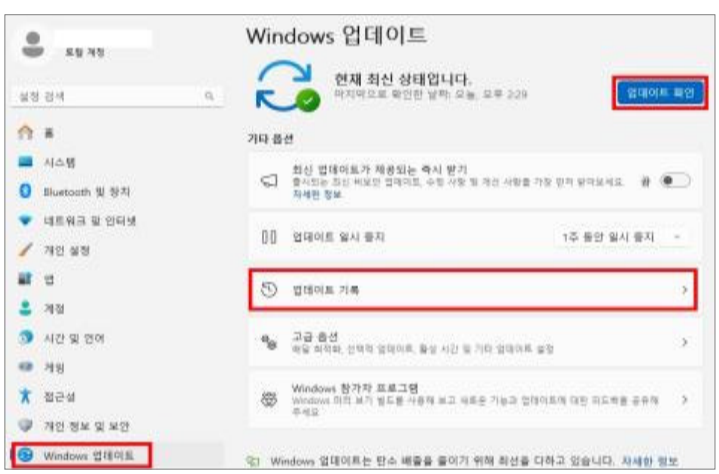
[Win10]

1) 시작 → 설정 → 업데이트 및 보안 → Windows 업데이트 → “업데이트 확인”, “업데이트 기록 보기”를 통하여 HOT FIX, 최신 보안 업데이트 등의 설치 여부 확인



[Win11]

2) 시작 → 설정 → Windows 업데이트 → ‘업데이트 확인’, “업데이트 기록”을 통하여 HOT FIX, 최신 보안 업데이트 등의 설치 여부 확인



조치 방법

※ HOT FIX, 최신 보안 업데이트 등을 설치한다.

■ 최신 패치

[Win10]

1) 시작 → 설정 → 업데이트 및 복구 → “업데이트 확인”, “지금 설치”를 통하여 HOT FIX, 최신 보안 업데이트 등의 설치 여부 확인 및 설정 변경

[Win11]

2) 시작 → 설정 → 업데이트 및 복구 → “업데이트 확인”, “모두 다운로드 및 설치”를 통하여 HOT FIX, 최신 보안 업데이트 등의 설치 여부 확인 및 설정 변경

최신 서비스팩 적용

항목설명

서비스 팩은 Windows의 안정성을 높이기 위해 응용 프로그램, 서비스, 실행파일 등 여러 수정 파일들을 모아 놓은 프로그램으로 최신 보안패치가 적용된 버전을 유지해야 한다.

진단 기준

양호
최신 서비스 팩이 적용 되어 있는 경우

취약
최신 서비스 팩이 적용 되어 있지 않은 경우

진단 방법

※ 최신 서비스팩이 설치되어 있는지 확인

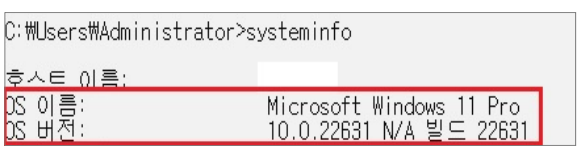
■ 실행을 통한 확인

[Win10, Win11]

1) 시작 → 실행(Win+r) → winver 입력 → Windows 정보 확인

■ 명령 프롬프트에서 확인

1) 시작 → 실행(Win+r) → cmd 입력 → systeminfo



조치 방법

※ 최신 서비스 팩을 설치한다.
※ 네트워크와 분리된 상태에서 서비스 팩 설치를 권장한다. 현재 많은 인터넷 웜(Worm)이 Windows의 취약점을 이용하여 공격하므로 OS 설치 후 곧바로 네트워크에 연결하는 것은 서버에 피해를 입을 수 있다.

■ 수동 조치

[Win11]

1) 확인 후 최신 버전이 아닐 경우 Microsoft 홈페이지에서 다운로드하여 설치

1. 참고 사이트
   https://www.microsoft.com/ko-kr/software-download/windows11
   https://www.microsoft.com/ko-kr/software-download/windows10

바이러스 백신 프로그램 설치 및 주기적 업데이트

항목설명

바이러스 백신 프로그램 바이러스, 웜 등으로부터 시스템을 보호하기 위한 중요한 보안 요소이다. 최신 바이러스 탐지를 위하여 패턴 업데이트가 자주 발생하므로 이를 즉각적으로 반영하는 것이 중요하다.

진단 기준

양호

백신이 설치되어 있고, 최신 업데이트가 적용되어 있는 경우

취약

백신이 설치되어 있지 않거나, 최신 업데이트가 적용되어 있지 않은 경우

진단 방법

■ 수동점검

백신 프로그램의 설치 여부와 최신 Update 여부를 수동으로 점검

조치 방법

■ 바이러스 백신 설치 후 최신 업데이트를 적용

바이러스 백신 프로그램에서 제공하는 실시간 감시 기능 활성화

항목설명

바이러스 백신 프로그램의 실시간 감시 기능으로 바이러스, 스파이웨어 탐지 및 방화벽 설정 등이 가능하다. 시스템에 대한 위협 발생 시 즉시 대응이 가능하도록 실시간 감시 기능을 사용할 것을 권고한다.

진단 기준

양호

설치된 백신의 실시간 감시 기능이 활성화되어 있는 경우

취약

백신이 설치되어 있지 않거나, 실시간 감시 기능이 비활성화되어 있는 경우

진단 방법

■ 수동점검

백신의 실시간 감시 기능이 활성화되어 있는지 수동으로 점검

조치 방법

■ 바이러스 백신의 실시간 감시 기능을 활성화

OS에서 제공하는 침입차단 기능 활성화

항목설명

윈도우에서 제공하는 침입차단 기능인 윈도우 방화벽을 사용함으로써 PC의 자료 유출 방지, 불법 접근 차단 등을 가능하게 한다. 네트워크 방화벽과 더불어 각각의 PC에 윈도우 방화벽과 같은 호스트 기반의 방화벽을 구현할 때 네트워크의 방어 수준이 향상될 수 있다.

진단 기준

양호

Windows 방화벽이 “사용”으로 설정되어 있는 경우

취약

Windows 방화벽이 “사용 안 함”으로 설정되어 있는 경우

진단 방법

■ 제어판에서 확인

[Win10, Win11]

1) 제어판 → Windows Defender 방화벽(관리도구(큰 아이콘, 작은 아이콘))
시작 → 실행(Win+r) → “firewall.cpl” 입력

2) Windows 방화벽 사용 여부를 확인

조치 방법

※ Windows 방화벽을 사용하도록 설정

■ 제어판에서 설정

[Win10, Win11]

1) 시작 → 제어판 → Windows Defender 방화벽 → Windows Defender 방화벽 설정 또는 해제

2) “Windows Defender 방화벽 사용” 설정

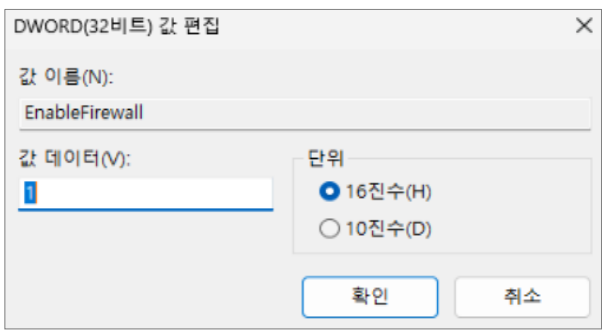
■ 레지스트리에서 설정

[Win10, Win11]

1) 시작 → 실행(Win+r) → “regedit” 입력

2) HKLM\SYSTEM\CurrentControlSet\Services\SharedAccess\Parameters\FirewallPolicy\StandardProfile

3) EnableFirewall의 값 데이터를 1로 설정



화면보호기 대기 시간 설정 및 재시작 시 암호 보호 설정

항목설명

사용자가 일정 시간 동안 아무런 작업을 수행하지 않을 경우 자동으로 로그오프 되거나 워크스테이션이 잠기도록 설정하여야 한다. 해당 기능을 설정하지 않은 경우 사용자가 자리를 비운 사이에 임의의 사용자가 해당 시스템에 접근하여 중요 정보를 유출하거나, 악의적인 행위를 통해 시스템 운영에 악영향을 미칠 수 있으므로 화면보호기 대기 시간 및 암호 사용 설정을 이용해서 비인가자의 물리적 접근을 차단한다.

진단 기준

양호

화면보호기 설정 및 암호로 보호가 설정되어 있는 경우

취약

화면보호기 설정 및 암호로 보호가 설정되어 있지 않은 경우

진단 방법

■ 화면보호기 설정이 되어 있는지 확인

[Win10]

1) 시작 → 제어판 → 개인 설정 → 화면보호기에서 화면 보호기설정 확인

[Win11]

1) 바탕화면 → 마우스 우클릭 → 개인 설정 → 잠금 화면 → 화면 보호기에서 화면보호기 설정 확인

2) 시작 → 실행(Win+r) → “regedit” 입력 → HKEY_CURRENT_USER\Control Panel\Desktop에서 ScreenSaveActive, ScreenSaverIlSecure, ScreenSaveTimeOut 설정값 확인

조치 방법

■ 화면보호기 설정이 되어 있는지 확인

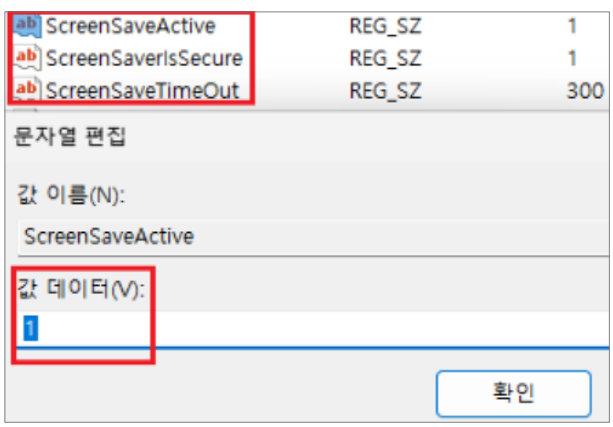
[Win10, Win11]

1) 바탕화면 → 마우스 우클릭 → 개인 설정 → 잠금 화면 → 화면 보호기에서 화면보호기 설정

2) 대기 시간을 5분~10분 사이로 설정 후 “다시 시작할 때 로그온 화면 표시(R)” 체크

3) 시작 → 실행(Win+r) → “regedit” 입력 → HKEY_CURRENT_USER\Control Panel\Desktop에서 ScreenSaveActive, ScreenSaverlSecure, ScreenSaveTimeOut 설정

4) ScreenSaveActive 값 1, ScreenSaverIsSecure 값 1, ScreenSaveTimeOut 값 600 이하로 설정



CD, DVD, USB 메모리 등과 같은 미디어의 자동실행 방지 등 이동식 미디어에 대한 보안 대책 수립

항목설명

CD/DVD, USB 메모리 등과 같은 미디어에 탑재된 “Autorun.inf*” 파일을 통해 다른 응용 프로그램이 자동 실행될 수 있다. 대부분의 USB 관련 악성코드들은 Autorun.inf 파일을 통해 자동 실행되도록 제작되므로 이를 통해 악성코드가 PC로 쉽게 유입될 가능성이 존재한다.

* 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 제어한다.

진단 기준

양호

미디어 사용 시 자동 실행되지 않는 경우

취약

미디어 사용 시 자동 실행되는 경우

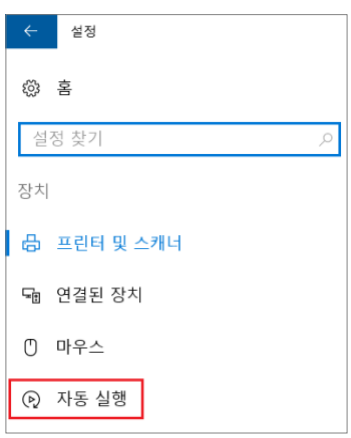
진단 방법

※ 미디어 사용 시 자동 실행되지 않도록 설정되어 있는지 확인

■ 설정에서 확인

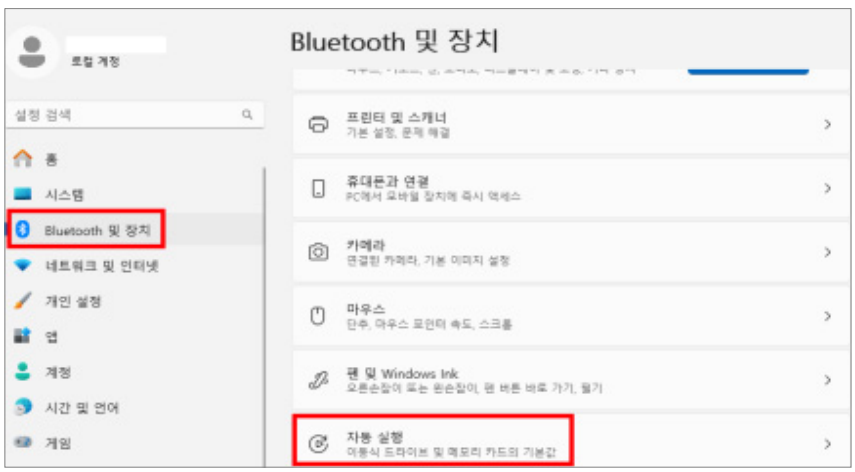
[Win10]

1) 시작 → 설정 → 장치 → 자동 실행 → 모든 미디어 및 장치에 자동 실행 사용 설정 확인



[Win11]

1) 시작 → 설정 → Bluetooth 및 장치 → 자동 실행 → 모든 미디어 및 장치에 자동 실행 사용 설정 확인



■ 레지스트리에서 확인

[Win10, Win11]

1) 시작 → 실행(Win+r) → "regedit" 입력

2) HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\AutoplayHandlers

3) DisableAutoplay 값이 1로 설정되어 있는지 확인
(모든 미디어 및 장치에 자동 실행 사용 설정이 "켬"으로 설정되어 있는 경우 DisableAutoplay 데이터가 존재하지 않음.)

조치 방법

※ 미디어 사용 시 자동 실행되지 않도록 설정

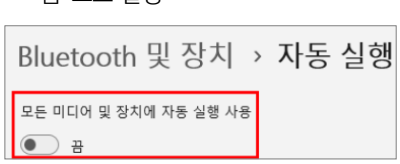
■ 설정에서 설정

[Win10]

1) 시작 → 설정 → 장치 → 자동 실행 → 모든 미디어 및 장치에 자동 실행 사용 설정 확인

[Win11]

1) 시작 → 설정 → Bluetooth 및 장치 → 자동실행 → 모든 미디어 및 장치에 자동 실행 사용 "끔"으로 설정



■ 레지스트리에서 설정

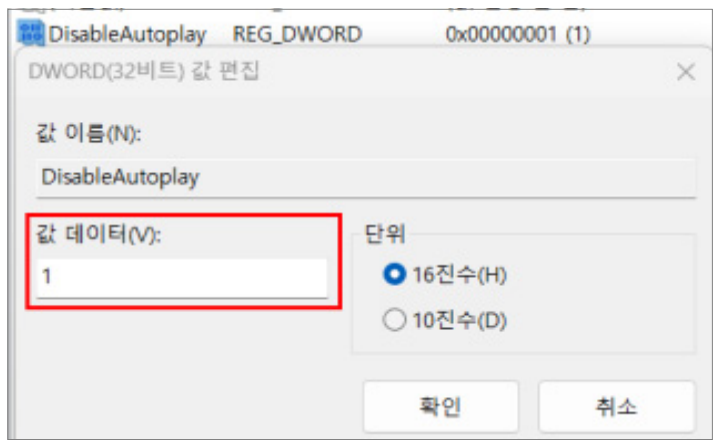
[Win10, Win11]

1) 시작 → 실행(Win+r) → “regedit” 입력

2) HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\AutoplayHandlers

3) DisableAutoplay 데이터 값을 1로 설정

4) DisableAutoplay가 존재하지 않는 경우 DWORD(32비트) 값으로 생성 후 데이터 값 1로 설정



비인가 무선 랜 사용제한

항목설명

내부에 설치된 비인가 AP 또는 사용자의 잘못된 설정으로 인한 Ad-Hoc 네트워크가 기업 네트워크의 백도어 역할을 하여 해당 위협 요소를 통해 불법 침입자가 내부 네트워크로 접근할 수 있다. 공공장소 무선 AP의 경우 해킹이나 관리자 계정의 중요성을 알지 못하거나, 손님 편의를 위해 패스워드를 공개하고, 번거롭다는 이유로 보안에 취약한 펌웨어 업데이트를 하지 않는 등 다양한 보안 위협요소가 존재한다.

진단 기준

양호
비인가 무선 랜을 사용하고 있지 않은 경우

취약
비인가 무선 랜을 사용하고 있는 경우

진단 방법

※ 무선 랜 사용 여부를 확인

■ 명령 프롬프트에서 확인

[Win10, Win11]

1) 시작 → 실행(Win+r) → cmd → netsh wlan show profile 입력

2) 사용자 프로필에서 비인가 무선 랜 사용 여부 확인

```
C:₩Windows₩System32>netsh wlan show profile

Wi-Fi 인터페이스의 프로필:

그룹 정책 프로필(읽기 전용)
---------------------------
    <없음>

사용자 프로필
------------
    모든 사용자 프로필 :
    모든 사용자 프로필 :
    모든 사용자 프로필 : iptime
    모든 사용자 프로필 :
```

조치 방법

※ 비인가 무선 랜을 차단
※ 허용할 무선 랜들을 접근 허용으로 설정 후 denyall 정책을 사용
※ 명령 프롬프트(cmd)는 관리자 권한으로 실행

■ 명령 프롬프트에서 설정

[Win10, Win11]

1) 시작 → 실행(Win+r) → cmd

2) netsh wlad add filterpermission=allow ssid=허용할 무선 랜 SSID networktype=infrastructure 입력

3) netsh wlan add filter permission=denyall network=infrastructure 입력

2.8.

PC(MAC)

2.8. PC(MAC)

계정 관리(4개 항목), 파일 시스템(2개 항목), 패치 관리(1개 항목), 보안 관리(8개 항목) 총 4개 영역에서 15개 항목으로 구성된다.

[표 8] PC(MAC) 진단 체크리스트

구분	진단 항목
가. 계정 관리	패스워드의 주기적 변경
	기관 보안 정책과 패스워드 정책 일치
	Guest 계정 비활성화
	자동 로그인 비활성화
나. 파일 시스템	공유 폴더 제거
	상용 메신저의 사용 금지
다. 패치 관리	안전한 버전의 OS 사용
라. 보안 관리	OS에서 제공하는 침입 차단 기능 활성화
	화면보호기 대기 시간 설정 및 재시작 시 암호 보호 설정
	시스템 수준의 환경설정에 접근 시 관리자 암호 요구 설정
	앱 보안 설정
	비인가 무선랜 사용 금지
	바이러스 백신 프로그램 설치 및 주기적 업데이트
	바이러스 백신 프로그램에서 제공하는 실시간 감시 기능 활성화
	원격 기능 비활성화

패스워드 주기적 변경

항목설명

계정의 패스워드를 주기적으로 변경하지 않고 오랜 기간 사용하는 경우 계정 패스워드가 외부로 유출될 수 있으며 관리자 계정의 패스워드가 유출될 시 자료 유출 등 심각한 사고 발생 가능성이 존재한다.

진단 기준

양호

암호 만료 기간이 90일(129600분) 이하로 설정된 경우

취약

암호 만료 기간이 설정되어 있지 않거나 90일(129600분)을 초과하는 경우

진단 방법

■ 명령 프롬프트에서 확인

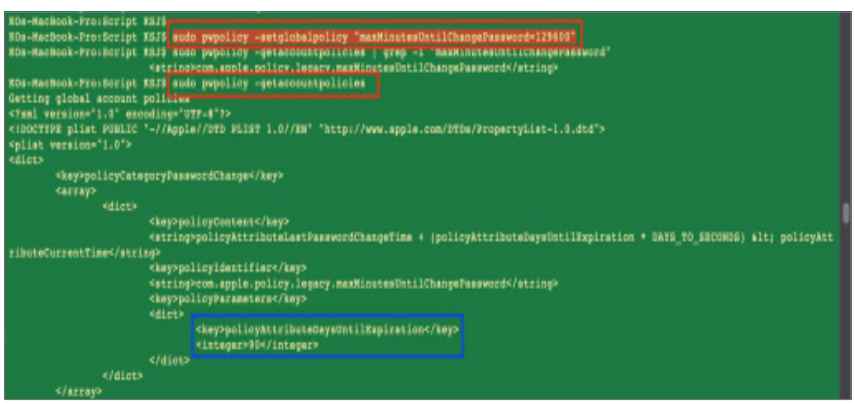
1) # pwpolicy getglobalpolicy 명령어 실행

2) "maxMinutesUntilChangePassword" 설정이 129600(분 단위) 이하로 적용되어 있는지 확인

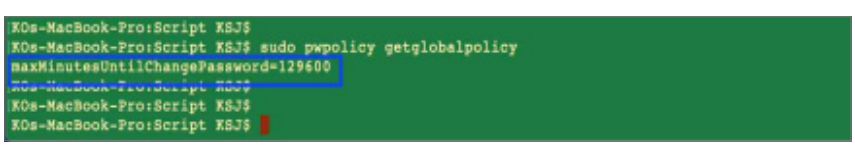
조치 방법

■ 터미널에서 최대 암호 사용 기간 설정

1) 패스워드 최대 사용 기간 설정
sudo pwpolicy -setglobalpolicy "maxMinutesUntilChangePassword=[암호 만료 기간(분 단위)]" 명령어 실행



2) 패스워드 최대 사용기간 설정 확인
pwpolicy getglobalpolicy 명령어 실행을 통해 최대 암호 사용 기간 적용 여부 확인



기관 보안 정책과 패스워드 정책 일치

항목설명

대부분 환경에서 3종류(영문 · 숫자 · 특수문자) 조합의 경우 8자리 패스워드 사용, 2종류(영문 · 숫자) 조합의 경우 10자리 암호 사용을 권고하고 있다. 패스워드 정책에 적합하게 패스워드가 설정된 경우 무작위 대입 공격(Brute Force Attack)이나 패스워드 추측 공격(Password Guessing)에 대한 대비가 가능하다.

진단 기준

양호

최소 암호 길이가 해당 기관의 보안 정책을 반영하여 설정되어있는 경우

취약

암호를 사용하지 않거나, 추측하기 쉬운 문자 조합으로 이루어진 짧은 자릿수의 패스워드를 사용하고 있는 경우

진단 방법

■ 터미널에서 최소 암호 길이 확인

1) # pwpolicy getglobalpolicy 명령어 실행

2) "minChar" 설정이 8자리 이상으로 적용되어 있는지 확인

```
KOs-MacBook-Pro:Script KSJ$
KOs-MacBook-Pro:Script KSJ$ pwpolicy getglobalpolicy
KOs-MacBook-Pro:Script KSJ$
KOs-MacBook-Pro:Script KSJ$
```

조치 방법

■ 터미널에서 최소 암호 길이 설정

1) # pwpolicy setglobalpolicy "minChar=[패스워드 길이]" 명령어 실행

```
KOs-MacBook-Pro:~ KSJ$
KOs-MacBook-Pro:~ KSJ$
KOs-MacBook-Pro:~ KSJ$ sudo pwpolicy setglobalpolicy "minChars=8"
Password:
KOs-MacBook-Pro:~ KSJ$
```

2) # pwpolicy getglobalpolicy 명령어 실행을 통해 적용 여부 확인

```
KOs-MacBook-Pro:~ KSJ$ pwpolicy getglobalpolicy
minChars=8 maxMinutesUntilChangePassword=129600
KOs-MacBook-Pro:~ KSJ$
KOs-MacBook-Pro:~ KSJ$
```

비고

■ 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
   (5) 주기성 패스워드 재사용 금지
   (6) 전화번호, 생일과 같이 추측하기 쉬운 개인정보를 패스워드로 사용 금지

3. SAM 파일에 암호를 저장하기 위해 사용되는 LANMan 알고리즘은 8자 단위로 글자를 나누어 암호화하기 때문에 8의 배수가 되는 암호 사용을 권장 (8자로 이루어진 암호 사용 권장)

4. 아래와 같은 암호 설정 지양
   Null, 계정과 동일하거나 유사한 스트링, 지역명, 부서명, 담당자명, 대표 업무명
   예) root, rootroot, root123, 123root, admin, admin123, 123admin, osadmin, adminos

항목 Guest 계정 비활성화

항목설명

MAC OS에는 Guest 계정 로그인 허용, 공유 폴더 연결 허용 설정이 존재한다. 만약 Guest 계정이 활성화되면 공유 폴더에 접근하여 중요 자료가 노출될 가능성이 존재한다

진단 기준

양호

Guest 계정 허용 설정이 적용되지 않은 경우

취약

Guest 계정 허용 설정이 적용된 경우

진단 방법

■ 터미널에서 Guest 계정 허용 설정 확인

1) # defaults read /Library/Preferences/com.apple.loginwindow GuestEnabled 명령어를 실행

```
KOs-MacBook-Pro:~ KSJ$
KOs-MacBook-Pro:~ KSJ$ defaults read /Library/Preferences/com.apple.loginwindow GuestEnabled
1
KOs-MacBook-Pro:~ KSJ$
```

- 출력값이 '0'인 경우 양호

2) # defaults read /Library/Preferences/com.apple.AppleFileServer.plist guestAccess 명령어를 실행

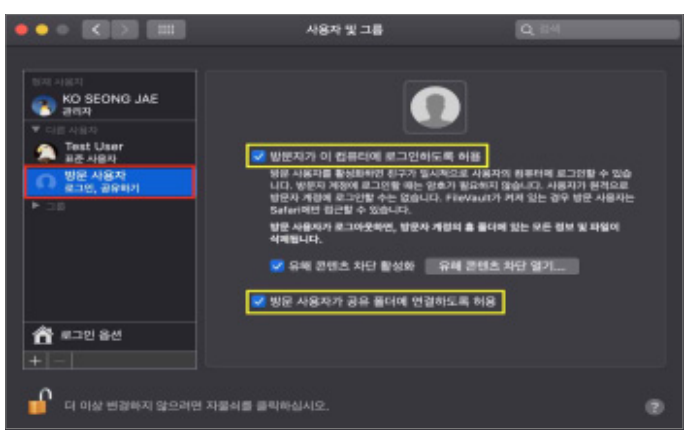
```
KOs-MacBook-Pro:~ KSJ$ defaults read /Library/Preferences/com.apple.AppleFileServer.plist guestAccess
1
KOs-MacBook-Pro:~ KSJ$
```

- 출력값이 '0'인 경우 양호

■ 시스템 환경설정에서 Guest 계정 설정 확인

1) 시스템 환경설정 → 사용자 및 그룹 → 방문 사용자

2) 방문 사용자 설정 확인



조치 방법

■ 터미널에서 Guest 계정 비활성화 설정

1) # sudo defaults write /Library/Preferences/com.apple.loginwindow GuestEnabled –bool false 실행

```
KOs-MacBook-Pro:~ KSJ$
KOs-MacBook-Pro:~ KSJ$
KOs-MacBook-Pro:~ KSJ$ defaults read /Library/Preferences/com.apple.loginwindow GuestEnabled
0
KOs-MacBook-Pro:~ KSJ$
```

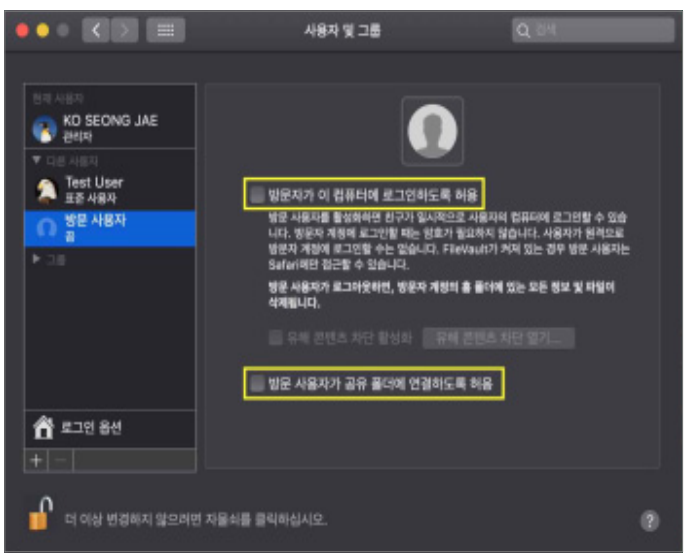
2) # sudo defaults write /Library/Preferences/com.apple.AppleFileServer.plist guestAccess –bool false 실행

```
KOs-MacBook-Pro:~ KSJ$
KOs-MacBook-Pro:~ KSJ$
KOs-MacBook-Pro:~ KSJ$ defaults read /Library/Preferences/com.apple.AppleFileServer.plist guestAccess
0
KOs-MacBook-Pro:~ KSJ$
KOs-MacBook-Pro:~ KSJ$
KOs-MacBook-Pro:~ KSJ$
```

■ 시스템 환경설정에서 Guest 계정 비활성화 설정

1) 시스템 환경설정 → 사용자 및 그룹 → 방문 사용자

2) 방문 사용자 체크박스 해제



자동 로그인 비활성화

항목설명

자동 로그인이 설정된 계정이 존재할 경우 비인가자가 인증절차 없이 로그인하여 설정을 변경하거나 주요 정보가 탈취될 가능성이 존재한다.

진단 기준

양호
자동 로그인이 비활성화되어 있는 경우

취약
자동 로그인이 활성화되어 있는 경우

진단 방법

■ 터미널에서 자동 로그인이 설정된 계정 확인

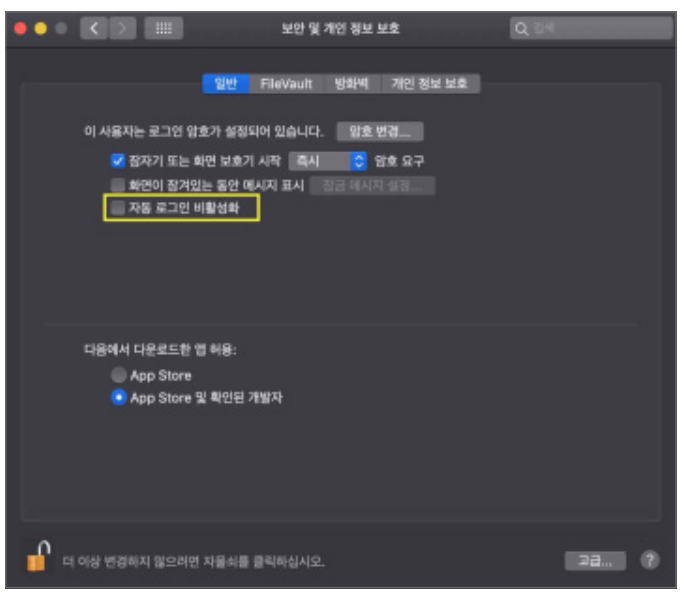
1) # defaults read /Library/Preferences/com.apple.loginwindow autoLoginUser 명령어를 실행

- 자동 로그인이 설정된 계정(KSJ)을 확인할 수 있음

■ 시스템 환경설정에서 자동 로그인 설정 확인

1) 시스템 환경설정 → 보안 및 개인 정보 보호 → 일반

2) 자동 로그인 비활성화 확인



- '자동 로그인 비활성화'가 체크 해제되어 있음을 알 수 있음

조치 방법

■ 터미널에서 자동 로그인 비활성화 설정

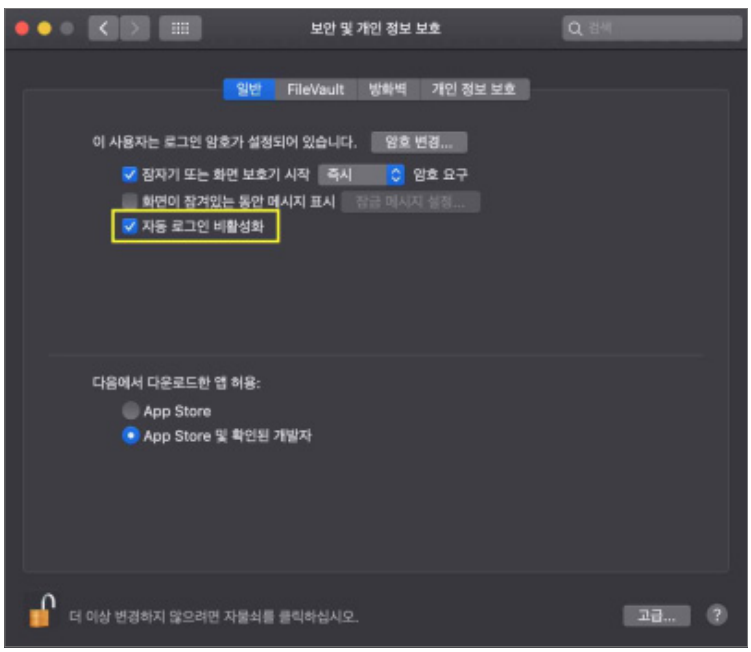
```
KOs-MacBook-Pro:~ KSJ$ sudo defaults delete /Library/Preferences/com.apple.loginwindow autoLoginUser
KOs-MacBook-Pro:~ KSJ$ defaults read /Library/Preferences/com.apple.loginwindow autoLoginUser
2021-01-06 16:14:30.020 defaults[4421:1372061]
The domain/default pair of (/Library/Preferences/com.apple.loginwindow, autoLoginUser) does not exist
KOs-MacBook-Pro:~ KSJ$
KOs-MacBook-Pro:~ KSJ$
```

- autoLoginUser가 삭제됨을 알 수 있음

■ 시스템 환경설정에서 자동 로그인 비활성화 설정

1) 시스템 환경설정 → 보안 및 개인 정보 보호 → 일반

2) 자동 로그인 비활성화 체크



공유 폴더 제거

항목설명

MAC은 계정 생성 시 공유 폴더가 생성되며 파일 공유를 Default로 설정할 경우, 읽기 권한을 가진 계정도 파일을 복사할 수 있어 비인가자가 악의적으로 대용량 파일을 다량 복사하여 하드디스크 자원을 고갈시킬 수 있으므로 공유 폴더 사용 시 별도의 폴더를 사용하고 Everyone 권한을 제거해야 한다.

진단 기준

양호

불필요한 공유 폴더가 존재하지 않는 경우

취약

불필요한 공유 폴더가 존재하는 경우

진단 방법

■ 터미널에서 파일 공유 활성화 확인

1) # launchctl print system | egrep “smbd|AppleFileServer” 명령어를 실행

- “com.apple.smbd” 설정이 false인 경우, 파일 공유 활성화 상태

■ 시스템 환경설정에서 파일 공유 활성화 확인

1) 시스템 환경설정 → 공유 → 파일 공유에서 활성화 확인

조치 방법

■ 터미널에서 파일 공유 중지

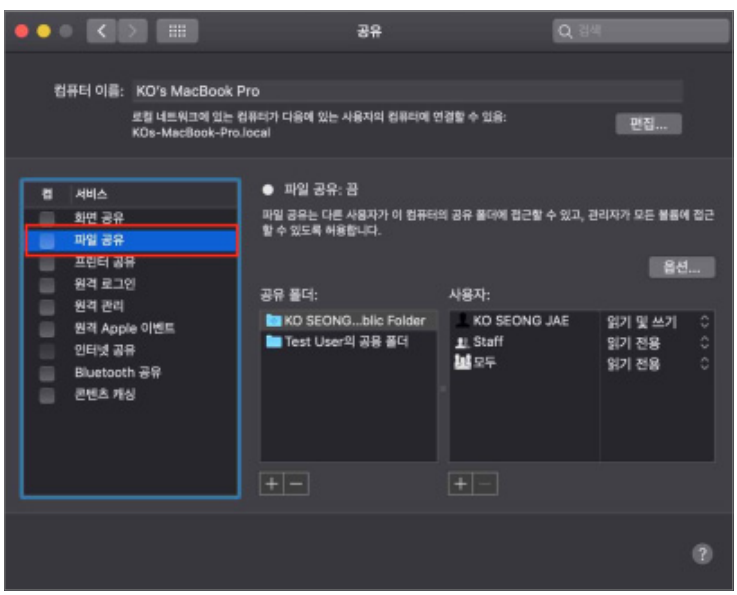
1) # sudo launchctl unload –w /System/Library/LaunchDaemons/com.apple.smbd.plist 명령어를 실행하여 SMB 파일 공유 중지

– “com.apple.smbd” 설정이 true인 경우, 파일 공유 비활성화 상태

2) # sudo launchctl unload –w /System/Library/LaunchDaemons/com.apple.AppleFileServer.plist 명령어를 실행하여 AppleFileServer 파일 공유 중지

■ 시스템 환경설정에서 기본 공유 중지

1) 시스템 환경설정 → 공유 → 파일 공유 체크박스 해제



■ 공유 폴더를 사용하는 경우

1) 시스템 환경설정 → 공유 → 파일 공유

2) 공용 폴더 제거 후 별도의 공유 폴더 지정

3) 공유 폴더 → 사용자에서 Everyone(모두) 권한을 접근 불가로 설정

상용 메신저의 사용 금지

항목설명

일반 사용자 PC에서 Messenger를 사용할 경우, 메신저(Messenger)를 통해서 주요 정보가 유출될 수 있을 뿐만 아니라 악성코드가 유입될 수 있다. 따라서 상용 메신저는 설치 및 실행하지 않아야 한다.

진단 기준

양호

상용 Messenger가 설치 및 실행되고 있지 않은 경우

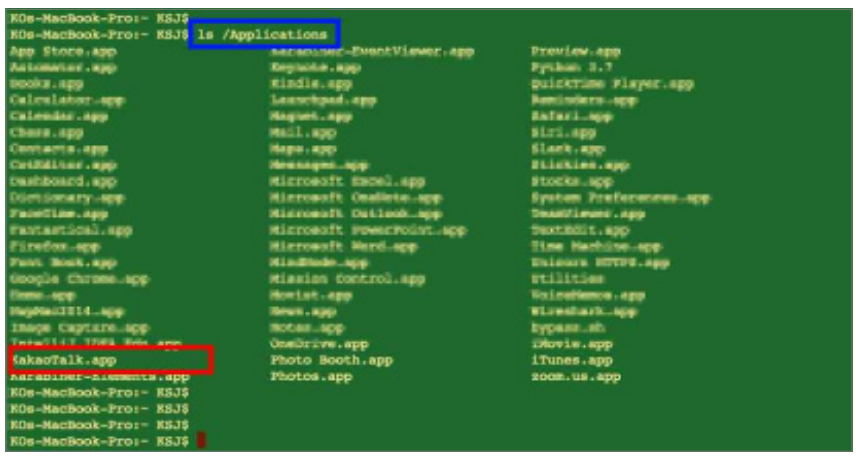
취약

상용 Messenger가 설치 및 실행되고 있는 경우

진단 방법

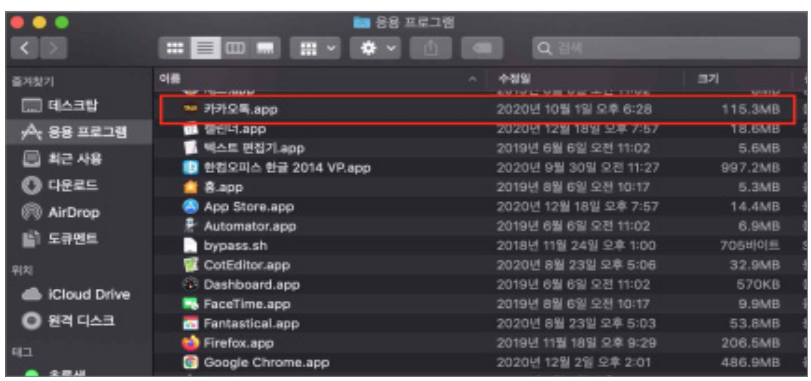
■ 터미널에서 확인

1) ls /Application 명령어를 실행



■ Finder에서 확인

1) Finder → 응용 프로그램에서 상용 메신저 설치 여부 확인



- "카카오톡.app" 메신저가 존재함을 알 수 있음

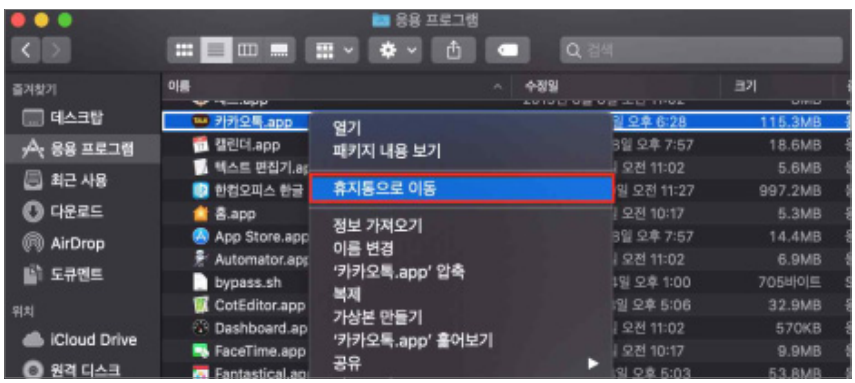
조치 방법

■ Finder에서 제거

1) Finder → 응용 프로그램

2) 상용 메신저 아이콘 우측 클릭 → 휴지통으로 이동 클릭

3) 휴지통 → 휴지통 비우기 클릭



안전한 버전의 OS 사용

항목설명

최신 HOT FIX 설치 및 자동 업데이트가 설정되어 있지 않은 경우 취약점으로 인한 공격이 발생할 수 있으므로 HOT FIX 출시 즉시 신속하게 설치하고 항상 최신의 보안 업데이트가 이루어져야 한다.

진단 기준

양호

최신 HOT FIX 설치 및 자동 업데이트 설정이 되어 있는 경우

취약

HOT FIX 설치 및 자동 업데이트 설정이 되어 있지 않은 경우

진단 방법

■ 최신 패치 여부 확인

1) 왼쪽 상단 Apple 아이콘 → “이 Mac에 관하여“ 클릭

조치 방법

■ 최신 패치 적용 및 자동 설정

1) 왼쪽 상단 Apple 아이콘 → “이 Mac에 관하여” → “소프트웨어 업데이트..” 클릭

2) 우측 하단 “고급...” 클릭

※ 자동으로 Mac 최신으로 유지하기“의 경우, 호환성을 위해 체크박스 체크 권고

3) ”업데이트 확인“, ”사용 가능할 때 새로운 업데이트 다운로드“, ”시스템 데이터 파일 및 보안 업데이트 설치“ 항목 체크

OS에서 제공하는 침입 차단 기능 활성화

항목설명

MAC에서 제공하는 침입 차단 기능인 방화벽을 사용함으로써 PC의 자료 유출 방지, 불법 접근 차단 등을 가능하게 한다. 네트워크 방화벽과 더불어 각각의 PC에 MAC 방화벽과 같은 호스트 기반의 방화벽을 구현할 때 네트워크의 방어 수준이 향상될 수 있다.

진단 기준

양호

MAC 방화벽이 “켬”으로 설정되어 있는 경우

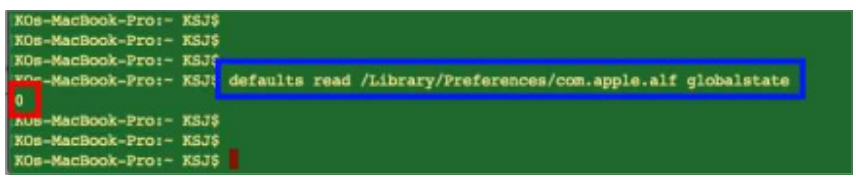
취약

MAC 방화벽이 “끔”으로 설정되어 있는 경우

진단 방법

■ 터미널에서 확인

1) # defaults read /Library/Preferences/com.apple.alf globalstate 명령어를 실행



- 출력값 0 (취약)

■ 시스템 환경설정에서 확인

1) 시스템 환경설정 → 보안 및 개인 정보보 호호 → 방화벽 탭 → 방화벽 설정 확인

- 방화벽: 끔(취약)

조치 방법

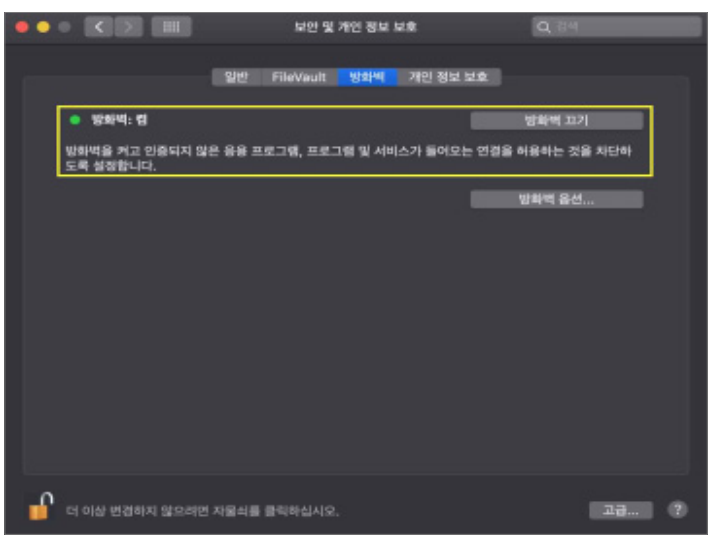
■ 명령어에서 방화벽 활성화

1) # defaults write /Library/Preferences/com.apple.alf globalstate –bool true 명령어 실행

■ 시스템 환경설정에서 방화벽 활성화

1) 시스템 환경설정 → 보안 및 개인 정보 보호 → 방화벽 탭에서 “방화벽 켜기” 클릭

2) 방화벽 설정 확인



화면보호기 대기 시간 설정 및 재시작 시 암호 보호 설정

항목설명

사용자가 일정 시간 동안 아무런 작업을 수행하지 않을 경우 자동으로 로그오프 되거나 워크스테이션이 잠기도록 설정해야 한다. 해당 기능을 설정하지 않은 경우 사용자가 자리를 비운 사이에 임의의 사용자가 해당 시스템에 접근하여 중요 정보를 유출하거나, 악의적인 행위를 통해 시스템 운영에 악영향을 미칠 수 있으므로 화면보호기 대기 시간 및 암호 사용 설정을 통해 비인가자의 물리적 접근을 차단 해야 한다.

진단 기준

양호

화면보호기 설정(10분 이하) 및 암호 요구 설정이 적용된 경우

취약

화면보호기 설정(10분 이하) 및 암호 요구 설정이 적용된 경우

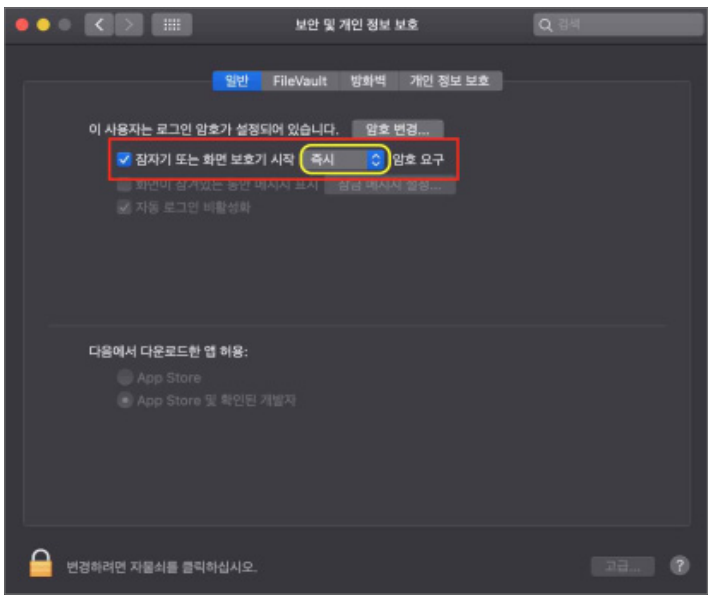
진단 방법

■ 시스템 환경설정에서 화면 보호기 및 암호 보호 설정 확인

1) 시스템 환경설정 → 데스크탑 및 화면 보호기 → [화면 보호기] 탭에서 화면 보호기 활성화 확인

- 화면 보호기 설정 20분(취약)

2) 시스템 환경설정 → 보안 및 개인 정보 보호 → [일반] 탭에서 화면 보호기 시작 및 암호 요구 시간 확인

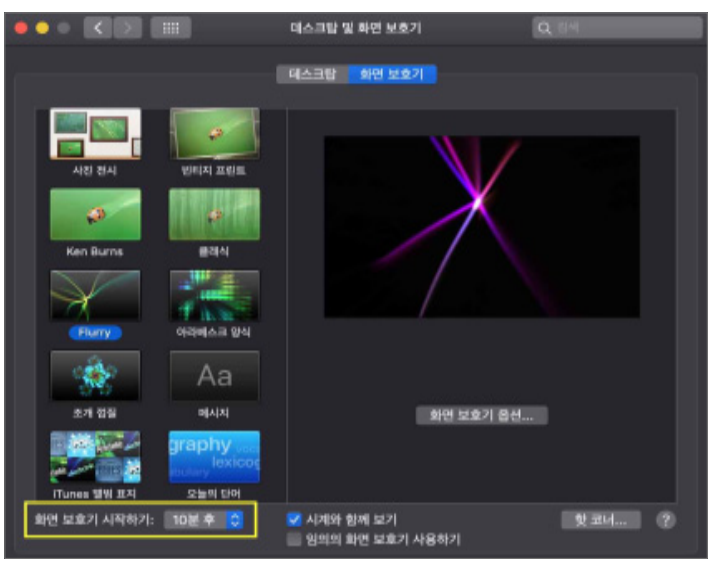


- '잠자기 또는 화면 보호기 시작 암호요구' 설정이 "즉시"(양호)

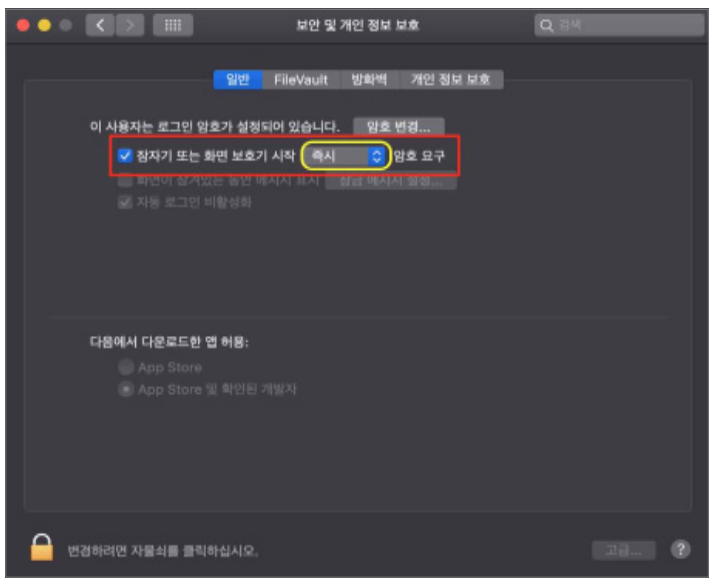
조치 방법

■ 화면보호기 설정이 되어 있는지 확인

1) 시스템 환경설정 → 데스크탑 및 화면 보호기 → [화면 보호기] 탭에서 화면 보호기 시간 5~10분 사이로 설정



2) 시스템 환경설정 → 보안 및 개인 정보 보호 → [일반] 탭에서 “잠자기 또는 화면 보호기 시작” 체크 후 암호 요구 시간을 “즉시”로 설정



터미널 접근 시 관리자 암호 요구 설정

항목설명

관리자 암호 요구 설정이 적용되지 않을 경우 비인가자가 해당 시스템의 설정을 변경하여 중요 정보를 탈취할 가능성이 존재한다.

진단 기준

양호

관리자 암호 요구 설정이 활성화되어 있는 경우

취약

관리자 암호 요구 설정이 비활성화되어 있는 경우

진단 방법

■ 터미널에서 관리자 암호 요구 설정 확인

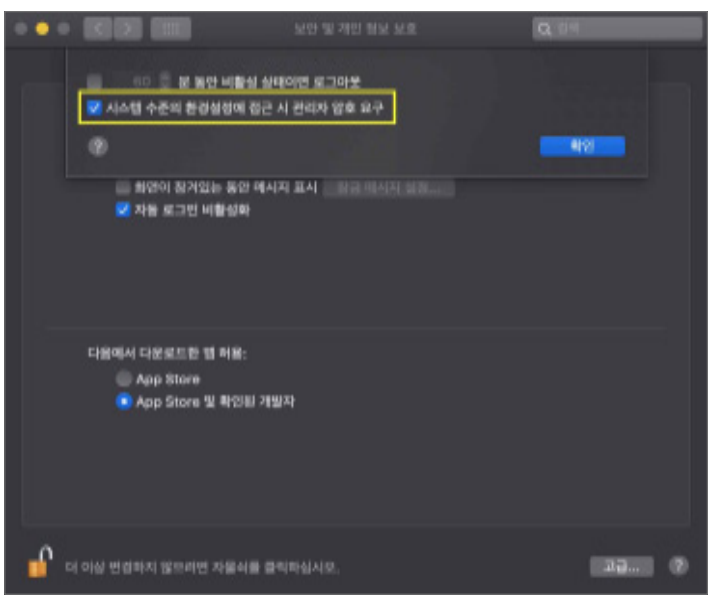
1) security authorizationdb read system.preferences | grep -A 1 shared 명령어 실행

```
KOs-MacBook-Pro:~ KSJ$
KOs-MacBook-Pro:~ KSJ$ security authorizationdb read system.preferences |  grep -A 1 shared
        <key>shared</key>
        <true/>
YES (0)
KOs-MacBook-Pro:~ KSJ$
```

- shared: true(취약)

■ 시스템 환경설정에서 관리자 암호 요구 설정 확인

1) 시스템 환경설정 → 보안 및 개인 정보 보호 → [일반] 탭에서 고급 버튼 클릭 후 확인



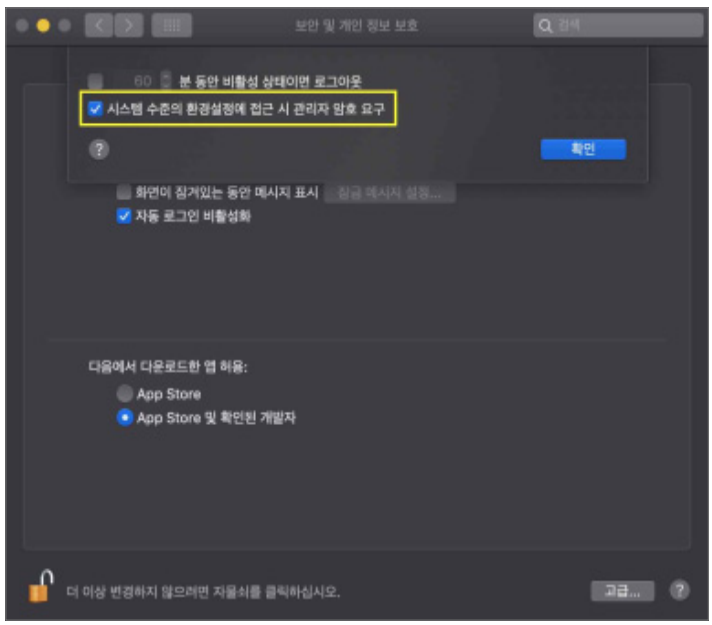
- '시스템 수준의 환경설정에 접근 시 관리자 암호 요구' 설정 체크 (양호)

조치 방법

■ 시스템 환경설정에서 관리자 암호 요구 설정

1) 시스템 환경설정 → 보안 및 개인 정보 보호 → [일반] 탭에서 고급 버튼 클릭

2) "시스템 수준의 환경설정에서 접근 시 관리자 암호 요구" 체크 후 승인 클릭



※ 위 암호 요구 설정 체크(활성화)시 아래와 같이 shared 설정값이 false로 바뀜

```
KOs-MacBook-Pro:~ KSJ$
KOs-MacBook-Pro:~ KSJ$ security authorizationdb read system.preferences |  grep -A 1 shared
        <key>shared</key>
        <false/>
YES (0)
KOs-MacBook-Pro:~ KSJ$
```

앱 보안 설정

항목설명

MAC OS에는 앱의 출처를 확인하는 기능이 존재한다. 만약 앱 보안 설정을 "모든 곳"으로 허용할 경우 악의적인 프로그램이 설치되어 주요 정보가 유출되거나 시스템 운영에 악영향을 미칠 가능성이 존재한다.

진단 기준

양호

"웹에서 다운로드한 앱을 허용" 설정이 "모든 곳"으로 설정되어 있지 않은 경우

취약

"웹에서 다운로드한 앱을 허용" 설정이 "모든 곳"으로 설정되어 있는 경우

진단 방법

■ 터미널에서 앱 보안 설정 확인

1) # spctl --status 명령어 실행

```
KOs-MacBook-Pro:~ KSJ$
KOs-MacBook-Pro:~ KSJ$
KOs-MacBook-Pro:~ KSJ$ spctl --status
assessments disabled
```

- assessments disabled (취약)

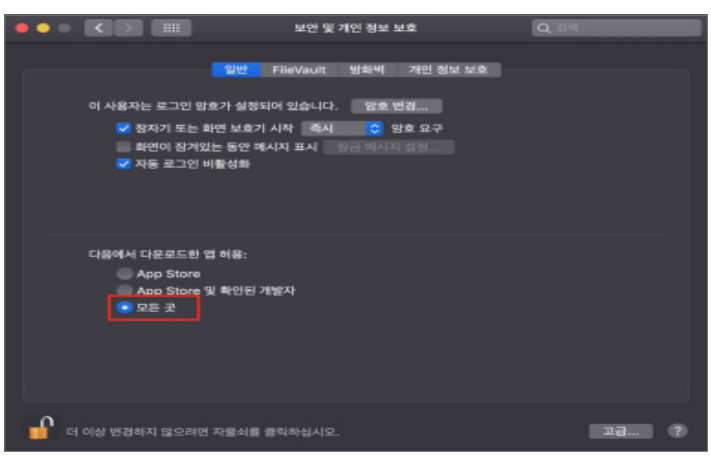
2) # defaults read com.apple.LaunchServices | grep LSQuarantine 명령어 실행

```
KOs-MacBook-Pro:~ KSJ$
KOs-MacBook-Pro:~ KSJ$ defaults read com.apple.LaunchServices | grep LSQuarantine
    LSQuarantine = 0;
KOs-MacBook-Pro:~ KSJ$
KOs-MacBook-Pro:~ KSJ$
```

- LSQuarantine: 0 (GateKeeper 비활성화)

■ 시스템 환경설정에서 앱 보안 설정 확인

1) 시스템 환경설정 → 보안 및 개인 정보 보호 → [일반] 탭에서 앱 허용 수준 확인



- 다음에서 다운로드한 앱 허용: → 모든 곳 활성화 (취약)

조치 방법

■ 터미널에서 앱 보안 설정 확인

1) # defaults write com.apple.LaunchServices LSQuarantine –bool true 명령어 실행

2) # defaults delete com.apple.LaunchServices 명령어 실행

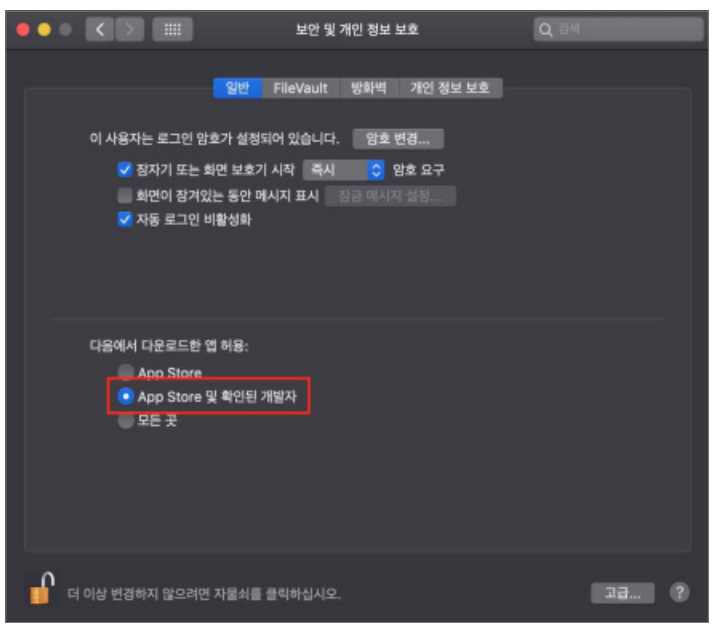
```
KOs-MacBook-Pro:~ KSJ$
KOs-MacBook-Pro:~ KSJ$ defaults write com.apple.LaunchServices LSQuarantine -bool true
KOs-MacBook-Pro:~ KSJ$ defaults read com.apple.LaunchServices | grep LSQuarantine
    LSQuarantine = 1;
KOs-MacBook-Pro:~ KSJ$
KOs-MacBook-Pro:~ KSJ$
KOs-MacBook-Pro:~ KSJ$ defaults delete com.apple.LaunchServices
KOs-MacBook-Pro:~ KSJ$
KOs-MacBook-Pro:~ KSJ$ defaults read com.apple.LaunchServices
2021-01-06 15:01:17.775 defaults[1005:44013]
Domain com.apple.LaunchServices does not exist
KOs-MacBook-Pro:~ KSJ$
KOs-MacBook-Pro:~ KSJ$
```

– LSQuarantine 설정값이 존재하지 않으므로 GateKeeper가 활성화됨을 알 수 있음

■ 시스템 환경설정에서 앱 보안 설정 확인

1) 시스템 환경설정 → 보안 및 개인 정보 보호 → [일반] 탭

2)" 다음에서 다운로드한 앱 허용" 수준의 App Store 및 확인된 개발자 이상으로 체크



비고

※ MacOS Sierra 이상부터 앱 허용 수준에 "모든 곳"이 존재하지 않으나 터미널 명령어를 통해 우회할 수 있음

비인가 무선랜 사용 금지

항목설명

비인가된 무선랜을 사용할 경우 NAC 등의 통제를 우회하여 인터넷에 접근이 가능하며 PC가 악성코드에 감염될 가능성이 존재한다.

진단 기준

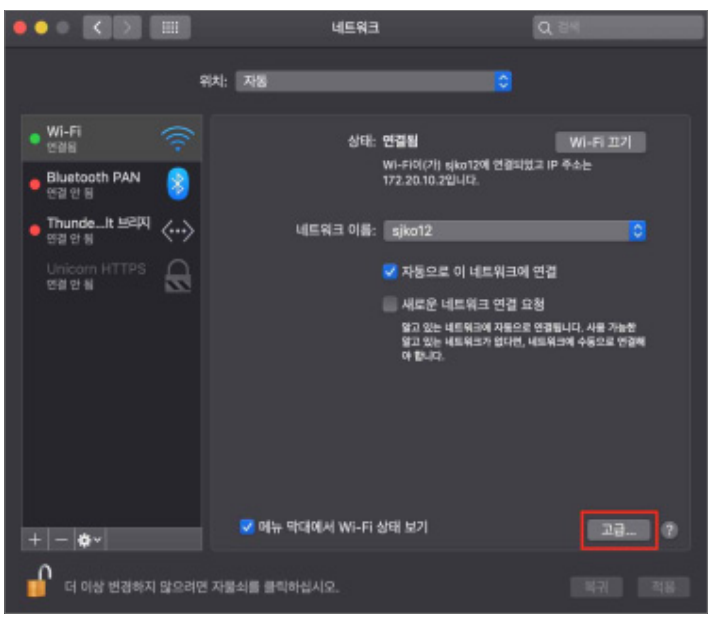
양호
비인가 무선랜을 사용하고 있지 않은 경우

취약
비인가 무선랜을 사용하고 있는 경우

진단 방법

■ 무선 랜 사용 여부 확인

1) 왼쪽 상단 Apple 아이콘 → 시스템 환경설정 → "네트워크" 클릭하여 무선 랜 사용 여부 확인



■ 무선 랜카드를 사용하는 경우

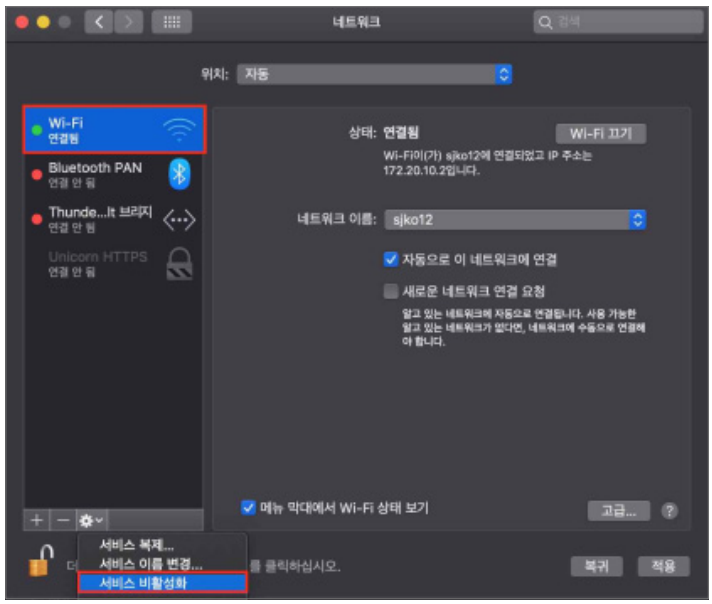
1) 벤더 전용 프로그램에서 비인가 무선랜 접속 확인

■ Mac AirPort를 사용하는 경우

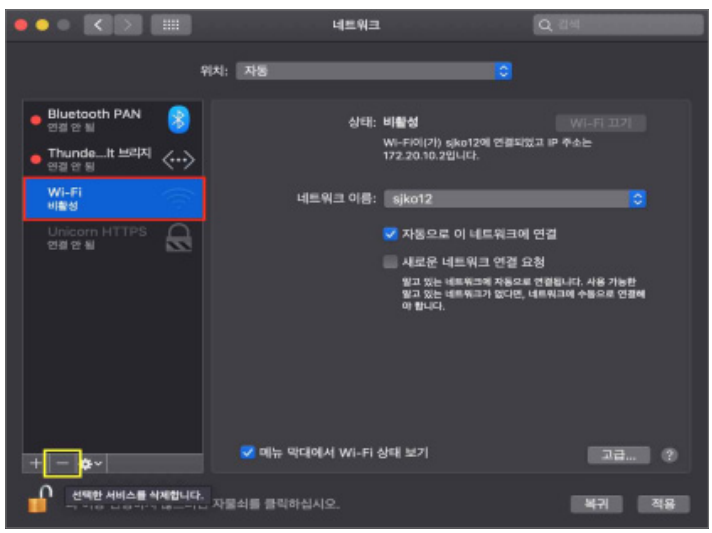
1) Finder → 응용 프로그램 → 유틸리티 → 키체인 접근 → 시스템에서 "AirPort 네트워크 암호"의 이름 (SSID) 확인

조치 방법

■ 무선 랜 비활성화 적용



-"WI-FI" 클릭 후 서비스 비활성화 클릭



-"WI-FI"를 클릭 후 "-"을 클릭하여 제거

■ 무선 AP를 사용하지 않을 시 무선랜 드라이버 제거

바이러스 백신 프로그램 설치 및 주기적 업데이트

항목설명

바이러스 백신 프로그램은 바이러스, 웜 등으로부터 시스템을 보호하기 위한 중요한 보안 요소이다. 백신 프로그램을 설치해야 하며 최신 바이러스 탐지를 위하여 패턴 업데이트가 자주 발생하므로 이를 즉각적으로 업데이트하여 반영하는 것이 중요하다.

진단 기준

양호

백신이 설치되어 있고, 최신 업데이트가 적용되어 있는 경우

취약

백신이 설치되어 있지 않거나, 최신 업데이트가 적용되어 있지 않은 경우

진단 방법

■ 백신 설치 여부 및 최신 업데이트

1) 백신 프로그램 설치 여부와 최신 Update 여부를 점검

조치 방법

■ 바이러스 백신 설치 후 최신 업데이트 적용

1) Avast Security for MAC 설치 (예시)

2) 백신 프로그램 실행 → 메뉴 → 기본 설정 → 일반 → '자동 업데이트 켜기' 활성화

백신 프로그램 실시간 감시 기능 활성화

항목설명

바이러스 백신 프로그램의 실시간 감시 기능으로 바이러스, 스파이웨어 탐지 등이 가능하다. 시스템에 대한 위협 발생 시 즉시 대응이 가능하도록 실시간 감시 기능을 사용할 것을 권고한다.

진단 기준

양호

설치되어 있는 백신의 실시간 감시 기능이 활성화되어 있는 경우

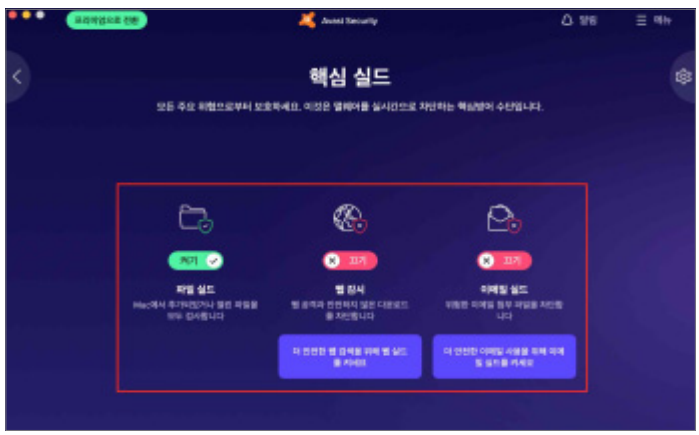
취약

설치되어 있는 백신의 실시간 감시 기능이 비활성화되어 있는 경우

진단 방법

■ 백신의 실시간 감시 기능 활성화 여부

1) 백신 프로그램의 실시간 감시 기능이 활성화되어 있는지 점검 (예시)



조치 방법

■ 백신의 실시간 감시 기능 활성화 (예시)

1) 백신 프로그램 실행 → 핵심 실드 → '실시간 실드 기능' 활성화

원격 기능 비활성화

항목설명

MAC OS에는 원격으로 접속하거나 명령어를 전달받아 실행하는 기능이 존재한다. 만약 원격기능을 허용할 경우 임의의 사용자에 의한 시스템 설정 변경 및 중요 정보 유출 가능성이 존재한다. 따라서 원격 기능이 불필요한 경우 해당 기능을 비활성화해야 한다.

진단 기준

양호

원격 기능이 비활성화되어 있는 경우

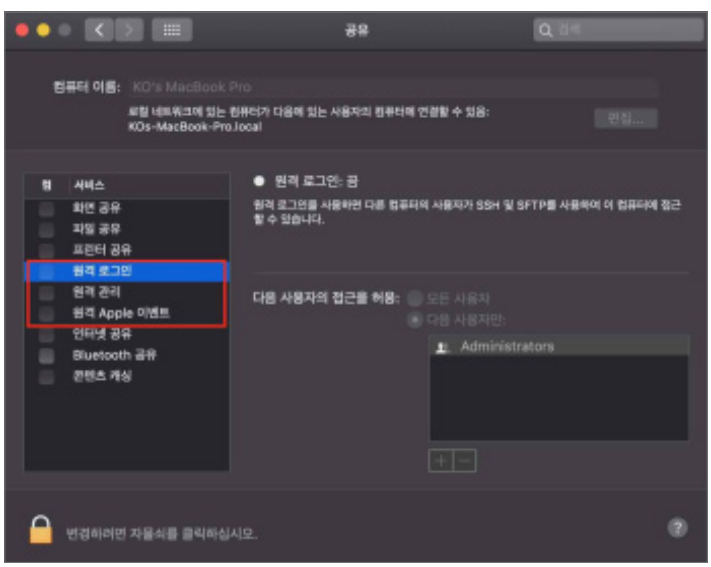
취약

원격 기능이 활성화되어 있는 경우

진단 방법

■ 시스템 환경설정에서 원격 기능 활성화 여부 확인

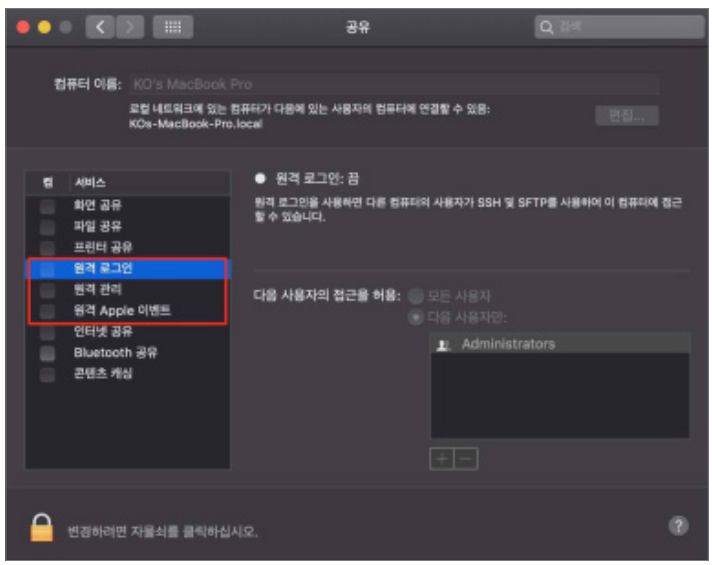
1) 왼쪽 상단 Apple 아이콘 → 공유 → [원격 로그인], [원격 관리], [원격 Apple 이벤트] 기능 확인



조치 방법

■ 시스템 환경설정에서 원격 기능 비활성화

1) 왼쪽 상단 Apple 아이콘 → 공유 → [원격 로그인], [원격 관리], [원격 Apple 이벤트] 기능 체크해제



2.9.

PC(Linux)

2.9. PC(Linux)

계정 관리(4개 항목), 파일 시스템(2개 항목), 패치 관리(1개 항목), 보안 관리(5개 항목) 총 4개 영역에서 12개 항목으로 구성된다.

[표 9] PC(Linux) 진단 체크리스트

구분	진단 항목
가. 계정 관리	root 계정 원격 접속 금지
	패스워드의 주기적 변경
	기관 보안 정책과 패스워드 정책 일치
	자동 로그인 비활성화
나. 파일 시스템	공유 폴더 제거
	상용 메신저의 사용 금지
다. 패치 관리	안전한 버전의 OS 사용
라. 보안 관리	계정 및 패스워드 파일 소유자 및 권한 설정
	OS에서 제공하는 침입차단 기능 활성화
	화면보호기 대기 시간 설정 및 재시작 시 암호 보호 설정
	비인가 무선랜 사용 금지
	이동식 미디어에 대한 보안 대책 수립

root 계정의 원격 접속 제한

항목설명

root 계정은 운영체제의 모든 기능 설정 및 변경이 가능하며(프로세스, 커널 변경 등) 비인가자가 외부 원격 접속을 통해 root 계정을 탈취할 경우 시스템 장악, 중요 데이터의 위·변조, 정보 유출 등 침해사고가 발생할 수 있다.

진단 기준

양호

원격 터미널 서비스를 사용하지 않거나, 사용 시 root 직접 접속을 차단한 경우

취약

원격 터미널 서비스 사용 시 root 직접 접속을 허용한 경우

진단 방법

■ root 접속 가능 여부 확인 (SSH 사용 시)

- /etc/ssh/sshd_config 파일 내 PermitRootLogin 설정 확인

■ root 접속 가능 여부 확인 (Telnet 사용 시)

- /etc/securetty 파일 내 pts/0 ~ pts/x 설정 확인

조치 방법

■ root 접속 차단 (SSH 사용 시)

- vi 편집기를 이용하여 /etc/ssh/sshd_config 파일 열기
- PermitRootLogin No로 변경

■ root 접속 차단 (Telnet 사용 시)

- “/etc/securetty” 파일에서 pts/0 ~ pts/x 설정 제거 또는 주석 처리
- “/etc/pam.d/login” 파일 내 auth required /lib/security/pam_securetty.so 삽입 또는 주석 제거 (파일이 없다면 생성해야 함)

비고

■ SSH를 사용하는 경우 PermitRootLogin No 설정 앞에 주석(#)이 제거되어 있어야 함

패스워드의 주기적 변경

항목설명

패스워드 최대 사용 기간을 설정하지 않은 경우 비인가자가 각종 공격(무작위 대입 공격, 사전 대입 공격 등)을 장기적으로 시도할 수 있으며, 패스워드 변경 주기에 비례하여 패스워드 유출 확률이 증가할 수 있다.

진단 기준

양호

패스워드 최대 사용 기간이 90일(12주) 이하로 설정되어 있는 경우

취약

패스워드 최대 사용 기간이 90일(12주) 이하로 설정되어 있지 않은 경우

진단 방법

■ 패스워드 최대 사용 기간 설정 확인

- /etc/login.defs 파일 내 PASS_MAX_DAYS 설정 확인

■ 각 계정별 패스워드 최대 사용 기간 설정 확인

- chage –l [계정명] | grep –i maximum

조치 방법

■ 패스워드 최대 사용 기간 90일로 설정

- vi 편집기를 이용하여 /etc/login.defs 파일 열기
- PASS_MAX_DAYS 90 (단위: 일) 삽입

■ 각 계정별 패스워드 최대 사용 기간 90일로 설정

- chage –E –I –M 90 [계정명]

비고

/etc/login.defs 설정을 변경할 경우, 변경 시점 이후부터 생성되는 계정에만 적용됨

기관 보안 정책과 패스워드 정책 일치

항목설명

패스워드 복잡도 설정을 점검하여 해당 기관의 보안 정책에 적합하게 패스워드 정책이 설정되어 있는지 확인하고, 비인가자의 패스워드 추측 공격(무작위 대입 공격, 사전 대입 공격 등)에 대한 대비가 되어있는지 확인한다.

진단 기준

양호

기관 정책에 맞게 패스워드 복잡도 설정이 적용되어 있는 경우

취약

기관 정책에 맞게 패스워드 복잡도 설정이 적용되어 있지 않은 경우

진단 방법

■ 비밀번호 복잡도 설정 확인

- cat /etc/pam.d/common-password (또는 /etc/security/pwquality.conf)

조치 방법

■ 비밀번호 복잡도 설정 정책 적용

- /etc/pam.d/common-password (또는 /etc/security/pwquality.conf) 파일에서 아래와 같이 설정

vi /etc/pam.d/common-password

```
password requisite pam_pwquality.so
enforce_for_root retry=3 minlen=8 lcredit=-1
ucredit=-1 dcredit=-1 ocredit=-1
```

■ RHEL 계열의 경우 /etc/pam.d/system-auth 파일에도 복잡도 설정이 가능하며 위 파일에 enforce_for_root 설정 적용 필요

비고

■ lcredit : 포함되어야 할 알파벳 소문자의 수('-' 로 입력하면 최소)
■ ucredit : 포함되어야 할 알파벳 대문자의 수('-' 로 입력하면 최소)
■ dcredit : 포함되어야 할 숫자 수('-' 로 입력하면 최소)
■ ocredit : 포함되어야 할 특수문자 수('-' 로 입력하면 최소)
■ minclass : 각기 다른 문자의 조합 수(4로 설정한 경우 숫자, 대·소문자, 특수문자 모두 포함되어야 함)
■ enforce_for_root: root 계정 또한 정책 적용

※ 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

자동 로그인 비활성화

항목설명

자동 로그인 기능이 활성화되어 있을 경우, 침입자가 해킹 도구를 이용하여 저장된 로그인 계정 및 패스워드 정보 유출이 가능하다.

진단 기준

양호
자동 로그인 설정이 되어있지 않은 경우

취약
자동 로그인 설정이 적용되어 있는 경우

진단 방법

■ 자동 로그인 설정 여부 확인

- /etc/gdm3/custom.conf 파일 내 AutomaticLoginEnable 값 확인
- 설정 → 사용자 → 자동 로그인 설정 확인

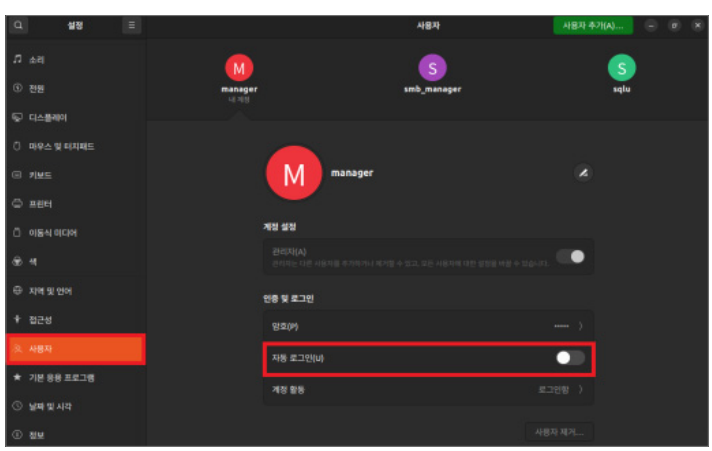
조치 방법

■ 자동 로그인 비활성화 설정

CLI 설정
- /etc/gdm3/custom.conf 파일 내 AutomaticLoginEnable 값 False 또는 주석 처리

```
[daemon]
# Uncomment the line below to force the login screen to use Xorg
#WaylandEnable=false

# Enabling automatic login
#  AutomaticLoginEnable = true
#  AutomaticLogin = user1

# Enabling timed login
#  TimedLoginEnable = true
#  TimedLogin = user1
#  TimedLoginDelay = 10
```

GUI 설정
- 설정 → 사용자 → 자동 로그인 체크 해제



공유 폴더 제거

항목설명

불필요한 공유 폴더를 제거하지 않고 사용하는 경우 익명의 사용자에 의한 공유 폴더의 내부 정보 유출 및 악성코드 감염 위험이 존재한다.

진단 기준

양호
공유 폴더를 사용하고 있지 않은 경우

취약
불필요한 공유 폴더를 사용하고 있는 경우

진단 방법

■ 공유 폴더 존재 여부 확인

- ps –ef | egrep –i “smbd|nfsd” 입력 후 공유 폴더 확인

■ 공유 폴더 존재하고 있는 경우

- net usershare info —long 입력 후 공유 폴더 권한 확인

조치 방법

■ 공유 폴더가 불필요한 경우 (NFS 서비스 사용 시)

- systemctl stop nfs-kernel-server
- systemctl disable nfs-kernel-server

■ 공유 폴더를 사용하지 않는 경우 (Samba 서비스 사용 시)

- systemctl stop smbd
- systemctl disable smbd

■ Linux Mint, Ubuntu에서 제공하는 공유 기능 이용 시

- 공유 디렉터리 속성 → 공유 “다른 사용자가 이 폴더에 파일을 생성하거나 지우는 것을 허용”, “게스트 접속 허용” 설정 체크 해제

■ Samba 서비스 이용 시

vi /etc/samba/smb.conf
- 공유 디렉터리에 ID 지정 및 guest ok = No 설정

■ NFS 서비스 사용 시

vi /etc/exports (예시)
- /data 172.27.0.0/16(rw,no_root_squash)

비고

■ service 명령어를 사용하는 경우

- service nfs-kernel-server(smbd) stop
- service nfs-kernel-server(smbd) disable

상용 메신저의 사용 금지

항목설명

일반 사용자 PC에서 메신저 차단을 하지 않을 경우 메신저를 통해 주요 정보가 유출되거나, 악성코드가 유입될 가능성이 있다.

진단 기준

양호

상용 메신저를 사용하고 있지 않은 경우

취약

상용 메신저를 사용하고 있는 경우

진단 방법

■ 시스템 테이블에 접근할 수 있는 일반 사용자 출력

– ps –ef | egrep –i “kakao|nate|telegram” | grep –v grep

※ 상용 메신저: 카카오톡, Line, 텔레그램, 위챗 등)

조치 방법

■ 상용 메신저 삭제

안전한 버전의 OS 사용

항목설명

주기적인 패치 적용을 통해 보안성 및 시스템 안정성을 확보하는 것이 시스템 운용의 중요한 요소이다. 서비스 중인 시스템의 경우 패치 적용에 따르는 문제점(현재 운용 중인 응용프로그램의 예기치 않은 중지, 패치 자체의 버그 등)과 재부팅의 어려움 등으로 많은 패치를 적용하는 것이 매우 어렵기 때문에 패치 적용 시 많은 부분을 고려해야 한다.

진단 기준

양호

안전한 버전의 패치를 적용하고 있는 경우

취약

안전한 버전의 패치를 적용하고 있지 않은 경우

진단 방법

■ 버전 확인

- lsb_release –a
- uname –r

조치 방법

■ 버전 패치

- OS 관리자, 서비스 개발자가 패치 적용에 따른 서비스 영향도를 파악하여 최신 패치를 OS 관리자 및 벤더에서 적용 시스템의 보안성 및 안전성을 위하여 패치 적용 정책을 수립하여 주기적으로 패치를 적용하는 것이 바람직함.
- 단, 아래의 사항을 고려하여 OS벤더 엔지니어의 충분한 검토 후, 서버에서 운용 중인 서비스에 아무런 영향이 없다고 판단될 때 패치를 적용해야 함

NO	패치 적용 시 고려 및 준수해야 할 사항
1	해당 패치가 시스템 자체에 미칠 수 있는 영향을 OS벤더 측에서 검토 후, 이상이 없을 때 패치를 적용해야 함
2	해당 패치가 시스템에서 운용 중인 서비스 프로그램에 미칠 수 있는 영향을 OS벤더 측과 서비스 프로그램(즉 응용프로그램) 개발자 측과 함께 검토 후, 이상이 없을 때 패치를 적용해야 함
3	패치 적용 후 예기치 않은 서비스의 중지에 대비하여, 패치 작업을 실시하기 전에 Roll-Back 및 비상복구절차를 수립 및 테스트해야 함
4	패치 적용 전/후 시스템에 대한 Full Backup을 실시해야 함

계정 및 패스워드 파일 소유자 및 권한 설정

항목설명

/etc/passwd 파일은 사용자의 ID, 패스워드(보안상 'x'로 표시), UID, GID, 홈 디렉토리, shell 정보를 담고 있는 중요 파일로, 이 파일이 노출되면 보안상 심각한 문제를 발생할 수 있어 관리자 이외의 사용자는 접근 제한이 필요하다.
/etc/shadow 파일은 암호화된 패스워드와 패스워드 설정 정책을 담고 있는 중요 파일로 이 파일이 노출되면 보안상 심각한 문제를 발생할 수 있어 소유자 외의 사용자는 접근 제한이 필요하다.

진단 기준

양호
불필요한 일반 사용자의 쓰기 권한이 부여되어 있지 않고, 소유자가 root인 경우

취약
불필요한 일반 사용자의 쓰기 권한이 부여되어 있지 않고, 소유자가 root가 아닌 경우

진단 방법

■ 계정 및 패스워드 파일 설정 확인

- ls –l /etc/passwd
- ls –l /etc/shadow

조치 방법

■ 계정 및 패스워드 파일 권한 변경

- chmod 644 /etc/passwd
- chmod 400 /etc/shadow

■ 소유자를 root로 변경

- chown root /etc/passwd
- chown root /etc/shadow

OS에서 제공하는 침입차단 기능 활성화

항목설명

침입차단 기능인 방화벽을 사용함으로써 PC의 자료 유출 방지, 불법 접근 차단 등을 가능하게 한다. 네트워크 방화벽과 더불어 각각의 PC에 OS 방화벽과 같은 호스트 기반의 방화벽을 구현할 때 네트워크의 방어 수준이 향상될 수 있다.

진단 기준

양호

OS에서 제공하는 방화벽을 사용하고 있는 경우

취약

OS에서 제공하는 방화벽을 사용하고 있지 않은 경우

진단 방법

■ OS에서 제공하는 방화벽 활성화 여부 확인

- ufw status

조치 방법

■ OS에서 제공하는 방화벽 활성화
(방화벽 활성화 시, 모든 포트 차단되므로 별도 접근 설정 필요)

- ufw enable

■ 접근 허용 Rule 설정

- ufw allow [허용 포트]

■ 접근 차단 Rule 설정

- ufw deny [차단 포트]

화면보호기 대기 시간 설정 및 재시작 시 암호 보호 설정

항목설명

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 있다.

진단 기준

양호

화면보호기 설정(대기 시간 10분 이하) 및 암호로 보호가 설정되어 있는 경우

취약

화면보호기 설정(대기 시간 10분 초과) 및 암호로 보호가 설정되어 있지 않은 경우

진단 방법

■ 화면보호기 설정 여부 확인

- Setting → Privacy → Screen Lock 설정값 확인

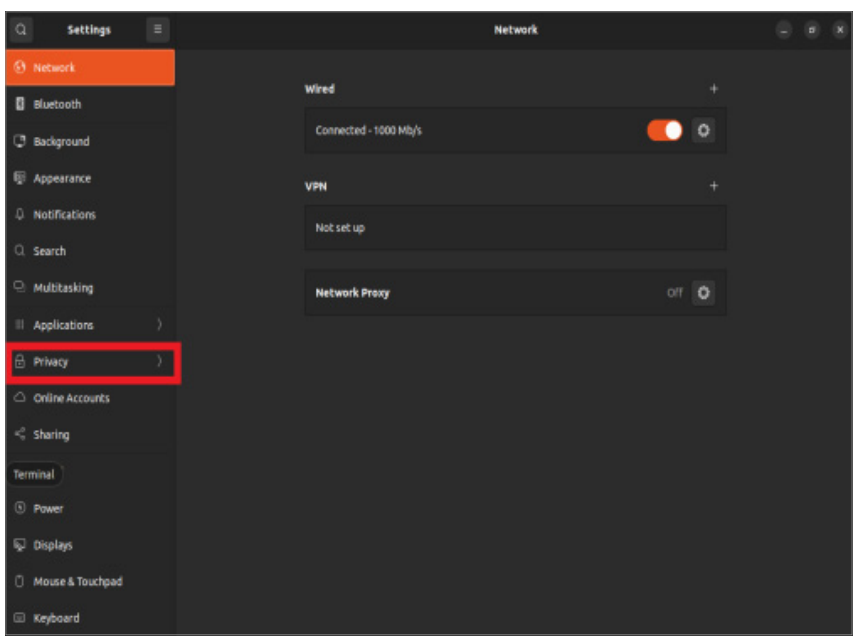
조치 방법

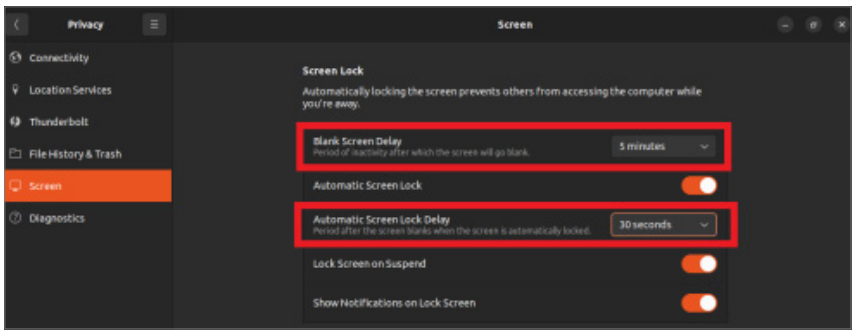
■ 화면보호기 설정

- Setting → Privacy → Screen Lock → 화면보호기 설정

■ Black Screen Delay, Automatic Screen Lock Delay 설정

- 모두 시간 설정, 총 10분 이하





비고

※ Black Screen Delay: 빈 화면 지연 시간
※ Automatic Screen Lock Delay: 자동 화면 잠금 지연 시간

비인가 무선랜 사용 금지

항목설명

내부에 설치된 비인가 AP 또는 사용자의 잘못된 설정으로 인한 Ad-Hoc 네트워크가 기업 네트워크의 백도어 역할을 하여 해당 위협요소를 통해 불법 침입자가 내부 네트워크로 접근할 수 있다. 공공장소 무선 AP의 경우 해킹이나 관리자 계정의 중요성을 알지 못하거나, 손님 편의를 위해 패스워드를 공개하고, 번거롭다는 이유로 보안에 취약한 펌웨어 업데이트를 하지 않는 등 다양한 보안 위협요소가 존재한다.

진단 기준

양호
비인가 무선랜을 사용하고 있지 않은 경우

취약
비인가 무선랜을 사용하고 있는 경우

진단 방법

■ CLI 환경 무선랜 접속 이력 확인
- ls -l /etc/NetworkManager/system-connections

■ GUI 환경 무선랜 접속 이력 확인
- Setting → WIFI 설정

조치 방법

■ 무선랜 사용 중지
■ 비인가 무선랜 사용 기록 삭제
■ 무선랜 드라이버 제거

이동식 미디어에 대한 보안 대책 수립

항목설명

CD/DVD, USB 메모리 등과 같은 미디어에 탑재된 파일을 통해 다른 응용프로그램이 자동 실행될 수 있다. 대부분의 USB 관련 악성코드들은 자동 실행되도록 제작되므로 이를 통해 악성코드가 PC로 쉽게 유입될 가능성이 존재한다.

진단 기준

양호

이동식 미디어 사용 시 자동 실행되지 않는 경우

취약

이동식 미디어 사용 시 자동 실행되는 경우

진단 방법

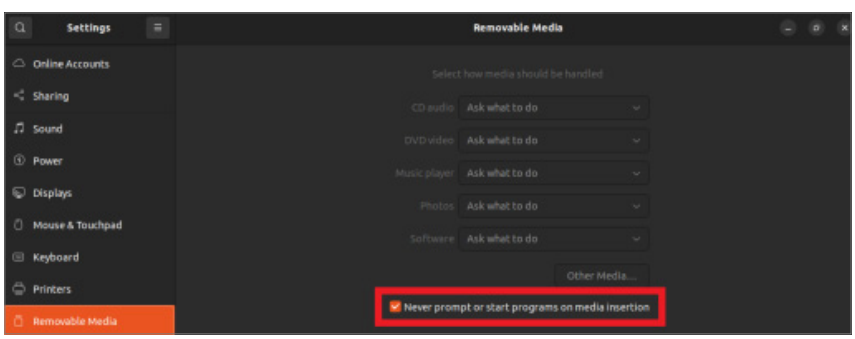
■ 이동식 미디어 자동실행 설정 확인

- Setting → 이동식 미디어
- gsettings get org.gnome.desktop.media-handling autorun-never

조치 방법

■ 이동식 미디어 자동실행 방지 설정

- Setting → 이동식 미디어 → 미디어가 연결되어도 물어보거나 프로그램 시작하지 않기 설정



2.10.

MY-SQL

2.10. MY-SQL

계정 관리(4개 항목), 보안 설정(3개 항목), 패치 및 로그 관리(2개 항목) 총 3개 영역에서 9개 항목으로 구성된다.

[표 10] MYSQL 진단 체크리스트

구분	진단 항목
가. 계정 관리	불필요한 계정 제거
	취약한 패스워드 사용 제한
	타 사용자에 권한 부여 옵션 제한
	DB 사용자 계정 정보 테이블 접근 권한
나. 보안 설정	root 권한으로 서버 구동 제한
	환경설정 파일 접근 권한
	안전한 패스워드 암호화 알고리즘 사용
라. 패치 및 로그 관리	로그 활성화
	최신 보안 패치 적용

불필요한 계정 제거

항목설명

데이터베이스의 계정 중 인가되지 않은 계정, 퇴직자 계정, 테스트 계정 등 업무에 사용하지 않는 불필요한 계정이 있는 경우 비인가자가 쉽게 데이터베이스에 접속하여 데이터를 열람, 삭제, 수정 등을 할 위험이 있다. 또한 DB 접속 시 지정된 IP주소만 접근 가능하도록 설정되어 있는지 확인하여 비인가자의 DB 접근을 제한해야 한다.

진단 기준

양호

DB 설치 시 Default로 생성된 계정 및 테스트 계정, 의심스러운 계정, 불필요한 계정이 없는 경우

취약

DB 설치 시 Default로 생성되는 계정 및 테스트 계정, 의심스러운 계정, 불필요한 계정이 있는 경우

진단 방법

■ 사용자 계정 목록 조회

1) mysql〉 USE mysql;

2) mysql〉 SELECT host, user, authentication_string FROM user;

```
mysql> SELECT host, user, authentication_string FROM user;
+-----------+------------------+-------------------------------------------------------------------------+
| host      | user             | authentication_string                                                   |
+-----------+------------------+-------------------------------------------------------------------------+
| localhost | TEST             | *FE05E6547C26C426BE73C86246FEB4C9638679A1                               |
| localhost | debian-sys-maint | $A$005$p%<bL)H f`&AQW
Q.JjwLnzgwkAehMvQXgJJ6sxiFkxRN/WEbSivJDYhQD |
| localhost | mysql.infoschema | $A$005$THISISACOMBINATIONOFINVALIDSALTANDPASSWORDTHATMUSTNEVERBRBEUSED |
| localhost | mysql.session    | $A$005$THISISACOMBINATIONOFINVALIDSALTANDPASSWORDTHATMUSTNEVERBRBEUSED |
| localhost | mysql.sys        | $A$005$THISISACOMBINATIONOFINVALIDSALTANDPASSWORDTHATMUSTNEVERBRBEUSED |
| localhost | root             |                                                                         |
+-----------+------------------+-------------------------------------------------------------------------+
6 rows in set (0.00 sec)

mysql>
```

조치 방법

■ 불필요한 계정 삭제

1) mysql〉 DELETE FROM user WHERE user='삭제할 계정명';

취약한 패스워드 사용 제한

항목설명

패스워드가 계정명과 동일하거나 Default 패스워드를 사용하는 경우 비인가자가 쉽게 데이터베이스에 접근할 위험이 있고 접근 시, 데이터베이스 삭제, 변경 등의 심각한 침해 사고를 일으킬 가능성이 있다.

진단 기준

양호

패스워드 복잡도 설정을 적용하고 있는 경우

취약

패스워드 복잡도 설정을 적용하고 있지 않은 경우

진단 방법

■ validate_password 패스워드 컴포넌트 활성화 및 복잡도 설정 확인

1) mysql> INSTALL COMPONENT 'file://component_validate_password';

2) mysql> SHOW VARIABLES LIKE 'validate_password%';

```
mysql>
mysql> SHOW VARIABLES LIKE 'validate_password%';
+--------------------------------------------------+---------+
| Variable_name                                    | Value   |
+--------------------------------------------------+---------+
| validate_password.changed_characters_percentage  | 0       |
| validate_password.check_user_name                | ON      |
| validate_password.dictionary_file                |         |
| validate_password.length                         | 8       |
| validate_password.mixed_case_count               | 1       |
| validate_password.number_count                   | 1       |
| validate_password.policy                         | MEDIUM  |
| validate_password.special_char_count             | 1       |
+--------------------------------------------------+---------+
8 rows in set (0.02 sec)

mysql>
```

※ validate_password.policy가 MEDIUM 또는 STRONG으로 설정되어 있으면 양호

조치 방법

■ validate_password 패스워드 정책 (예시)

1) mysql server configuration 파일에서 아래의 내용으로 수정

```
# vi /etc/mysql/mysql.conf.d/mysqld.cnf
  validate_password.length=8
  validate_password.mixed_case_count=1
  validate_password.number_count=1
  validate_password.special_char_count=1
  validate_password.policy=MEDIUM 또는 STRONG
```

2) # service mysql restart

3) mysql> SHOW VARIABLES LIKE 'validate_password%';

비고

※ validate password 플러그인은 mysql v5.6 이상에서 제공

패스워드 정책	
LOW	8자리 이상
MEDIUM	영문자, 숫자, 특수문자 조합 8자리 이상
STRONG	MEDIUM 정책 + dictionary 파일(금칙어)

타 사용자에 권한 부여 옵션 제한

항목설명

WITH GRANT OPTION과 함께 권한을 받은 사용자는 해당 권한을 다른 사용자에게 부여할 수 있다. 그러므로 다른 Object의 사용 권한 부여는 DBA만 할 수 있도록 제한해야 한다.

진단 기준

양호

grant_priv 권한이 적절한 사용자에게만 부여되어 있는 경우

취약

grant_priv 권한이 적절하지 않은 사용자에게 부여되어 있는 경우

진단 방법

■ grant_priv 권한을 부여 받은 사용자 조회

1) mysql〉 USE mysql;

2) mysql〉 SELECT host, user, Grant_priv FROM user WHERE Grant_priv='Y';

```
mysql> SELECT host, user, Grant_priv FROM user WHERE Grant_priv='Y';
+-----------+------------------+------------+
| host      | user             | Grant_priv |
+-----------+------------------+------------+
| localhost | debian-sys-maint | Y          |
| localhost | root             | Y          |
+-----------+------------------+------------+
2 rows in set (0.00 sec)

mysql>
mysql>
```

조치 방법

■ 불필요한 grant_priv 권한 제거

1) mysql〉 USE mysql;

2) mysql〉 REVOKE grant option ON *.* FROM '권한 제거 사용자 계정명'@'접속 IP';

3) mysql〉 FLUSH privileges;

사용자 계정 정보 테이블 접근 권한

항목설명

일반 사용자의 mysql.user 테이블 접근이 허용될 경우, 일반 사용자가 DB에 등록되어 있는 사용자 계정 및 패스워드를 알 수 있게 된다. 따라서 적절한 사용자에게만 user 테이블에 접근할 수 있도록 제한해야 한다.

진단 기준

양호

DB사용자 계정 정보 테이블의 접근 권한이 적절한 사용자에게 부여되어 있는 경우

취약

DB사용자 계정 정보 테이블의 접근 권한이 적절한 사용자에게 부여되어 있지 않은 경우

진단 방법

■ mysql.user 테이블 접근이 가능한 사용자 계정 조회

1) mysql〉 SELECT host, user, select_priv FROM mysql.user;

```
mysql>
mysql> SELECT host, user, select_priv FROM mysql.user;
+-----------+------------------+-------------+
| host      | user             | select_priv |
+-----------+------------------+-------------+
| localhost | TEST             | Y           |
| localhost | debian-sys-maint | Y           |
| localhost | mysql.infoschema | Y           |
| localhost | mysql.session    | N           |
| localhost | mysql.sys        | N           |
| localhost | root             | Y           |
+-----------+------------------+-------------+
6 rows in set (0.01 sec)

mysql>
mysql>
```

조치 방법

■ 일반 사용자 계정으로부터 mysql.user 테이블의 모든 권한 제거

1) mysql〉 REVOKE all ON *.* FROM '사용자 계정명'@'접속 IP';

2) mysql〉 FLUSH prvileges;

root 권한으로 서버 구동 제한

항목설명

root 권한은 데이터베이스 최고 상위 권한으로 소수의 관리자만이 제한적으로 사용되어야 한다.

진단 기준

양호

DBMS가 root 계정 또는 root 권한으로 구동되고 있지 않은 경우

취약

DBMS가 root 계정 또는 root 권한으로 구동되고 있을 경우

진단 방법

■ 실행 중인 프로세스를 통해 확인

1) # ps –ef | grep mysqld

```
root@ubuntu:~# ps -ef | grep mysqld
mysql       17783       1  2 14:05 ?        00:00:03 /usr/sbin/mysqld
root        17835   17755  0 14:06 pts/0    00:00:00 grep --color=auto mysqld
root@ubuntu:~#
```

■ mysql server configuration 파일에서 [mysqld] 그룹의 'user' 지시자의 설정값 확인

1) # cat [mysql server configuration 파일 위치] | grep user

```
root@ubuntu:/etc/mysql/mysql.conf.d# cat /etc/mysql/mysql.conf.d/mysqld.cnf | grep user
user            = mysql
```

※ user = mysql로 설정되어 있으면 양호

조치 방법

■ mysql server configuration 파일에서 [mysqld] 그룹의 'user' 지시자 설정

1) # vi [mysql server configuration 파일 위치]

2) user = 〈mysqld를 구동할 시스템의 일반 사용자 계정〉

```
[mysqld]
#
# * Basic Settings
#
user            = mysql
# pid-file      = /var/run/mysqld/mysqld.pid
# socket        = /var/run/mysqld/mysqld.sock
 port           = 3306
# datadir       = /var/lib/mysql
```

환경설정 파일 접근 권한

항목설명

MySQL 데이터 베이스의 주요 파일 중에 하나인 환경설정 파일에 비인가자가 접근하여 수정 및 삭제를 한다면 데이터베이스 운영에 장애가 발생할 수 있으며 계정 패스워드 정보 등의 중요한 정보가 유출될 수 있다.

진단 기준

양호

환경설정 파일의 접근 권한이
640(-rw-r-----) 이하이면 양호

취약

환경설정 파일의 접근 권한이
640(-rw-r-----) 초과이면 양호

진단 방법

■ mysql server configuration 파일의 접근 권한 확인 (my.cnf 또는 mysqld.cnf)

1) # ls –alL [mysql server configuration 파일 위치]

```
root@ubuntu:/# ls -alL /etc/mysql/mysql.conf.d/mysqld.cnf
-rw-r--r-- 1 root root 2249 11월   7 10:20 /etc/mysql/mysql.conf.d/mysqld.cnf
root@ubuntu:/#
```

조치 방법

■ mysql server configuration 파일 접근 권한 변경

1) # chmod 640 [mysql server configuration 파일 위치]

```
root@ubuntu:/# chmod 640 /etc/mysql/mysql.conf.d/mysqld.cnf
root@ubuntu:/#
root@ubuntu:/# ls -alL /etc/mysql/mysql.conf.d/mysqld.cnf
-rw-r----- 1 root root 2249 11월   7 10:20 /etc/mysql/mysql.conf.d/mysqld.cnf
root@ubuntu:/#
root@ubuntu:/#
```

안전한 암호화 알고리즘 사용

항목설명

SHA-1의 취약점이 발견됨에 따라 SHA-1은 더 이상 안전한 암호화 알고리즘이 아니다. 따라서 SHA-256 이상의 암호화 알고리즘을 사용해야 한다.

진단 기준

양호

해시 알고리즘 SHA-256 이상의 암호화 알고리즘을 사용하고 있는 경우

취약

해시 알고리즘 SHA-256 미만의 암호화 알고리즘을 사용하고 있는 경우

진단 방법

■ 안전한 패스워드 암호화 알고리즘 사용

1) mysql〉 SELECT host, user, plugin, authentication_string FROM user;

조치 방법

■ 안전한 패스워드 암호화 알고리즘 사용

1) mysql〉 ALTER user '사용자 계정 이름'@'localhost' IDENTIFIED WITH caching_sha2_password BY '패스워드';

2) mysql〉 FLUSH privileges;

```
mysql> ALTER user 'TEST'@'localhost' IDENTIFIED WITH caching_sha2_password BY 'Test123!@#';
Query OK, 0 rows affected (0.01 sec)
```

비고

※ mysql v8.0 이상부터 암호화 알고리즘으로 caching_sha2_password(SHA-256)가 적용됨

로그 활성화

항목설명

로그 기능을 수행할 수 있게 설정함으로써 사용자에 의한 문장에 대한 감사, 권한에 대한 감사, 객체에 대한 감사를 수행할 수 있다. 또한 침해 사고 및 장애 시 로그 자료를 분석하여 정확한 분석을 할 수 있다.

진단 기준

양호

로그 기능이 활성화되어 있는 경우

취약

로그 기능이 비활성화되어 있는 경우

진단 방법

■ General log 설정 확인

1) mysql> SHOW VARIABLES LIKE 'general_log%';

■ Slow log 설정 확인

1) mysql> SHOW VARIABLES LIKE 'slow%';

조치 방법

■ General log 설정

1) # vi [mysql server configuration 파일]
general_log = 1;

2) # vi [mysql server configuration 파일]
general_log_file 경로 설정

■ Slow log 설정

1) # vi [mysql server configuration 파일]
slow_query_log = 1;

2) # vi [mysql server configuration 파일]
slow_launch_time 설정

3) # vi [mysql server configuration 파일]
slow_query_log_file 경로 설정

비고

※ general_log가 비활성화되어 있으나 slow_query_log가 활성화되어 있으면 양호로 처리

최신 보안 패치 적용

항목설명

데이터베이스의 주요 보안 패치 등을 설치하지 않은 경우, 버그 또는 알려진 취약점으로 인한 침해 사고가 발생할 수 있고 취약점을 이용하여 데이터베이스에 접근할 수 있다. 따라서 최신 보안패치 버전을 적용하여 데이터베이스의 보안성을 높여야 한다.

진단 기준

양호

최신 보안패치 버전이 적용되어 있으면 양호

취약

최신 보안패치 버전이 적용되어 있지 않으면 취약

진단 방법

■ MySQL 버전 확인 후 최신 보안패치 버전 적용 여부 확인

1) mysql〉 use mysql;

2) mysql〉 SELECT @@VERSION;

```
mysql> SELECT @@VERSION;
+-------------------------+
| @@VERSION               |
+-------------------------+
| 8.0.35-0ubuntu0.22.04.1 |
+-------------------------+
1 row in set (0.00 sec)
```

3) # dpkg –l | grep –i mysql–server

4) # rpm –qa | grep –i mysql

조치 방법

■ 데이터베이스에 대한 최신 보안 패치 버전으로 업그레이드 및 패치 수행

버그 패치 릴리즈 사이트 : http://downloads.mysql.com/archives/
버그 현황 사이트 : http://bugs.mysql.com/bugstats.php

※ 최신 버전을 사용하도록 권고하고 있으나 시스템 운영상 적용이 어려운 경우 최신이 아닌 취약점이 존재하지 않는 버전도 허용하고 있음

비고

※ 보안 패치를 적용할 경우, 시스템 영향도를 파악하여 충분한 테스트 후 적용 권고

2.11.

MS-SQL

2.11. MS-SQL

계정 관리(4개 항목), 보안 설정(2개 항목), 패치 및 로그 관리(2개 항목) 총 3개 영역에서 8개 항목으로 구성된다.

[표 11] MS-SQL 진단 체크리스트

구분	진단 항목
가. 계정 관리	불필요한 계정 제거
	SYSADMIN 권한 제한
	SA 계정 패스워드 관리
	guest 계정 사용 제한
나. 보안 설정	Registry Procedure Permission 제한
	xp_cmdshell 사용 제한
라. 패치 및 로그 관리	로그 활성화
	최신 보안 패치 적용

불필요한 계정 제거

항목설명

데이터베이스의 계정 중 인가되지 않은 계정, 퇴직자 계정, 테스트 계정 등 업무에 사용하지 않는 불필요한 계정이 있는 경우 비인가자가 쉽게 데이터베이스에 접속하여 데이터를 열람, 삭제, 수정 등을 할 위험이 있다. 또한 DB 접속 시 지정된 IP주소만 접근 가능하도록 설정되어 있는지 확인하여 비인가자의 DB 접근을 제한해야 한다.

진단 기준

양호

불필요한 계정이 존재하지 않는 경우

취약

불필요한 계정이 존재하는 경우

진단 방법

■ 새 쿼리를 통해 불필요한 계정 삭제

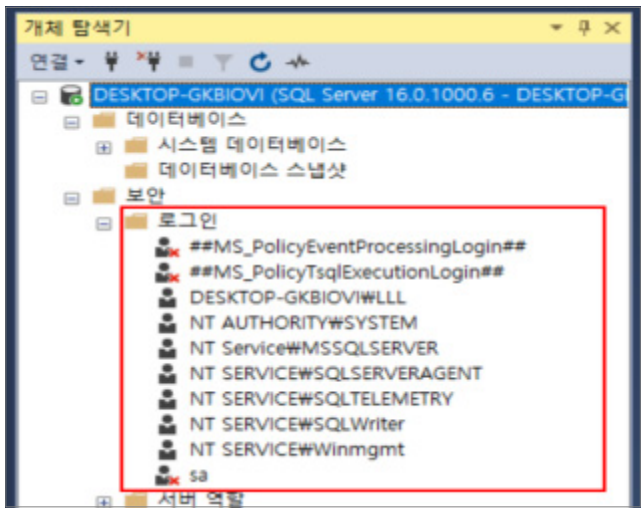
1) Microsoft SQL Server Mnagement Studio → 새 쿼리

2)
```
SELECT log.name AS [Name]
,log.type_desc
,log.is_disabled AS [IsDisabled]
,log.create_date AS [CreateDate]
FROM sys.server_principals AS log
WHERE (
log.type in ('U', 'G', 'S', 'C', 'K')
AND log.principal_id not between 101 and 255
AND log.name <> N'##MS_AgentSigningCertificate##'
) ORDER BY [Name] ASC
```

	Name	type_desc	IsDisabled	CreateDate
1	##MS_PolicyEventProcessingLogin##	SQL_LOGIN	1	2022-10-08 06:32:02.537
2	##MS_PolicyTsqlExecutionLogin##	SQL_LOGIN	1	2022-10-08 06:32:02.543
3	DESKTOP-GKBIOVI₩LLL	WINDOWS_LOGIN	0	2023-12-04 16:50:25.910
4	NT AUTHORITY₩SYSTEM	WINDOWS_LOGIN	0	2023-12-04 16:50:25.937
5	NT Service₩MSSQLSERVER	WINDOWS_LOGIN	0	2023-12-04 16:50:25.930
6	NT SERVICE₩SQLSERVERAGENT	WINDOWS_LOGIN	0	2023-12-04 16:50:26.543
7	NT SERVICE₩SQLTELEMETRY	WINDOWS_LOGIN	0	2023-12-04 16:50:27.460
8	NT SERVICE₩SQLWriter	WINDOWS_LOGIN	0	2023-12-04 16:50:25.920
9	NT SERVICE₩Winmgmt	WINDOWS_LOGIN	0	2023-12-04 16:50:25.927
10	sa	SQL_LOGIN	1	2003-04-08 09:10:35.460

■ 개체 탐색기를 통해 불필요한 계정 삭제

1) SSMS(SQL Server Management Studio) → 개체 탐색기 → 보안 → 로그인



조치 방법

■ 새 쿼리를 통해 불필요한 계정 삭제

1) SQL Server Management Studio → 새 쿼리

2) DROP login “로그인 사용자 계정명“

■ 개체 탐색기를 통해 불필요한 계정 삭제

1) SQL Server Management Studio → 개체 탐색기 → 보안 → 로그인

2) 해당 계정 오른쪽 마우스 → 삭제 → 확인

SYSADMIN 권한 제한

항목설명

sysadmin(시스템 관리자)의 역할은 SQL 서버와 설치된 데이터베이스에 대해서 완전한 관리 권한이 필요한 사용자를 위해 만들어진 역할로 이 역할의 구성원은 SQL 서버에서 모든 작업을 수행할 수 있으며 비인가 사용자 계정에 해당 권한이 부여될 경우, DB에 직접적인 공격이 가능해진다. 따라서 sysadmin 권한 제한 여부를 확인해야 한다.

진단 기준

양호

sysadmin 역할 구성원에 관리자 구성원만 존재하는 경우

취약

sysadmin 역할 구성원에 불필요한 계정이 존재하는 경우

진단 방법

■ 새 쿼리를 통해 확인

1) SQL Server Management Studio → 새 쿼리

2) EXEC sp_helpsrvrolemember 'sysadmin'

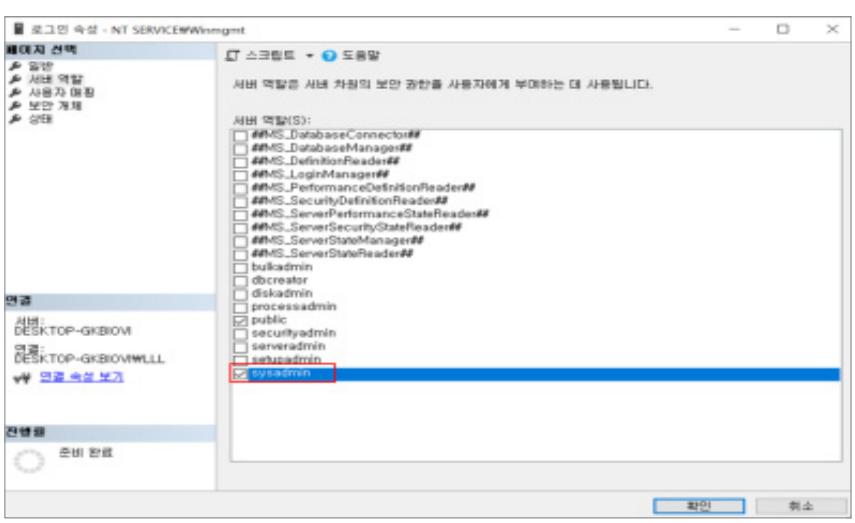
결과 | 메시지

	ServerRole	MemberName	MemberSID
1	sysadmin	sa	0x01
2	sysadmin	DESKTOP-GKBIOVI₩LLL	0x010500000000000515000000CD2728479C267E7EC42339...
3	sysadmin	NT SERVICE₩SQLWriter	0x010600000000000550000000732B9753646EF90356745CB...
4	sysadmin	NT SERVICE₩Winmgmt	0x010600000000000550000000A048DDFF9C7430AB450D4...
5	sysadmin	NT Service₩MSSQLSERVER	0x010600000000000550000000E20F4FE7B15874E48E19026...
6	sysadmin	NT SERVICE₩SQLSERVERAGENT	0x010600000000000550000000DCA88F14B79FD47A992A3D...

■ 개체 탐색기를 통해 확인

1) SQL Server Management Studio → 개체 탐색기 → 보안 → 로그인

2) 계정별 오른쪽 마우스 → 속성 → 서버 역할에서 확인



조치 방법

■ 새 쿼리를 통해 역할 제거

1) SQL Server Management Studio → 새 쿼리

2) EXEC sp_droprolemember '〈구성원 이름〉', 'sysadmin'

■ 개체 탐색기를 통해 역할 제거

1) SQL Server Management Studio → 개체 탐색기 → 보안 → 로그인

2) 계정별 오른쪽 마우스 → 속성 → 서버 역할에서 sysadmin 권한 해제

SA 계정 패스워드 관리

항목설명

MS-SQL 설치 시, sa 계정은 sysadmin 권한을 가지며 디폴트로 생성된다. sa 계정의 패스워드가 설정되어 있지 않다면 악의적인 사용자가 해당 계정을 통해 데이터베이스에 접근하여 데이터를 열람, 삭제, 수정하는 위험이 존재한다. 따라서 sa 계정 패스워드를 설정해야 한다.

진단 기준

양호

sa 계정에 패스워드가 설정된 경우

취약

sa 계정에 패스워드가 설정되어 있지 않은 경우

진단 방법

■ sa 패스워드 설정 확인

1) SQL Server Management Studio → sa 계정으로 로그인

조치 방법

■ 새 쿼리를 통해 변경

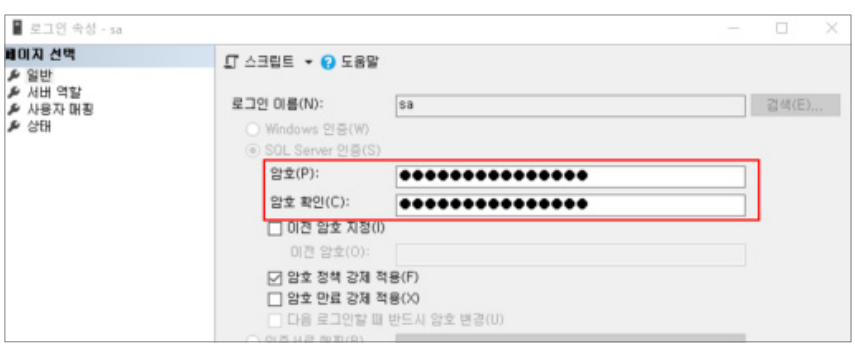
1) SQL Server Management Studio → 새 쿼리

2) ALTER LOGIN sa WITH password='변경할 패스워드';

■ 개체 탐색기를 통해 변경

1) SQL Server Management Studio → 개체 탐색기 → 보안 → 로그인

2) sa 계정 오른쪽 마우스 → 속성 → 일반 → 암호 변경



Guest 계정 사용 제한

항목설명

SQL의 모든 사용자가 접근 가능한 Guest 계정은 기본 설정으로 활성화되어 있으므로 모든 데이터베이스에서 Guest 권한을 제거해야 한다.

진단 기준

양호

데이터베이스에 Guest 계정이 활성화되어 있지 않은 경우

취약

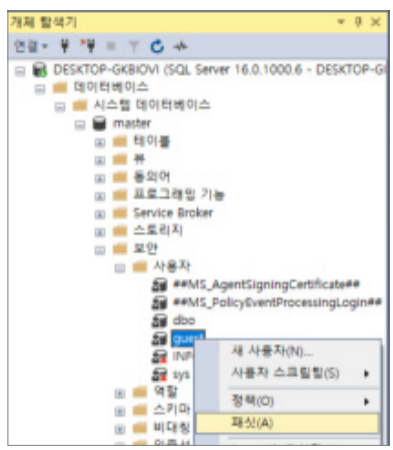
데이터베이스에 Guest 계정이 활성화되어 있는 경우

진단 방법

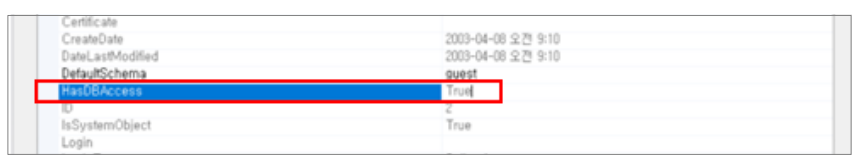
■ 데이터베이스에 부여된 Guest 계정 확인

1) SQL Server Management Studio → 개체 탐색기 → 데이터베이스

2) 데이터베이스 별 → 보안 → 사용자 → guest 계정 오른쪽 마우스 → 패싯



3) 패싯 속성에서 DasDBAccess 설정 값



※ master, tempdb 데이터베이스에 Guest 계정이 디폴트로 활성화되어 있으며 삭제가 불가능함 (Microsoft SQL Server 2022 기준)

조치 방법

■ 데이터베이스에 존재하는 Guest 계정 비활성화

1) SQL Server Management Studio → 새 쿼리

2) USE [해당 데이터베이스]

3) REVOKE connect FROM guest;

Regisrtry Procedure Permission 제한

항목설명

레지스트리 확장 저장 프로시저를 이용하면 Windows 레지스트리에 액세스할 수 있다. 레지스트리에는 SQL에 대한 구성 정보가 들어있으며 원격 또는 로컬 시스템에 대한 암호가 포함되어 있을 수 있으므로 악의적인 사용자가 windows 레지스트리를 이용하여 서버 및 데이터베이스에 손상 및 비 인가된 접근을 할 위험이 존재한다. 따라서 시스템 확장 저장 프로시저 제한 목록의 프로시저를 제한해야 한다.

진단 기준

양호

제한이 필요한 시스템 확장 저장 프로시저들이 DBA 외 guest/public에게 부여되어 있지 않은 경우

취약

제한이 필요한 시스템 확장 저장 프로시저들이 DBA 외 guest/public에게 부여되어 있는 경우

진단 방법

■ 새 쿼리를 통해 프로시저 확인

1) SQL Server Management Studio → 새쿼리

2) SELECT object_name(id) AS sp, user_name(id) AS grantee, user_name(grantor) AS 'Granted by' FROM sysprotects WHERE object_name(id) LIKE '%xp_reg%'

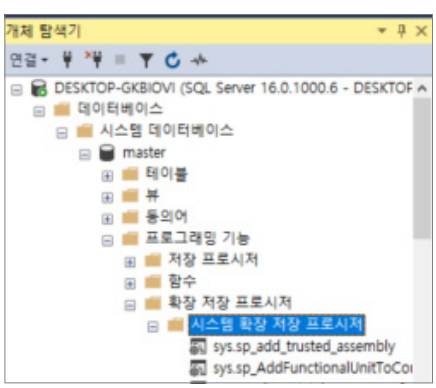
결과 메시지

	sp	grantee	Granted by
1	xp_regread	NULL	dbo

■ 개체 탐색기를 통해 프로시저 확인

1) SQL Server Management Studio → 개체 탐색기 → 데이터베이스

2) 시스템 데이터베이스 → master → 프로그래밍 기능 → 확장 저장 프로시저 → 시스템 확장 저장 프로시저



3) 아래 *비고) 시스템 확장 저장 프로시저 제한 목록의 프로시저 별 → 마우스 우클릭 → 속성 → 사용 권한

4) 사용 권한에 public 실행 권한 확인

조치 방법

■ 새 쿼리를 통해 프로시저 제한

1) SQL Server Management Studio → 새쿼리

2) USE master;

3) REVOKE 〈권한〉 ON object :: 〈시스템 확자 저장 프로시저명〉 TO public;

■ 개체 탐색기를 통해 프로시저 제한

1) SQL Server Management Studio → 개체 탐색기 → 데이터베이스

2) 시스템 데이터베이스 → master → 프로그래밍 기능 → 확장 저장 프로시저 → 시스템 확장 저장 프로시저

3) 아래 *비고) 시스템 확장 저장 프로시저 제한 목록의 프로시저 별 → 마우스 우클릭 → 속성

4) 사용 권한 → public 실행 권한 제거

비고

시스템 확장 저장 프로시저 제한		
sys.xp_readdmultistring	sys.xp_redeletekey	sys.xp_regdeletevalue
sys.xp_regenumvalues	sys.xp_regread	sys.xp_regremovemultistring
sys.xp_regwrite		

xp_cmdshell 사용 제한

항목설명

MS-SQL이 제공 중인 확장 프로시저 중에 서버의 유지 관리 목적으로 사용되고 있는 확장 프로시저들이 해킹 툴에서 자주 이용되고 있으며 특히 중국에서 제작된 해킹 툴에서 자주 이용되고 있으므로 불필요한 경우 반드시 제거해야 한다.

진단 기준

양호

xp_cmdshell이 제한되어 있는 경우

취약

xp_cmdshell이 제한되어 있지 않은 경우

진단 방법

■ 새 쿼리를 통해 프로시저 확인

1) SQL Server Management Studio → 새쿼리

2) SELECT name, value FROM sys.configurations WHERE name = 'xp_cmdshell';

결과 메시지

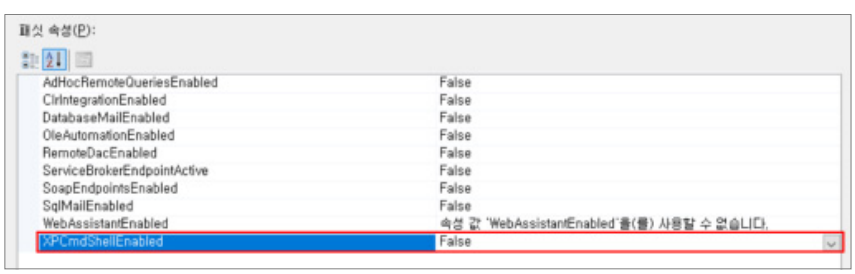
	name	value
1	xp_cmdshell	0

※ xp_cmdshell 값이 0(false)일 경우 양호

■ 개체 탐색기를 통해 프로시저 확인

1) SQL Server Management Studio → 개체 탐색기 → 컴퓨터 이름 → 오른쪽 마우스 → 패싯 → 일반

2) XPCmdShellEnabled 값 확인



※ XPCmdShellEnable 값이 false일 경우 양호

조치 방법

■ 새 쿼리를 통해 프로시저 확인

1) SQL Server Management Studio → 새쿼리

2) EXEC sp_configure ‘xp_cmdshell’, 0;

■ 개체 탐색기를 통해 프로시저 확인

1) SQL Server Management Studio → 개체 탐색기 → 컴퓨터 이름 → 오른쪽 마우스 → 패싯 → 일반

2) XPCmdShellEnabled 값 false 설정

비고

※ EXEC sp_configure 'xp_cmdshell' 쿼리 실행 시 다음과 같은 에러가 출력된다면 이 문제는 sp_configure 저장 프로시저의 업데이트 허용 매개 변수가 1로 설정되어 있어서 발생. 이 문제를 해결하려면 업데이트 허용 매개 변수를 0으로 설정 필요

1) EXEC sp_configure ‘xp_cmdshell’ 쿼리 실행

2) SELECT * FROM sys.configurations WHERE name = ‘allow updates’;

3) allow updates 설정값이 1로 되어있을 경우 아래의 스크립트를 실행하여 0으로 변경

로그 활성화

항목설명

데이터베이스 로그는 침해사고 발생 시, 원인 분석을 위한 자료로 사용되므로 로그 기능을 활성화하여 데이터, 응용프로그램에 대한 로그를 주기적으로 관리해야 한다. 또한 백업 정책을 수립하여 주기적으로 백업을 진행해야 한다.

진단 기준

양호

백업 정책이 수립되어 있으며 데이터, 응용프로그램에 대한 로그를 주기적으로 관리하고 있는 경우

취약

백업 정책이 수립되어 있지 않거나 데이터, 응용프로그램에 대한 로그를 주기적으로 관리하고 있지 않은 경우

진단 방법

■ 개체 탐색기를 통해 확인

1) SQL Server Management Studio → 개체 탐색기 → 컴퓨터 이름 → 오른쪽 마우스 → 보안 → 로그인 감사 설정 여부 확인

2) (실패한 로그인만/성공한 로그인만/실패한 로그인과 성공한 로그인 모두) 이 3가지 중 1가지가 설정되어 있는지 확인

■ 백업 정책 확인

1) 인터뷰를 통해 백업 정책 및 주기적 백업 확인

조치 방법

■ 개체 탐색기를 통해 로그 활성화

1) SQL Server Management Studio → 개체 탐색기 → 컴퓨터 이름 → 오른쪽 마우스 → 보안 → 로그인 감사 설정 여부 확인

2) (실패한 로그인만/성공한 로그인만/실패한 로그인과 성공한 로그인 모두) 이 3가지 중 1가지로 설정

■ 백업 정책 수립

1) 백업 정책을 수립하고 주기적으로 로그 파일을 백업

※ DBMS 유지 보수 및 업그레이드 시에는 전체 FULL 백업 절차 수립 (권고)

최신 보안 패치 적용

항목설명

데이터베이스의 주요한 보안 패치 등을 설치하지 않으면 공격자가 해당 버전의 취약점을 이용하여 데이터베이스에 접근하여 데이터를 열람, 수정, 삭제가 가능하므로 지속적인 관리를 수행하고 최신 보안 패치를 적용해야 한다.

진단 기준

양호
최신 보안 패치가 적용되어 있는 경우

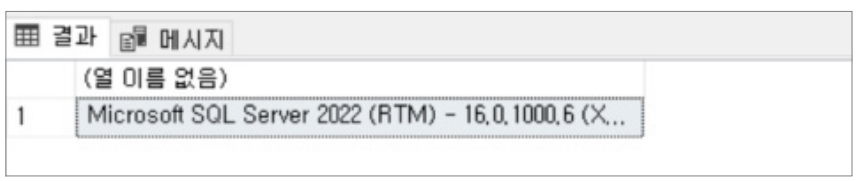
취약
최신 보안 패치가 적용되어 있지 않은 경우

진단 방법

■ 새 쿼리를 통해 현재 버전 확인

1) SQL Server Management Studio → 새 쿼리

2) SELECT @@VERSION;



조치 방법

■ 최신 보안 패치 적용

1) 최신 보안 패치가 발표되면 패치 적용

※ 최신 버전을 사용하도록 권고하고 있으나 시스템 운영상 적용이 어려운 경우 최신이 아닌 취약점이 존재하지 않는 버전도 허용하고 있음

비고

※ 보안 패치를 적용할 경우, 시스템 영향도를 파악하여 충분한 테스트 후 적용 권고

2.12.

Redis

2.12. Redis

보안 설정(4개 항목), 디렉터리 및 파일권한 관리(2개 항목), 패치 및 로그 관리(2개 항목) 총 3개 영역에서 8개 항목으로 구성된다.

[표 12] Redis 진단 체크리스트

구분	진단 항목
가. 보안 설정	Redis 인증 패스워드 설정
	Binding 설정
	Slave 읽기 전용 모드 설정
	rename-command 설정
나. 디렉터리 및 파일권한 관리	데이터 디렉터리 접근권한 설정
	설정 파일 접근권한 설정
라. 패치 및 로그 관리	로그 활성화
	최신 보안 패치 적용

Redis 인증 패스워드 설정

항목설명

Redis 패스워드 설정이 되어 있지 않은 경우, 비인가자가 데이터베이스에 접근이 가능하며 이로 인해 데이터베이스 장악 및 정보 유출의 위험이 존재한다.

진단 기준

양호

인증패스워드가 설정되어 있는 경우

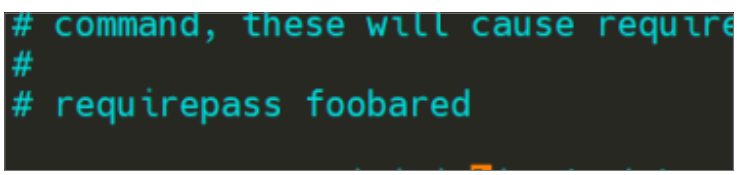
취약

인증패스워드가 설정되어 있지 않은 경우

진단 방법

■ 인증 패스워드 설정

1) # cat [redis 디렉터리/redis.conf] | grep –i requirepass

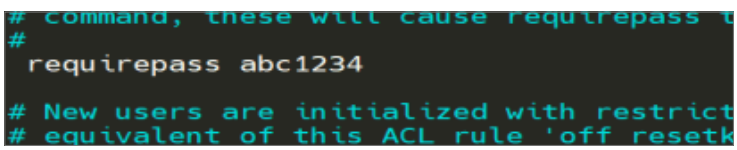


조치 방법

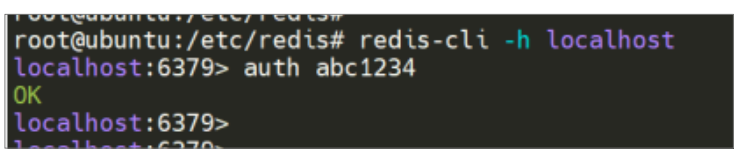
■ redis.conf 파일 안의 requirepass 설정

1) # vi /etc/redis/redis.conf

2) requirepass 값 설정



3) 인증 로그인 확인



Binding 설정

항목설명

인가된 IP만 접근 가능하도록 설정되어 있지 않은 경우, 비인가자가 해당 데이터베이스에 접근할 위험이 존재한다.

진단 기준

양호

인가된 IP만 접근 가능하도록 설정되어 있는 경우

취약

비인가된 IP가 접근 가능하도록 설정되어 있는 경우

진단 방법

■ redis.conf 파일 안의 bind 설정 확인

1) # cat [redis 디렉터리/redis.conf | grep –i bind

```
# COMMENT OUT THE FOLLOWING LINE.
#
# You will also need to set a password unless you explicitly disable protected
# mode.
# ~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
bind 127.0.0.1 -::1

# By default, outgoing connections (from replica to master, from Sentinel to
# instances, cluster bus, etc.) are not bound to a specific local address. In
# most cases, this means the operating system will handle that based on routing
```

※ default 설정 : 127.0.0.1 (로컬호스트에서만 접근 가능)

조치 방법

■ redis.conf 파일 안의 bind 설정

1) # vi [redis 디렉터리/redis.conf]
(인가된 IP만 접근 가능하도록 설정)

Slave 읽기 모드 전용 모드 설정

항목설명

Master와 Slave 환경에서 Slave에 read only 기능만을 설정하여 Master에 있는 자원을 변경할 수 없도록 해야 한다.

진단 기준

양호

Slave에 읽기 권한만 설정되어 있는 경우

취약

Slave에 쓰기 설정이 가능하도록 설정되어 있는 경우

진단 방법

■ redis.conf 파일 내 replica-read-only 설정 확인

1) cat [redis 디렉터리]/redis.conf | grep -i replica-read-only

```
# security of read only replicas using 'rename-command' to shadow all the
# administrative / dangerous commands.
replica-read-only yes

# Replication SYNC strategy: disk or socket.
#
# New replicas and reconnecting replicas that are not able to continue the
```

※ default 설정 : replica-read-only yes

조치 방법

■ redis.conf 파일 내 replica-read-only 설정

1) # vi [redis 디렉터리]/redis.conf
replica-read-only를 yes로 변경

rename-command 설정

항목설명

공유되는 환경에서는 위험한 command들의 이름을 변경할 수 없다. 비인가된 사용자가 환경을 변경하거나 데이터를 가져오는 위험한 command를 사용할 수 없도록 설정해야 한다.

진단 기준

양호

rename-command CONFIG를 빈칸으로 설정하고 있거나 운영상 필요한 command외 나머지 command의 이름을 변경하여 사용하고 있는 경우

취약

rename-command CONFIG 설정이 되어 있지 않은 경우(주석 처리 되어 있는 경우)

진단 방법

■ redis.conf 파일 안의 rename-command CONFIG 확인

1) cat [redis 디렉터리]/redis.conf | grep –i rename-command

```
#
# rename-command CONFIG ""
#
# Please note that changing the name of commands that are l
# AOF file or transmitted to replicas may cause problems.
```

조치 방법

■ redis.conf 파일 안의 rename-command CONFIG 설정

1) # vi [redis 디렉터리]/redis.conf
rename-command CONFIG “” 주석 처리 해제

```
#
 rename-command CONFIG ""
#
# Please note that changing the name of co
# AOF file or transmitted to replicas may
```

데이터 디렉터리 접근 권한 설정

항목설명

일반 사용자가 redis 설치 디렉토리에 임의의 파일을 생성, 삭제 및 변경할 수 있으면 중요 파일 삭제, 백도어 삽입 등의 피해가 발생할 수 있다.

진단 기준

양호

데이터 디렉토리의 접근 권한이 750(-rwxr-x---) 이하인 경우

취약

데이터 디렉토리의 접근 권한이 750(-rwxr-x---) 초과인 경우

진단 방법

■ redis 데이터 디렉터리 접근 권한 확인

예시)

1) ls –ld [redis 데이터 디렉터리]

```
root@ubuntu:/# ls -ld /etc/redis
drwxrws--- 2 redis redis 4096 11월   7 17:50 /etc/redis
root@ubuntu:/#
```

조치 방법

■ redis 데이터 디렉터리 접근 권한 750으로 설정

1) # chmod 750 [redis 데이터 디렉터리]

```
root@ubuntu:/#
root@ubuntu:/# ls -ld /etc/redis
drwxr-s--- 2 redis redis 4096 11월   7 17:50 /etc/redis
root@ubuntu:/#
```

설정 파일 접근권한 설정

항목설명

설정 파일에 other 권한이 존재할 경우, 비인가자가 설정 파일에 접근하여 설정 변경을 통해 서비스 장애를 일으킬 위험이 존재하며 또한 설정 파일을 통해 정보를 획득하여 2차 공격의 정보로 사용할 위험이 존재한다.

진단 기준

양호

설정 파일의 접근 권한이 600(-rw-------) 이하로 설정되어 있는 경우

취약

설정 파일의 접근 권한이 600(-rw-------) 초과로 설정되어 있는 경우

진단 방법

■ redis 디렉터리의 redis.conf 권한 확인

예시)

1) # ls –al [redis 디렉터리]/redis.conf

```
root@ubuntu:/# ls -al /etc/redis/redis.conf
-rw-r----- 1 redis redis 107579 11월   7 17:37 /etc/redis/redis.conf
root@ubuntu:/#
```

조치 방법

■ redis.conf 파일의 권한을 600 이하로 설정

1) # chmod 600 [redis 데이터디렉터리]/redis.conf

로그 활성화

항목설명

로그를 정기적으로 분석하여 침입 유무를 파악하고 침입 시도 의심 사례를 분석하여 사전에 해당 장비에 대한 접근을 차단하는 등 체계적인 로그 관리 작업이 수행되어야 한다.

진단 기준

양호

로그가 활성화되어 있는 경우

취약

로그가 비활성화되어 있는 경우

진단 방법

■ slow query 로그 확인

1) 127.0.0.1〉 config get slowlog-log-slower-than

```
127.0.0.1:6380> config get slowlog-log-slower-than
1) "slowlog-log-slower-than"
2) "10000"
127.0.0.1:6380>
```

※ default 설정 : 10000

■ 로그 레벨 설정 확인

1) 127.0.0.1:6379〉 config get slowlog-log-slower-than

```
root@ubuntu:/etc/redis#
root@ubuntu:/etc/redis# cat /etc/redis/redis.conf | grep loglevel
loglevel notice
root@ubuntu:/etc/redis#
```

조치 방법

■ slow query 로그 설정

1) 127.0.0.1:6379〉 config set slowlog-log-slower-than 100

■ slow query 로그 설정

1) # vi /etc/[redis 디렉터리]/redis.conf 파일 안의 loglevel notice로 변경

※ default 설정 : notice

최신 보안 패치 적용

항목설명

최신 보안 패치가 적용되어 있지 않을 경우, 잘 알려진 취약점에 데이터베이스가 노출될 위험이 존재한다.

진단 기준

양호
최신 보안 패치가 적용되어 있는 경우

취약
최신 보안 패치가 적용되어 있지 않은 경우

진단 방법

■ redis-cli를 이용한 확인

1) # redis-cli -h 127.0.0.1 -p 6379

2) 127.0.0.1:6379> info

```
# Server
redis_version:7.2.3
redis_git_sha1:00000000
```

■ redis 디렉터리에서 확인

1) # [redis 디렉터리]/redis-cli -v

```
root@ubuntu:/etc/redis#
root@ubuntu:/etc/redis# redis-cli -v
redis-cli 7.2.3
```

조치 방법

■ 보안 패치 적용

1) 취약점이 없는 보안 패치가 적용된 버전으로 업데이트해야 함

※ 최신 버전을 사용하도록 권고하고 있으나 시스템 운영상 적용이 어려운 경우 최신이 아닌 취약점이 존재하지 않는 버전도 허용하고 있음

비고

※ 보안 패치를 적용할 경우, 시스템 영향도를 파악하여 충분한 테스트 후 적용 권고

2.13.

Elasticsearch

2.13. Elasticsearch

보안 설정(4개 항목), 디렉터리 및 파일권한 관리(4개 항목), 패치 및 로그 관리(2개 항목) 총 3개 영역에서 10개 항목으로 구성된다.

[표 13] Elasticsearch 진단 체크리스트

구분	진단 항목
가. 보안 설정	Elasticsearch 인증 설정
	디폴트 계정 및 패스워드 변경
	불필요한 계정 제거
	IP 접근 제한 설정
나. 디렉터리 및 파일권한 관리	설치 디렉터리 접근 권한 설정
	플러그인 디렉터리 접근 권한 설정
	설정 파일 접근 권한 설정
	Search-Guard 스크립트 접근 권한 설정
다. 패치 및 로그 관리	로그 활성화
	최신 보안 패치 적용

Elasticsearch 인증 설정

항목설명

Elasticsearch 아이디 및 패스워드 설정이 되어 있지 않은 경우, 서버에 접근하는 사용자 모두 Elasticsearch에 접근이 가능하므로 Elasticsearch 장악 및 정보 유출의 위험이 존재한다.

진단 기준

양호

인증 아이디 및 패스워드가 설정되어 있는 경우

취약

인증 아이디 및 패스워드가 설정되어 있는 경우

진단 방법

■ 설정 파일을 통해 확인

1) Elasticsearch v5.x, v6.x (X-Pack 플러그인 사용)
cat [Elasticsearch 설정 디렉터리]/x-pack/users

```
test@test-virtual-machine:~$ cat /home/test/elasticsearch-5.0.2/config/x-pack/users
es_admin:$2a$10$x8HyZdlFW2a4gTUA2ky6UuHMjeAdvBnHeCqVTA2DS9AkpAZKH2pcC
```

2) Elasticsearch v7.0 이상 (X-Pack 플러그인 사용)
cat [Elasticsearch 설정 디렉터리]/users

```
root@ubuntu:/etc/elasticsearch# cat users
test:$2a$10$OlTPZpsdFgYc5PXt7Ic8MumVkMu48jqKN0OCu4EuwuJdVnherW9XK
root@ubuntu:/etc/elasticsearch#
```

3) Elasticsearch v5.0 이상 (Search-Guard 플러그인)
cat [Elasticsearch 설치 디렉터리]/search-guard-버전/sgconfig/sg_internal_users.yml

```
[root@ELK-TEST ~]# cat /usr/share/elasticsearch/plugins/search-guard-5/sgconfig/sg
_internal_users.yml
# This is the internal user database
# The hash value is a bcrypt hash and can be generated with plugin/tools/hash.sh
admin:
  hash: $2a$12$VcCDgh2NDk07JGNOrjGbM.Ad41qVR/YFJcgHp0UGns5JDymv..TOG
  #password is: admin
logstash:
  hash: $2a$12$u1ShR4l4uBS3Uv59Pa2y5.1uQuZBrZtmNfqB3iM/.jLOXoV9sghS2
  #password is: logstash
kibanaserver:
  hash: $2a$12$4AcgAt3xwOWadA5s5blL6ev39OXDNhmOesEoo33eZtrq2N0YrU3H.
  #password is: kibanaserver
kibanaro:
  hash: $2a$12$JJSXNfTowz7Uu5ttXfeYpeYE0arACvcwlPBStB1F.MI7f0U9Z4DGC
  #password is: kibanaro
  roles:
    - kibanarole
```

■ CURL 명령어을 통해 확인

1) # curl localhost:9200

※ 사용자, 패스워드 입력 없이 위 명령어를 입력하여 결과가 출력된다면 취약 (인증 설정 비활성화 상태)

조치 방법

■ X-Pack 플러그인을 통해 설정

- Elasticsearch v5.x, v6.x

1) # [Elasticsearch 설치 디렉터리/bin/x-pack] ./users useradd '계정명' -r '계정권한' 실행

```
test@test-virtual-machine:~/elasticsearch-5.0.2/bin/x-pack$ ./users useradd es_admin -r superuser
Enter new password:
Retype new password:
```

- Elasticsearch v7.0 이상

1) # vi [Elasticsearch 설정 디렉터리/elasticsearch.yml]

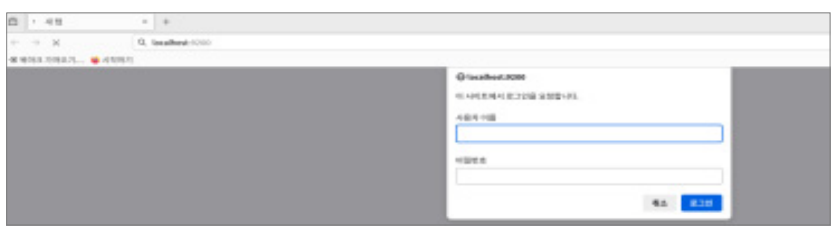
```
xpack.security.enabled: true
xpack.security.transport.ssl.enabled: true
```

2) security 필드에 아래의 내용 추가

3) # [Elasticsearch 설치 디렉터리]/bin/elasticsearch-setup-passwords interactive

4) 사용자 계정 인증 및 인증 창 확인
curl --user '사용자 계정':'패스워드' localhost:9200 입력 또는 검색창에 http://localhost:9200 입력

```
root@ubuntu:~# curl --user elastic:123456 localhost:9200
{
  "name" : "ubuntu",
  "cluster_name" : "elasticsearch",
  "cluster_uuid" : "wHx-7zVqTL-mXF6MxOsuXw",
  "version" : {
    "number" : "7.17.15",
    "build_flavor" : "default",
    "build_type" : "deb",
    "build_hash" : "0b8ecfb4378335f4689c4223d1f1115f16bef3ba"
```



■ Search-Guard 플러그인을 통해 설정

- Elasticsearch v5.0 이상

1) # cd [Elasticsearch 설치 디렉터리]/bin/search-guard-*/tools를 통해 디렉터리 이동

2) # ./hash.sh 명령어를 통해 패스워드 해시값 생성

3) 출력된 해시값과 계정명을 [Elasticsearch 설치 디렉터리]/plugin/search-guard-*/sgconfig/sg_internal_users.yml 설정 파일에 기입

※ 띄어쓰기에 민감하므로 아래 예시된 그림과 같이 라인 간격을 맞춰야 함

```
monitor1234:
  hash: $2a$12$7lR1gr8Rl9XZ8NEk0MsCZ.nVxIX9AvJjmOB7dys13eFwXuxTlMl4a
```

4) [Elasticsearch 설치 디렉터리/bin/search-guard-*/sgconfig/sg_roles_mapping.yml 설정 파일에서 role과 계정 매핑

```
sg_all_access:
  users:
    - admin
    - monitor1234
```

5) [Elasticsearch 설치 디렉터리/bin/search-guard-*/tools/sgadmin_demo.sh 스크립트를 실행하여 설정 적용

비고

1) Elasticsearch X-Pack(Shield) 버전 별 관리자 권한 이름
   [Elasticsearch2.4 이하] admin – 관리자 권한
   [Elasticsearch5.0 이상] superuser – 관리자 권한
2) Elasticsearch SearchGuard 관리자 권한 이름
   admin – 관리자 권한

디폴트 계정 및 패스워드 변경

항목설명

Elasticsearch는 인증을 위해 플러그인 설치 시 디폴트 계정 및 패스워드가 존재하며, 각 정보는 인터넷 등을 통해 쉽게 구할 수 있다. 이를 통해 악의적인 사용자가 디폴트 계정, 패스워드를 이용하여 Elasticsearch에 접근 가능하므로, 데이터 변조, 정보 유출 등의 위험이 존재한다.

진단 기준

양호

디폴트 계정 및 패스워드를 변경한 경우

취약

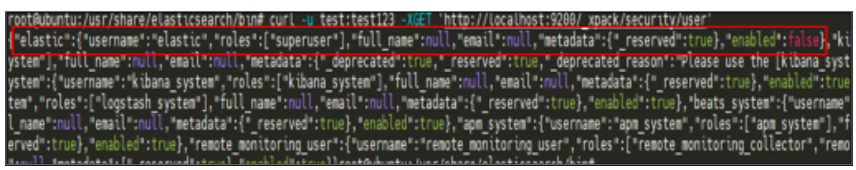
디폴트 계정 및 패스워드를 변경하지 않은 경우

진단 방법

■ CURL 명령어을 통해 확인 (X-Pack 사용 시)

1) 명령어를 통해 확인 (예시)

curl –u test:test123 –XGET 'http://localhost:9200/_xpack_security/user'



※ elastic 계정의 enabled 값이 false : 계정 비활성화 상태 (양호)

■ 설정 파일을 통해 확인(Search-Guard 사용 시)

조치 방법

■ 디폴트 계정 삭제/비활성화 (X-Pack 사용 시)

1) 디폴트 계정을 비활성화하기 전 새로운 계정 생성

```
root@ubuntu:/usr/share/elasticsearch/bin# ./elasticsearch-users useradd test
Enter new password:
Retype new password:
root@ubuntu:/usr/share/elasticsearch/bin#
```

2) 관리자 권한 부여

```
root@ubuntu:/usr/share/elasticsearch/bin# ./elasticsearch-users roles test -a superuser
root@ubuntu:/usr/share/elasticsearch/bin#
```

3) 디폴트 계정 비활성화

```
root@ubuntu:/usr/share/elasticsearch/bin# curl -u test -XPUT 'localhost:9200/_xpack/security/user/elastic/_disable'
Enter host password for user 'test':
{}root@ubuntu:/usr/share/elasticsearch/bin#
```

■ 디폴트 계정 삭제/비활성화 (Search-Guard 사용 시)

1) 디폴트 계정을 비활성화하기 전 새로운 계정 생성

```
[root@ELK-TEST ~]# /usr/share/elasticsearch/plugins/search-guard-5/tools/hash.sh
[Password:]
$2a$12$2a2Hd.s7jiQdmrooYUGx3OmRfq9Z7wYOyyUUbtXOWXu.5yIniOFrO
```

2) # [Elasticsearch 설치 디렉터리]/plugins/search-guard-*/sgconfig/sg_internal_users.yml 파일을 수정하여 기존 관리자 계정 영역 삭제 및 신규 계정 및 패스워드 적용

```
[redacted]
  hash: $2a$12$2a2Hd.s7jiQdmrooYUGx3OmRfq9Z7wYOyyUUbtXOWXu.5yIniOFrO
```

3) # [Elasticsearch 설치 디렉터리]/plugins/search-guard-*/sgconfig/sg_roles_mapping.yml 파일을 수정하여 기존 관리자 계정 삭제 및 신규 계정 적용

```
sg_all_access:
  users:
    - [redacted]
```

비고

※ Elasticsearch Shield 플러그인의 경우 디폴트 계정이 존재하지 않음

※ Elasticsearch X-Pack 플러그인의 경우 디폴트 계정은 elastic, 패스워드는 changeme로 설정되어 있음

※ Elasticsearch Search-Guard 플러그인의 경우 디폴트 계정은 admin, 패스워드는 admin으로 설정되어 있음

불필요한 계정 제거

항목설명

Elasticsearch의 계정 중 인가되지 않은 계정, 퇴직자 계정, 테스트 계정 등 실질적으로 업무에 사용하지 않은 불필요한 계정들이 있는 경우 비인가자가 쉽게 데이터베이스에 접속하여 데이터를 열람, 삭제, 수정 등을 할 위험이 있다.

진단 기준

양호

테스트 계정, 의심스러운 계정, 불필요한 계정이 존재하지 않는 경우

취약

테스트 계정, 의심스러운 계정, 불필요한 계정이 존재하는 경우

진단 방법

■ 사용자 계정 조회

- Elasticsearch v5.x, v6.x (X-Pack 플러그인 사용 시)

1) # cat [Elasticsda 설정 디렉터리]/x-paxk/user_roles 또는

```
test@test-virtual-machine:~$ cat /home/test/elasticsearch-5.0.2/config/x-pack/users_roles
ingest_admin:test
superuser:es_admin
```

[Elasticsearch 설치 디렉터리]/bin/x-pack/elasticsearch-users list

```
test@test-virtual-machine:~/elasticsearch-5.0.2/bin/x-pack$ ./users list
test            : ingest_admin
es_admin        : superuser
```

- Elasticsearch v7.0 이상 (X-Pack 플러그인 사용 시)

1) # cat [Elasticsearch 설정 디렉터리]/users_roles 또는

```
root@ubuntu:/etc/elasticsearch# cat users_roles
superuser:test
root@ubuntu:/etc/elasticsearch#
```

[Elasticsearch 설치 디렉터리]/bin/elasticsearch-users list

```
root@ubuntu:/usr/share/elasticsearch/bin# ./elasticsearch-users list
test            : superuser
root@ubuntu:/usr/share/elasticsearch/bin#
```

- Elasticsearch v5.0 이상 (Search-Guard 플러그인 사용 시)

1) # cat [Elasticsearch 설정 디렉터리]/sgconfig/sg_internal_users.yml 를 통해 확인

```
[root@ELK-TEST /]# cat /usr/share/elasticsearch/plugins/search-guard-5/sgconfig/sg_roles_mapping.yml

# In this file users, backendroles and hosts can be mapped to search guard roles.
# What a role is allowed to do you specify in sg_roles.yml

sg_all_access:
  users:
    - ksel

sg_logstash:
  users:
    - logstash
```

조치 방법

- Elasticsearch v5.x, v6.x (X-Pack 플러그인 사용 시)

  1) # [Elasticsearch 설치 디렉터리]/bin/x-pack/users userdel '계정명' 실행

```
test@test-virtual-machine:~/elasticsearch-5.0.2/bin/x-pack$ ./users userdel test
```

- Elasticsearch v7.0 이상 (X-Pack 플러그인 사용 시)

  1) # [Elasticsearch 설치 디렉터리]/bin/elasticsearch-users userdel 〈사용자 명〉

```
root@ubuntu:/usr/share/elasticsearch/bin# ./elasticsearch-users userdel test_go
root@ubuntu:/usr/share/elasticsearch/bin#
```

■ 설정 파일 및 명령어를 통해 변경 (SearchGuard 사용 시)

- Elasticsearch 5.0 이상 SearchGuard 플러그인 사용 시

  1) # [Elasticsearch 설치 디렉터리]/plugins/search-guard-*/sgconfig/sg_roles_mapping.yml 파일을 수정하여 불필요한 계정 제거

  2) # [Elasticsearch 설치 디렉터리]/plugins/search-guard-*/tools/sgadmin_demo.sh을 실행하여 설정 적용

IP 접근 제한 설정

항목설명

인가된 IP만 접근 가능하도록 설정되어 있지 않은 경우, 비 인가된 사용자가 해당 데이터베이스에 접근할 위험이 존재한다.

진단 기준

양호

인가된 IP만 접근 가능하도록 설정되어 있는 경우

취약

비 인가된 IP의 접근이 가능하도록 설정되어 있는 경우

진단 방법

■ Elasticsearch 설정 파일에서 network.host 확인

1) # cat [Elasticsearch 디렉터리]/elasticsearch.yml | grep network.host

```
root@ubuntu:~# cat /etc/elasticsearch/elasticsearch.yml | grep network.host
#network.host: 192.168.0.1
root@ubuntu:~#
```

조치 방법

■ Elasticsearch 설정 파일 안의 network.host 설정 변경

1) # vi cat [Elasticsearch 디렉터리]/elasticsearch.yml

2) network.host 인가된 IP로 변경

```
# address here to expose this node on the network:
#
network.host: 192.168.153.138
#
# By default Elasticsearch listens for HTTP traffic on the first free port it
```

설치 디렉터리 접근 권한 설정

항목설명

일반 사용자가 Elasticsearch 설치 디렉토리에 임의의 파일을 생성, 삭제 및 변경 할 수 있으면, 중요파일 삭제, 백도어 삽입 등의 피해가 발생할 수 있다.

진단 기준

양호

설치 디렉터리의 권한이 750(-rwxr-x---) 이하인 경우

취약

설치 디렉터리의 권한이 750(-rwxr-x---) 초과한 경우

진단 방법

■ Elasticsearch 설치 디렉터리 권한 확인

1) # ls –ld [Elasticsearch 설치 디렉터리]

```
root@ubuntu:~# ls -ld /etc/elasticsearch
drwxr-s--- 3 root elasticsearch 4096 12월   5 16:55 /etc/elasticsearch
root@ubuntu:~#
```

조치 방법

■ Elasticsearch 설치 디렉터리 권한 750으로 변경

1) # chmod 750 [Elasticsearch 설치 디렉터리]

플러그인 디렉터리 접근 권한 설정

항목설명

Elasticsearch 플러그인을 설치하게 되면 플러그인 디렉터리가 생성되고 그 안에서 설치한 플러그인을 관리하게 된다. 만약 일반 사용자가 해당 디렉터리에 접근이 가능할 경우 임의의 파일을 생성, 삭제 및 변경할 수 있으며 플러그인 파일 삭제, 백도어 삽입 등의 피해가 발생할 수 있다.

진단 기준

양호

플러그인 디렉터리 권한이
750(-rwx-r-x----) 이하인 경우

취약

플러그인 디렉터리 권한이
750(-rwx-r-x----) 초과된 경우

진단 방법

■ Elasticsearch 플러그인 디렉터리 권한 확인

1) # ls- ld [Elasticsearch 설치 디렉터리]/plugins

```
root@ubuntu:~# ls -ld /usr/share/elasticsearch/plugins
drwxr-xr-x 2 root root 4096 11월  11 07:08 /usr/share/elasticsearch/plugins
root@ubuntu:~#
```

조치 방법

■ Elasticsearch 플러그인 디렉터리 권한 750으로 변경

1) # chmod 750 [Elasticsearch 설치 디렉터리]/plugins

```
root@ubuntu:~# chmod 750 /usr/share/elasticsearch/plugins
root@ubuntu:~# ls -ld /usr/share/elasticsearch/plugins
drwxr-x--- 2 root root 4096 11월  11 07:08 /usr/share/elasticsearch/plugins
root@ubuntu:~#
```

설정 파일 접근 권한 설정

항목설명

설정 파일에 others 권한이 존재할 경우, 비 인가된 사용자가 설정 파일에 접근하여 설정 변경을 통해 서비스 장애를 일으킬 위험이 존재하며 설정 파일을 통해 정보를 획득하여 2차 공격의 정보로 사용할 위험이 존재한다.

진단 기준

양호

설정 파일 권한이 660(-rw-rw----) 이하인 경우

취약

설정 파일 권한이 660(-rw-rw----) 초과인 경우

진단 방법

■ Elasticsearch.yml 파일 권한 확인

1) # ls -l [Elasticsearch 설정 디렉터리]/elasticsearch.yml

```
root@ubuntu:~# ls -l /etc/elasticsearch/elasticsearch.yml
-rw-rw---- 1 root elasticsearch 3431 11월  11 07:05 /etc/elasticsearch/elasticsearch.yml
root@ubuntu:~#
```

■ SearchGuard 이용 시 설정 파일의 권한 확인

1) # ls -l [Elasticsearch 설치 디렉터리]/plugins/search-guard-*/sgconfig 실행

조치 방법

■ 설정 파일의 권한을 660 이하로 변경

1) # chmod 660 [Elasticsearch 디렉터리/elasticsearch.yml]

Search-Guard 스크립트 접근 권한 설정

항목설명

Search-guard를 통해 인증을 적용할 때 설정 파일에 적용 후 Search-guard에서 제공하는 스크립트를 실행해야 인증 설정이 적용된다. 스크립트 파일 권한에 other 권한이 있을 경우 스크립트 내용이 노출되거나 스크립트가 실행되어 악의적인 영향을 끼칠 수 있다.

진단 기준

양호

Search-guard 스크립트 파일 권한이 750(-rwxr-x---) 이하인 경우

취약

Search-guard 스크립트 파일 권한이 750(-rwxr-x---) 초과인 경우

진단 방법

※ Search-guard 플러그인이 설치되어 있지 않은 경우에는 해당 사항 없음

■ Elasticsearch 설정 파일의 권한 확인

1) # ls -l [Elasticsearch 설정 디렉터리]/plugins/search-guard-*/tools

```
[root@ELK-TEST /]# ls -l /usr/share/elasticsearch/plugins/search-guard-5/tools/
합계 36
-rw-r--r--. 1 root root   214  7월 12 13:59 hash.bat
-rwxrwx---. 1 root root   373  7월 12 13:59 hash.sh
-rwx------. 1 root root 15839  7월 12 13:59 install_demo_configuration.sh
-rw-r--r--. 1 root root   282  7월 12 13:59 sgadmin.bat
-rwxr-xr-x. 1 root root   414  7월 12 13:59 sgadmin.sh
-rwxr-xr-x. 1 root root   264  7월 12 13:59 sgadmin_demo.sh
```

조치 방법

■ Search-guard 스크립트 파일 권한을 750 이하로 변경

1) chmod 750 [Elasticsearch 디렉터리]/plugins/search-guard-*/tools/[Search-Guard 스크립트 파일]

로그 활성화

항목설명

로그를 정기적으로 분석하여 침입 유무를 파악하고, 침입 시도 의심 사례를 분석하여 사전에 해당 장비에 대한 접근을 차단하는 등 체계적인 로그 관리 작업이 이루어져야 한다.

진단 기준

양호
로그가 활성화되어 있는 경우

취약
로그가 활성화되어 있지 않은 경우

진단 방법

■ 감사로그 활성화 확인 (Elasticsearch v7.0 이상 X-pack 사용)

1) # cat [Elasticsearch 설정 디렉터리]/elasticsearch.yml | grep xpack.security.audit

```
root@ubuntu:/etc/elasticsearch# cat /etc/elasticsearch/elasticsearch.yml | grep xpack.security.audit
xpack.security.audit.enabled: true
xpack.security.audit.outputs: [ "index" ]
root@ubuntu:/etc/elasticsearch#
```

2) xpack.security.audit.enabled : true 설정 확인

※ default : 설정이 존재하지 않음

조치 방법

■ 감사로그 활성화 (Elasticsearch v7.0 이상 X-pack 사용)

1) # vi [Elasticsearch 설정 디렉터리]/elasticsearch.yml에 아래 내용 추가

```
xpack.security.audit.enabled: true
xpack.security.audit.outputs: [ "index" ]
```

2) elasticsearch 재시작

3) /var/log/elasticsearch 내 감사 로그 파일 생성 확인

```
-rw-r--r--.  1 elasticsearch elasticsearch  13171 12월   8 10:20 elasticsearch.log
-rw-r--r--.  1 elasticsearch elasticsearch      0 12월   5 17:59 elasticsearch_audit.json
-rw-r--r--.  1 elasticsearch elasticsearch   4764 12월   6 13:19 elasticsearch_deprecation.json
```

비고

※ X-pack을 사용하지 않는 경우, /var/log/elasticsearch/elasticsearch.log 파일을 주기적으로 검토/관리해야 함
(elasticsearch.log 파일에는 실행 로그가 기록됨)

최신 보안 패치 적용

항목설명

최신 보안패치가 적용되어 있지 않을 경우, 보안 취약점에 데이터베이스가 노출될 위험이 존재한다.

진단 기준

양호

보안 취약점이 존재하지 않는 최신 보안패치 버전을 사용 중인 경우

취약

보안 취약점이 존재하지 않는 최신 보안패치 버전을 사용 중이지 않은 경우

진단 방법

■ CLI를 통해 확인

1) # [Elasticsearch 설치 디렉터리]/bin/elasticsearch -v

■ CURL를 통해 확인

1) # curl localhost:9200

```
root@ubuntu:~# curl localhost:9200
{
  "name" : "ubuntu",
  "cluster_name" : "elasticsearch",
  "cluster_uuid" : "oLHTK3fFScuz7aXJ6WAqnA",
  "version" : {
    "number" : "7.17.15",
    "build_flavor" : "default",
    "build_type" : "deb",
    "build_hash" : "0b8ecfb4378335f4689c4223d1f1115f16bef3ba",
    "build_date" : "2023-11-10T22:03:46.987399016Z",
    "build_snapshot" : false,
    "lucene_version" : "8.11.1",
    "minimum_wire_compatibility_version" : "6.8.0",
    "minimum_index_compatibility_version" : "6.0.0-beta1"
  },
  "tagline" : "You Know, for Search"
}
```

조치 방법

■ 보안 패치 적용

1) 보안 취약점이 존재하지 않는 버전으로 보안 패치를 적용해야 함

※ 최신 버전을 사용하도록 권고하고 있으나 시스템 운영상 적용이 어려운 경우 최신이 아닌 취약점이 존재하지 않는 버전도 허용하고 있음

비고

※ 보안 패치를 적용할 경우, 시스템 영향도를 파악하여 충분한 테스트 후 적용 권고

2.14.

MongoDB

2.14. MongoDB

계정 관리(4개 항목), 디렉터리 및 파일권한 관리(3개 항목), 패치 및 로그 관리(2개 항목) 총 3개 영역에서 9개 항목으로 구성된다.

[표 14] MongoDB 진단 체크리스트

구분	진단 항목
가. 계정 관리	불필요한 데이터베이스 및 테이블 제거
	불필요한 계정 제거
	데몬 실행 시 인증 옵션 사용
	관리자 계정 생성 여부
나. 디렉터리 및 파일권한 관리	주요 실행 및 설정 파일 권한 관리
	http interface 접근 통제
	데이터베이스 접근 제한 설정
라. 패치 및 로그 관리	로그 기록 및 백업
	최신 보안 패치 적용

불필요한 데이터베이스 및 테이블 제거

항목설명

사용하지 않거나 테스트 용도의 데이터베이스(collection)가 존재하면 관리 미흡으로 인해 침해사고가 발생할 가능성이 있으므로 불필요한 데이터베이스 및 테이블을 제거해야 한다.

진단 기준

양호

운영에 불필요한 데이터베이스, collection이 존재하지 않는 경우

취약

운영에 불필요한 데이터베이스, collection이 존재하는 경우

진단 방법

■ 존재하는 데이터베이스 확인

1) 〉 show dbs;

```
test_mongo> show dbs
admin        40.00 KiB
config      108.00 KiB
local        40.00 KiB
test_mongo    8.00 KiB
test_mongo>
```

■ 존재하는 collection 확인

1) 〉 use [DB 명];
2) 〉 show collections;

```
test_mongo> show collections
asd
collection_test
test_mongo>
```

조치 방법

■ 불필요한 데이터베이스 삭제

1) 〉 use [삭제할 DB명]
2) 〉 db.dropDatabase();

■ 불필요한 collection 삭제

1) 〉 use [삭제할 collection이 존재하는 DB명]
2) 〉 db.[collection명].drop();

불필요한 계정 제거

항목설명

사용하지 않거나 테스트 용도의 데이터베이스 계정이 존재하면 해당 계정의 관리 미흡으로 인해 비인가 사용자가 접근할 위험이 존재하므로 불필요한 계정을 제거해야 한다.

진단 기준

양호

운영에 불필요한 계정이 존재하지 않는 경우

취약

운영에 불필요한 계정이 존재하는 경우

진단 방법

■ 존재하는 계정 확인

1) 〉 show users;

```
admin> show users;
[
  {
    _id: 'admin.test_developer',
    userId: UUID('bfa865d3-ac3e-44dd-bcbe-a880c785041f'),
    user: 'test_developer',
    db: 'admin',
    roles: [ { role: 'readWrite', db: 'admin' } ],
    mechanisms: [ 'SCRAM-SHA-1', 'SCRAM-SHA-256' ]
  },
  {
    _id: 'admin.tester',
    userId: UUID('c79c4bfa-2d04-4735-b0e5-e17bc668eadf'),
    user: 'tester',
    db: 'admin',
    roles: [ { role: 'read', db: 'admin' } ],
    mechanisms: [ 'SCRAM-SHA-1', 'SCRAM-SHA-256' ]
  }
]
admin>
```

조치 방법

■ 불필요한 계정 삭제

1) 〉 db.dropUser("계정명");

```
admin> db.dropUser("test_developer");
{ ok: 1 }
admin>

admin> show users;
[
  {
    _id: 'admin.tester',
    userId: UUID('c79c4bfa-2d04-4735-b0e5-e17bc668eadf'),
    user: 'tester',
    db: 'admin',
    roles: [ { role: 'read', db: 'admin' } ],
    mechanisms: [ 'SCRAM-SHA-1', 'SCRAM-SHA-256' ]
  }
]
admin>
```

※ MongoDB v2.6까지 계정 삭제 시, db.removeUser() 명령어 사용

데몬 실행 시 인증 옵션 사용

항목설명

mongod(MongoDB 실행 데몬)를 실행할 때, 인증을 사용하는 옵션을 사용하여 비인가 사용자가 DB에 접근할 수 없도록 해야 한다.

진단 기준

양호

mongod 환경설정 파일에 authorization이 enabled로 설정된 경우

취약

mongod 환경설정 파일에 authorization 값이 존재하지 않거나 true로 설정되어 있지 않은 경우

진단 방법

■ 인증 옵션 확인

1) # cat [MongoDB 환경설정 파일] | grep auth (예시)

```
root@ubuntu:~# cat /etc/mongod.conf | grep auth
root@ubuntu:~#
root@ubuntu:~#
```

※ default : authorization 값 존재하지 않음

조치 방법

■ 인증 옵션 사용 활성화

1) 환경설정 파일 내 security 필드 아래 authorization 값 enabled 설정

```
security:
  authorization : enabled
```

※ MongoDB v3.0 이하에서는 auth=true로 설정

■ MongoDB 재구동 (예시)

1) # systemctl restart mongod

■ 사용자 인증 확인

1) 〉 db.auth("사용자 계정", "패스워드");

```
admin> db.auth("tester","1234");
{ ok: 1 }
admin>
```

관리자 계정 생성 여부

항목설명

관리자 계정이 없으면 인증 없이 DB에 접근하거나 DB 서버를 임의로 종료시키는 위험이 존재한다.

진단 기준

양호
관리자 계정이 존재하는 경우

취약
관리자 계정이 존재하지 않는 경우

진단 방법

■ 계정 목록 확인

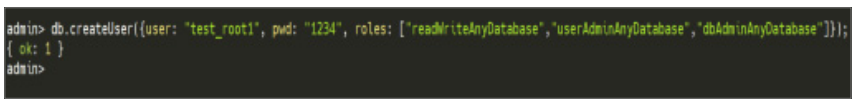
1) 〉 use admin;
2) 〉 show users;

```
admin> use admin
already on db admin
admin> show users;
[
  {
    _id: 'admin.test_developer',
    userId: UUID('bfa865d3-ac3e-44dd-bcbe-a880c785041f'),
    user: 'test_developer',
    db: 'admin',
    roles: [ { role: 'readWrite', db: 'admin' } ],
    mechanisms: [ 'SCRAM-SHA-1', 'SCRAM-SHA-256' ]
  },
  {
    _id: 'admin.test_root',
    userId: UUID('152d5c6c-e4f1-4059-aff8-644e87a0bdb3'),
    user: 'test_root',
    db: 'admin',
    roles: [ { role: 'root', db: 'admin' } ],
    mechanisms: [ 'SCRAM-SHA-1', 'SCRAM-SHA-256' ]
  },
  {
    _id: 'admin.test_root1',
    userId: UUID('31141f48-1427-412f-b1c8-0d385c738198'),
    user: 'test_root1',
    db: 'admin',
    roles: [
      { role: 'readWriteAnyDatabase', db: 'admin' },
      { role: 'userAdminAnyDatabase', db: 'admin' },
      { role: 'dbAdminAnyDatabase', db: 'admin' }
    ],
    mechanisms: [ 'SCRAM-SHA-1', 'SCRAM-SHA-256' ]
  },
  {
    _id: 'admin.tester',
    userId: UUID('c79c4bfa-2d04-4735-b0e5-e17bc668eadf'),
    user: 'tester',
    db: 'admin',
    roles: [ { role: 'read', db: 'admin' } ],
    mechanisms: [ 'SCRAM-SHA-1', 'SCRAM-SHA-256' ]
  }
]
```

조치 방법

■ 관리자 계정 생성

1) 쿼리 입력
〉 db.createUser({user: “관리자 계정명”, pwd: “패스워드”, roles: [“readWriteAnyDatabase”,“userAdminAnyDatabase”,“dbAdminAnyDatabase”]});



※ roles : superuser 권한(root)은 사용하지 않도록 설정

비고

권한	설명
readWriteAnyDatabase	전체 DB 읽기 쓰기 가능
userAdminAnyDatabase	전체 DB에서 역할과 사용자 생성, 수정 가능
dbAdminAnyDatabase	전체 DB 스키마 작업 가능, 권한 부여 불가
root	모든 DB의 권한을 부여

주요 실행 및 설정 파일 권한 관리

항목설명

실행 파일로 이루어진 파일은 전체 시스템에 손상을 줄 수 있으므로 별도의 계정이나 관리자가 소유해야 하며, other 권한에 읽기, 쓰기, 실행 권한을 제거하여 임의의 실행 및 정보 탈취 위험으로부터 보호해야 한다.

진단 기준

양호

실행 파일 및 설정 파일의 소유자 및 그룹이 별도의 계정의 소유이며 파일의 권한이 750(-rwxr-x---) 이하로 설정된 경우

취약

실행 파일 및 설정 파일의 소유자 및 그룹이 별도의 계정의 소유가 아니며 파일의 권한이 750(-rwxr-x---) 초과로 설정된 경우

진단 방법

■ 실행 파일 권한 확인 (예시)

1) # ls -al [MongoDB 실행 파일] | grep "mongo*"

```
root@ubuntu:/# ls -al /usr/bin | grep "mongo*"
-rwxr-xr-x  1 [redacted] 181872200 12월  19  2013 mongod
-rwxr-xr-x  1 [redacted]  16191528 11월  18 02:31 mongodump
-rwxr-xr-x  1 [redacted]  15882792 11월  18 02:31 mongoexport
-rwxr-xr-x  1 [redacted]  16731424 11월  18 02:31 mongofiles
-rwxr-xr-x  1 [redacted]  16134272 11월  18 02:31 mongoimport
-rwxr-xr-x  1 [redacted]  16522968 11월  18 02:31 mongorestore
-rwxr-xr-x  1 [redacted] 129520840 12월  19  2013 mongos
-rwxr-xr-x  1 [redacted] 111718960 11월  21 03:27 mongosh
-rwxr-xr-x  1 [redacted]  15751912 11월  18 02:31 mongostat
-rwxr-xr-x  1 [redacted]  15327224 11월  18 02:31 mongotop
root@ubuntu:/#
```

■ 설정 파일 권한 확인 (예시)

1) # ls -al [MongoDB 설정 파일]

```
root@ubuntu:/# ls -al /etc/mongod.conf
-rw-r--r-- 1 root root 604 11월  30 17:25 /etc/mongod.conf
root@ubuntu:/#
```

조치 방법

■ 실행 파일, 설정 파일 소유자 수정 및 Others 실행 권한 제거

1) # chown dba:dba [file명]
2) # chmod 750 [file명]

비고

※ MongoDB v7.0
실행 파일 위치 : /usr/bin
설정 파일 위치 : /etc/mongod.conf

http interface 접근 통제

항목설명

http interface에 접근 제한이 설정되어 있지 않으면 누구나 http interface를 통해 MongoDB를 모니터링 할 수 있으므로 http interface 접근 통제 설정을 적용해야 한다.

진단 기준

양호

http interface를 사용하지 않거나 해당 http://주소:포트번호로 접근할 시, 인증 창이 활성화되는 경우

취약

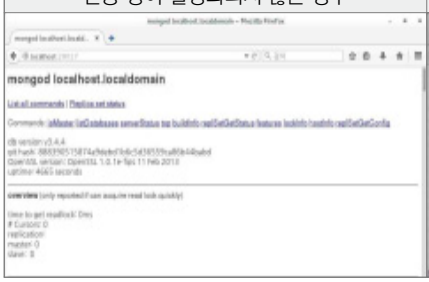
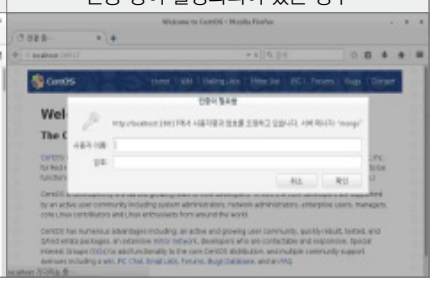
해당 http://주소:포트번호로 접근할 시, 인증 절차 없이 바로 모니터링이 가능한 경우

진단 방법

※ http interface 사용하고 있는지 확인 필요

■ http://주소:포트번호 확인

1) 해당 http 서비스를 사용하고 있는지 확인

인증 창이 활성화되지 않은 경우	인증 창이 활성화되어 있는 경우
	

※ default : https interface 비활성화

조치 방법

■ 인증 옵션 추가 후, 데몬 재시작 (예시)

1) --auth 옵션 설정 후, mongod 데몬 재시작
mongod—config [MongoDB 설정 파일] --auth

```
[root@localhost bin]# /usr/local/mongodb/bin/mongod --config /usr/local/mongodb/
conf/mongodb.conf --auth
```

2) 설정 파일 수정
vi [MongoDB 설정 파일]
authorization : enabled 설정

```
security:
  authorization : enabled
```

※ auth=true (일부 버전에 해당)

데이터베이스 접근 제한 설정

항목설명

MongoDB의 접근 제한을 설정하지 않으면 비인가 사용자가 데이터베이스에 접근하여 데이터를 열람, 수정, 삭제가 가능하므로 특정한 IP만 접근 가능하도록 접근 제한 설정을 해야 한다.

진단 기준

양호

인가된 IP만 접근할 수 있도록 제한 설정을 한 경우

취약

인가된 IP만 접근할 수 있도록 제한 설정을 하지 않은 경우

진단 방법

■ 환경 설정 파일에서 확인

1) # cat [MongoDB 환경 설정 파일] | grep bind

```
root@ubuntu:~# cat /etc/mongod.conf | grep bind
  bindIp: 127.0.0.1
root@ubuntu:~#
```

※ default : 127.0.0.1

조치 방법

■ 환경 설정 파일에서 bindip 수정

1) # vi [MongoDB 환경 설정 파일]
   bindIp : 인가된 IP

비고

※ bindIp가 설정되어 있지 않을 경우, 해당 DB의 서버 IP 접근 제한 정책도 함께 확인 필요

로그 기록 및 백업

항목설명

침해사고 발생 시, 사고 원인을 분석하기 위해 데이터베이스의 로그 백업 정책을 수립하여 로그 파일을 관리하여야 하며 해당 로그 파일을 주기적으로 백업해야 한다.

진단 기준

양호

백업 정책에 의해 로그를 관리하고 있으며 주기적으로 백업을 진행하고 있는 경우

취약

백업 정책에 의해 로그를 관리하고 있지 않으며 주기적으로 백업을 진행하고 있지 않은 경우

진단 방법

■ 수동 점검

1) 로그 파일 위치

cat [MongoDB 환경 설정 파일] | grep path

```
root@ubuntu:~# cat /etc/mongod.conf | grep path
  path: /var/log/mongodb/mongod.log
root@ubuntu:~#
```

2) 담당자 인터뷰를 통해 로그 파일 관리 방법 및 백업 진행 여부 확인

조치 방법

■ 정책 수립

1) 백업 정책을 수립하여 로그 파일을 관리
2) 주기적으로 로그 파일을 백업

최신 보안 패치 적용

항목설명

데이터베이스의 주요 보안 패치 등을 설치하지 않은 경우, 데이터베이스가 자체 취약점에 노출되어 공격자에 의해 공격당할 위험이 존재한다.

진단 기준

양호

최신 보안 패치를 적용한 경우

취약

최신 보안 패치를 적용하지 않은 경우

진단 방법

■ 설치 버전 확인

1) # mongod --version

```
root@ubuntu:~# mongod --version
db version v7.0.4
Build Info: {
    "version": "7.0.4",
    "gitVersion": "38f3e37057a43d2e9f41a39142681a76062d582e",
    "openSSLVersion": "OpenSSL 3.0.2 15 Mar 2022",
    "modules": [],
    "allocator": "tcmalloc",
    "environment": {
        "distmod": "ubuntu2204",
        "distarch": "x86_64",
        "target_arch": "x86_64"
    }
}
root@ubuntu:~#
```

2) # mongosh

```
root@ubuntu:~# mongosh
Current Mongosh Log ID: 656c9c37abd863aebfe01a0b
Connecting to:          mongodb://127.0.0.1:27017/?directConnection=t
Using MongoDB:          7.0.4
Using Mongosh:          2.1.0

For mongosh info see: https://docs.mongodb.com/mongodb-shell/

test>
```

조치 방법

■ 보안 패치 적용

1) 보안 취약점이 존재하지 않는 버전으로 보안패치를 적용해야 함

※ 최신 버전을 사용하도록 권고하고 있으나 시스템 운영상 적용이 어려운 경우 최신이 아닌 취약점이 존재하지 않는 버전도 허용하고 있음

비고

※ 보안 패치를 적용할 경우, 시스템 영향도를 파악하여 충분한 테스트 후 적용 권고

2.15.

PostgresSQL

2.15. PostgresSQL

보안 설정(7개 항목), 디렉토리 및 파일권한 관리(2개 항목), 패치 및 로그 관리(2개 항목) 총 3개 영역에서 11개 항목으로 구성된다.

[표 15] PostgreSQL 진단 체크리스트

구분	진단 항목
가. 보안 설정	불필요한 계정 제거
	취약한 패스워드 사용 제한
	불필요한 권한 제거
	public schema 사용 제한
	IP 접근 제한 설정
	안전한 인증 방식 설정
	안전한 암호화 알고리즘 사용
나. 디렉토리 및 파일권한 관리	데이터 디렉토리 권한 설정
	환경 설정파일 권한 설정
다. 패치 및 로그 관리	로그 활성화
	최신 패치 적용

불필요한 계정 제거

항목설명

데이터베이스의 계정 중 인가되지 않은 계정, 퇴직자 계정, 테스트 계정 등 실질적으로 업무에 사용하지 않은 불필요한 계정들이 있는 경우 비인가자가 쉽게 데이터베이스에 접속하여 데이터를 열람, 삭제, 수정 등을 할 위험이 있다.

진단 기준

양호

DB 설치 시 Default로 생성되는 계정 및 테스트 계정, 의심스러운 계정, 불필요한 계정이 없는 경우

취약

DB 설치 시 Default로 생성되는 계정 및 테스트 계정, 의심스럽거나 불필요한 계정이 있는 경우

진단 방법

■ psql 접속 후, \du 명령어로 확인

1) postgres=# \du

```
postgres=# \du
                                   List of roles
 Role name |                         Attributes                         | Member of
-----------+------------------------------------------------------------+-----------
 postgres  | Superuser, Create role, Create DB, Replication, Bypass RLS | {}
 test      | Superuser                                                  | {}
 test1     |                                                            | {}
 test2     |                                                            | {}
```

조치 방법

■ NOLOGIN 설정

1) postgres=# ALTER ROLE 계정명 WITH NOLOGIN;

```
postgres=# ALTER ROLE test2 WITH NOLOGIN;
ALTER ROLE
postgres=#
postgres=#
postgres=# \du
                                   List of roles
 Role name |                         Attributes                         | Member of
-----------+------------------------------------------------------------+-----------
 postgres  | Superuser, Create role, Create DB, Replication, Bypass RLS | {}
 test      | Superuser                                                  | {}
 test1     |                                                            | {}
 test2     | Cannot login                                               | {}
```

■ 불필요한 사용자 계정 제거

1) postgres=# DROP USER 계정명;

```
postgres=# DROP USER test1;
DROP ROLE
postgres=# \du
                                   List of roles
 Role name |                         Attributes                         | Member of
-----------+------------------------------------------------------------+-----------
 postgres  | Superuser, Create role, Create DB, Replication, Bypass RLS | {}
 test      | Superuser                                                  | {}
 test2     | Cannot login                                               | {}
```

취약한 패스워드 사용 제한

항목설명

패스워드가 추측이 가능하거나 null인 상태인 경우, 비인가자가 쉽게 데이터베이스에 접근할 위험이 있으며 이 경우 데이터베이스 데이터를 삭제, 변경 등의 심각한 침해 사고를 일으킬 가능성이 있으므로 패스워드 복잡도 설정을 만족하도록 패스워드를 변경해서 사용해야 한다.

진단 기준

양호
null인 패스워드를 사용하지 않으며 복잡도 설정을 만족하는 경우

취약
null인 패스워드를 사용하거나 복잡도 설정을 만족하지 않는 경우

진단 방법

■ psql 접속 후, 명령어를 통해 확인

1) postgres=# select usename, passwd from pg_shadow;

```
postgres=# select usename, passwd from pg_shadow;
 usename  |                                                     passwd
----------+-----------------------------------------------------------------------------
 postgres |
 test     |
 test2    |
 test3    | SCRAM-SHA-256$4096:LuJddHngmewGRNMfdpffkQ==$bEzFkFisF70sEB58UhBib0fgUKeABwBvf
 test1    | SCRAM-SHA-256$4096:b1eRZPV9UCsIC1xFi+yOlQ==$ZneV72Ao5tgI2yRKjIOXRq6EzpqI+e6vw
(5 rows)
```

※ passwd 필드가 비어있다면 null인 상태

■ 인터뷰를 통해 패스워드 정책 확인

1) 패스워드 복잡도 설정을 만족하고 있는지 확인

조치 방법

■ 기존 계정의 경우, ALTER 명령어를 통해 패스워드 설정

1) postgres=# ALTER ROLE 계정명 WITH PASSWORD '설정할 비밀번호';

```
postgres=# ALTER ROLE test1 WITH PASSWORD '5678';
ALTER ROLE
postgres=#
```

■ 새로운 계정의 경우, CREATE 명령어를 통해 패스워드 설정

2) postgres=# create user 계정명 password '설정할 비밀번호';

```
postgres=# create user test3 password '1234';
CREATE ROLE
postgres=#
postgres=#
```

※ 패스워드 복잡도를 만족하도록 패스워드 설정
영문(대문자, 소문자), 숫자, 특수문자 조합 중 3가지 조합 8자리 이상 또는 2가지 조합 10자리 이상을 만족해야 함

■ 불필요한 사용자 계정 제거

1) postgres=# DROP USER 계정명;

불필요한 권한 제거

항목설명

PostgreSQL의 Superuser는 모든 권한을 무시하고 작업을 수행할 수 있으며 Create Role은 계정을 생성하고 권한을 부여할 수 있다. 불필요한 계정에 Superuser, Create Role이 설정되어 있는 경우 비인가자가 데이터베이스에 접근하여 계정 생성 및 삭제, 데이터 열람, 수정 등을 할 위험이 존재한다.

진단 기준

양호

Superuser, Create Role이 적절한 계정에 설정된 경우

취약

Superuser, Create Role이 적절하지 않은 계정에 설정된 경우

진단 방법

■ psql 접속 후, 명령어로 사용자 계정 목록 조회

1) postgres=# \du

```
postgres-# \du
                                   List of roles
 Role name |                         Attributes                         | Member of
-----------+------------------------------------------------------------+-----------
 postgres  | Superuser, Create role, Create DB, Replication, Bypass RLS | {}
 test      | Superuser, Create role                                     | {}
 test1     |                                                            | {}
 test2     |                                                            | {}
 test3     |                                                            | {}

postgres-#
```

※ default로 생성되는 postgres 계정은 기본적으로 Superuser, Create Role 설정 존재함

조치 방법

■ 명령어를 통해 불필요한 권한을 제거

1) postgres=# ALTER ROLE 계정명 WITH NOSUPERUSER NOCREATEROLE;

```
postgres=# ALTER ROLE test WITH NOSUPERUSER NOCREATEROLE;
ALTER ROLE
postgres=#
postgres=#
```

■ 권한 제거 확인

1) postgres=# \du

```
postgres=# \du
                                   List of roles
 Role name |                         Attributes                         | Member of
-----------+------------------------------------------------------------+-----------
 postgres  | Superuser, Create role, Create DB, Replication, Bypass RLS | {}
 test      |                                                            | {}
 test1     |                                                            | {}
 test2     |                                                            | {}
 test3     |                                                            | {}
```

Public schema 사용 제한

항목설명

PosgreSQL에서 DB를 생성하는 경우에 Public Schema가 자동으로 생성된다. 별도의 schema를 생성하지 않고 table을 만드는 경우, 기본적으로 Public Schema 안에 생성된다. Public Schema는 모든 개체에서 접근이 가능하므로 정보 유출, 자원 고갈 등의 위험이 존재한다.

진단 기준

양호

Public Schema에 소유주와 특정 계정만이 접근 가능한 경우

취약

Public Schema에 모든 계정이 접근 가능한 경우

진단 방법

■ psql 접속 후, 명령어로 확인

1) postgres=# \dn+

```
postgres=# \dn+
                          List of schemas
  Name  |  Owner   |  Access privileges   |      Description
--------+----------+----------------------+------------------------
 public | postgres | postgres=UC/postgres+| standard public schema
        |          | =UC/postgres         |
(1 row)

postgres=#
```

※ +뒤의 '=UC/postgres'가 존재한다면 모든 계정에서 Public Schema에 접근이 가능하다는 의미

조치 방법

■ 명령어를 통해 Public Schema에 public 권한 제거 (예시)

1) postgres=# REVOKE all ON schema public from PUBLIC;

```
postgres=# REVOKE all ON schema public from PUBLIC;
REVOKE
postgres=#
```

■ 모든 계정 접근 제한 확인

1) postgres=# \dn+

```
postgres=# \dn+
                          List of schemas
  Name  |  Owner   |  Access privileges   |      Description
--------+----------+----------------------+------------------------
 public | postgres | postgres=UC/postgres | standard public schema
(1 row)

postgres=#
```

비고

※ PostgreSQL v15 이상에서는 postgres가 아닌 Public Schema에 현재 데이터베이스의 실제 소유자를 포함하는 pg_database_owner 접근 권한이 디폴트로 부여됨

IP 접근 제한 설정

항목설명

비인가된 IP가 데이터베이스에 접근이 가능할 경우, 데이터베이스의 데이터가 유출 및 변경될 가능성이 있으므로 인가된 IP만 접근이 가능하도록 설정해야 한다.

진단 기준

양호
인가된 IP만 접근이 가능하도록 설정된 경우

취약
비인가된 IP가 접근이 가능하도록 설정된 경우

진단 방법

■ postgresql.conf 확인

1) # cat /[postgresql 설치 디렉터리/postgresql.conf] | grep listen_address

```
root@ubuntu:/etc/postgresql/14/main# cat postgresql.conf | grep listen_address
#listen_addresses = 'localhost'         # what IP address(es) to listen on;
root@ubuntu:/etc/postgresql/14/main#
```

※ default : #listen_address = 'localhost'

■ pg_hba.conf 확인

1) # cat /[postgresql 설치 디렉터리/pg_hba.conf] | grep –v "#"

```
root@ubuntu:/etc/postgresql/14/main# cat pg_hba.conf | grep -v "#"


local   all             postgres                                peer


local   all             all                                     peer
host    all             all             127.0.0.1/32            scram-sha-256
host    all             all             ::1/128                 scram-sha-256
local   replication     all                                     peer
host    replication     all             127.0.0.1/32            scram-sha-256
host    replication     all             ::1/128                 scram-sha-256
root@ubuntu:/etc/postgresql/14/main#
```

조치 방법

■ postgresql.conf 수정

1) 인가된 IP 주소로 수정 (예시)

```
# - Connection Settings -

listen_addresses = '192.168.153.138'          # what IP address(es) to listen on;
                                    # comma-separated list of addresses;
                                    # defaults to 'localhost'; use '*' for all
                                    # (change requires restart)
port = 5432                         # (change requires restart)
```

2) 적용 후, PostgreSQL 재시작

```
# systemctl restart postgresql.service
```

■ pg_hba.conf 수정

1) 인가된 IP 주소로 수정

```
# Database administrative login by Unix domain socket
local   all             postgres                                peer

# TYPE  DATABASE        USER            ADDRESS                 METHOD

# "local" is for Unix domain socket connections only
local   all             all                                     peer
# IPv4 local connections:
host    all             all             127.0.0.1/32            scram-sha-256
# IPv6 local connections:
host    all             all             ::1/128                 scram-sha-256
# Allow replication connections from localhost, by a user with the
# replication privilege.
local   replication     all                                     peer
host    replication     all             127.0.0.1/32            scram-sha-256
host    replication     all             ::1/128                 scram-sha-256
```

2) 적용 후, PostgreSQL 재시작

```
# systemctl restart postgresql.service
```

비고

※ PostgreSQL이 설치된 서버(Linux, Windwos 등)의 IP 접근 통제 정책을 같이 확인 필요

※ postgresql.conf, pg_hba.conf 두 설정 파일이 연계되어 있으므로 한 설정에 오류가 발생하지 않도록 충분한 테스트 후 DB에 적용 필요

안전한 인증 방식 설정

항목설명

PostgreSQL에서는 다양한 인증 방식을 지원하지만 안전하지 않은 인증 방식이 존재하므로 cert, pam, scram_sha_256등 안전한 인증 방식을 적용해야 한다.

진단 기준

양호
안전한 인증 방식이 적용된 경우

취약
안전한 인증 방식이 적용되지 않은 경우

진단 방법

■ pg_hba.conf 확인

1) # cat [postgresql 설치 디렉터리/pg_hba.conf] | grep –v “#”

```
root@ubuntu:/etc/postgresql/14/main# cat pg_hba.conf | grep -v "#"


local   all             postgres                                peer


local   all             all                                     peer
host    all             all             127.0.0.1/32            scram-sha-256
host    all             all             ::1/128                 scram-sha-256
local   replication     all                                     peer
host    replication     all             127.0.0.1/32            scram-sha-256
host    replication     all             ::1/128                 scram-sha-256
root@ubuntu:/etc/postgresql/14/main#
```

조치 방법

■ pg_hba.conf 수정

1) METHOD 필드 안전한 인증 방식으로 수정

```
# Database administrative login by Unix domain socket
local   all             postgres                                peer

# TYPE  DATABASE        USER            ADDRESS                 METHOD

# "local" is for Unix domain socket connections only
local   all             all                                     peer
# IPv4 local connections:
host    all             all             127.0.0.1/32            scram-sha-256
# IPv6 local connections:
host    all             all             ::1/128                 scram-sha-256
# Allow replication connections from localhost, by a user with the
# replication privilege.
local   replication     all                                     peer
host    replication     all             127.0.0.1/32            scram-sha-256
host    replication     all             ::1/128                 scram-sha-256
```

안전한 암호화 알고리즘 사용

항목설명

SHA-1 암호화 알고리즘의 취약점이 발견됨에 따라 SHA-1 이하의 암호화 알고리즘을 사용하지 않고 SHA-256 이상의 안전한 암호화 알고리즘을 사용해야 한다.

진단 기준

양호

SHA-256 이상의 암호화 알고리즘을 사용하는 경우

취약

SHA-256 이상의 암호화 알고리즘을 사용하지 않는 경우

진단 방법

■ psql 접속 후, 계정별 암호화 알고리즘 확인

1) postgres=# select usename, passwd from pg_shadow;

```
postgres=# select usename, passwd from pg_shadow;
 usename  |                                          passwd
----------+------------------------------------------------------------------------------------------
 postgres |
 test2    |
 test3    | SCRAM-SHA-256$4096:LuJddHngmewGRNMfdpffkQ==$bEzFkFisF70sEB58UhBib0fgUKeABwBvfCdljb8KYrI
 test1    | SCRAM-SHA-256$4096:b1eRZPV9UCsIC1xFi+yOlQ==$ZneV72Ao5tgI2yRKjI0XRq6EzpqI+e6vwFqk+roBbLI
 test     |
(5 rows)

postgres=#
```

조치 방법

■ 명령어를 통해 안전한 암호화 알고리즘 적용

1) user 생성 시 적용
postgres=# CREATE user 계정명 PASSWORD '설정할 패스워드';

2) 기존 user 적용
postgres=# AlTER user 계정명 WITH PASSWORD '설정할 패스워드';

※ default 설정으로 SCRAM-SHA-256 암호화 알고리즘이 적용
※ peer : 로컬에서만 연결이 가능하며 OS에서 클라이언트의 OS 사용자 이름을 얻고 요청한 데이터베이스 사용자 이름과 일치하는지 확인하는 인증 방식

데이터 디렉터리 권한 설정

항목설명

일반 사용자가 PostgreSQL 데이터 디렉터리에 임의의 파일을 생성, 삭제, 변경이 가능하다면 중요 파일의 삭제, 백도어 삽입 등이 가능하므로 침해 사고가 발생할 위험이 존재한다.

진단 기준

양호

데이터 디렉터리 접근 권한이
700(drwx------) 이하로 설정된 경우

취약

데이터 디렉터리 접근 권한이
700(drwx------) 초과로 설정된 경우

진단 방법

■ PostgreSQL 데이터 디렉터리 접근 권한 확인 (예시)

1) # ls –ld [PostgreSQL [데이터 디렉터리]

```
root@ubuntu:/var/lib/postgresql/14/main/base# ls -ld /var/lib/postgresql/14/main/base
drwx------ 6 postgres postgres 4096 11월  29 00:20 /var/lib/postgresql/14/main/base
root@ubuntu:/var/lib/postgresql/14/main/base#
```

조치 방법

■ 명령어를 통해 접근 권한 변경

1) # chmod 700 [PostgreSQL 데이터 디렉터리]

환경설정 파일 권한 설정

항목설명

PostgreSQL 환경설정 파일이 비인가자에 의해 변경된다면 시스템 장애가 발생할 수 있으므로 환경설정 파일의 접근 권한을 비인가자가 접근할 수 없도록 설정해야 한다.

진단 기준

양호

환경설정 파일의 소유자 및 그룹이 별도의 계정의 소유이며 파일의 접근 권한이 600(-rw-------) 이하로 설정된 경우

취약

환경설정 파일의 소유자 및 그룹이 별도의 계정의 소유가 아니며 파일의 접근 권한이 600(-rw-------) 초과로 설정된 경우

진단 방법

■ 환경설정 파일 접근 권한 확인 (예시)

1) # ls –al [PostgreSQL 환경설정 파일]

```
root@ubuntu:/etc/postgresql/14/main# ls -al
합 계  68
drwxr-xr-x 3 postgres postgres  4096 11월  29 01:18 .
drwxr-xr-x 3 postgres postgres  4096 11월  28 23:33 ..
drwxr-xr-x 2 postgres postgres  4096 11월  28 23:33 conf.d
-rw-r--r-- 1 postgres postgres   315 11월  28 23:33 environment
-rw-r--r-- 1 postgres postgres   143 11월  28 23:33 pg_ctl.conf
-rw-r----- 1 postgres postgres  5002 11월  28 23:33 pg_hba.conf
-rw-r----- 1 postgres postgres  1636 11월  28 23:33 pg_ident.conf
-rw-r--r-- 1 postgres postgres 29053 11월  28 23:33 postgresql.conf
-rw-r--r-- 1 postgres postgres   317 11월  28 23:33 start.conf
```

조치 방법

■ 명령어를 통해 접근 권한 변경

1) # chmod 600 [PostgreSQL 환경설정 파일]

로그 활성화

항목설명

로그를 정기적으로 분석하여 침입 유무를 파악하고 침입 시도 의심 사례를 분석하여 사전에 해당 장비에 대한 접근을 차단하는 등 체계적인 로그 관리 작업이 이루어져야 한다.

진단 기준

양호

로그가 활성화되어 있는 경우

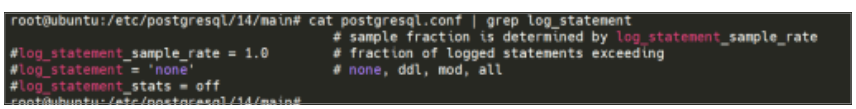
취약

로그가 비활성화되어 있는 경우

진단 방법

■ 로그 활성화 확인

1) # cat [PostgreSQL [PostgreSQL 환경설정 파일] | grep log_statement



※ default : log_statement = 'none'

조치 방법

■ 명령어를 통해 접근 권한 변경 (예시)

1) # chmod 600 [PostgreSQL 환경 설정 파일]

비고

수준	설명
none	쿼리를 남기지 않는 수준
ddl	Table Create나 Drop과 같이 구조 변경을 하는 쿼리 이상을 로그로 남기는 수준
mod	Data Record 단위로 변경하는 쿼리 이상을 로그로 남기는 수준
all	모든 쿼리를 로그로 남기는 수준

최신 보안 패치 적용

항목설명

최신 보안 패치가 적용되어 있지 않을 경우, 비인가자가 데이터베이스에 보안 취약점을 이용하여 침해 사고를 일으킬 수 있다.

진단 기준

양호

보안 취약점이 존재하지 않는 버전을 사용 중인 경우

취약

보안 취약점이 존재하는 버전을 사용 중인 경우

진단 방법

■ 설치 버전 확인

1) postgres=# select version();

```
postgres=# select version();
                                                  version
-----------------------------------------------------------------------------------------------------------------------------
 PostgreSQL 14.9 (Ubuntu 14.9-0ubuntu0.22.04.1) on x86_64-pc-linux-gnu, compiled by gcc (Ubuntu 11.4.0-1ubuntu1~22.04) 11.4.0, 64-bit
(1 row)

postgres=#
```

조치 방법

■ 보안 패치 적용

1) 보안 취약점이 존재하지 않는 버전으로 보안 패치를 적용해야 함

※ 최신 버전을 사용하도록 권고하고 있으나 시스템 운영상 적용이 어려운 경우 최신이 아닌 취약점이 존재하지 않는 버전도 허용하고 있음

비고

※ 보안 패치를 적용할 경우, 시스템 영향도를 파악하여 충분한 테스트 후 적용 권고

2.16.

Cubrid

2.16. Cubrid

계정 관리(2개 항목), 보안 설정(5개 항목), 패치 및 로그 관리(2개 항목) 총 3개 영역에서 9개 항목으로 구성된다.

[표 16] Cubrid 진단 체크리스트

구분	진단 항목
가. 계정 관리	불필요한 계정 제거
	취약한 패스워드 사용 제한
나. 보안 설정	타 사용자에 권한 부여 옵션 사용 제한
	root 권한으로 서버 구동 제한
	환경 설정 파일 접근 권한
	demodb 제거
	안전한 암호화 알고리즘 사용
라. 패치 및 로그 관리	로그 기능 활성화
	최신 보안 패치 적용

불필요한 계정 제거

항목설명

데이터베이스 계정 중 인가되지 않은 계정, 퇴직자 계정, 테스트 계정, 용도를 모르는 계정 등 실질적으로 업무에 사용하지 않는 불필요한 계정들이 존재하는 경우 비인가자가 쉽게 데이터베이스에 접속하여 데이터를 열람, 삭제, 수정 등을 할 위험이 있다.

진단 기준

양호

테스트 계정, 용도를 모르는 계정 등 업무에 불필요한 계정이 존재하지 않는 경우

취약

테스트 계정, 용도를 모르는 계정 등 업무에 불필요한 계정이 존재하는 경우

진단 방법

■ 데이터베이스 사용자 계정 목록 확인

1) csql〉 SELECT name, password FROM db_user;

```
csql> SELECT name, password FROM db_user;

=== <Result of SELECT Command in Line 3> ===

  name                  password
============================================
  'DBA'                 NULL
  'PUBLIC'              NULL
  'TESTER'              db_password
  'WORK_TEST'           NULL

4 rows selected. (0.007908 sec) Committed. (0.000439 sec)

1 command(s) successfully processed.
```

조치 방법

■ 불필요한 계정 제거

1) csql〉 DROP USER “사용자 계정명“;

취약한 패스워드 사용 제한

항목설명

데이터베이스 사용자 계정의 패스워드가 계정명과 동일하거나, default 패스워드를 사용하는 경우 비인가자가 쉽게 데이터베이스에 접근할 수 있으며 접근 시, 데이터베이스 수정, 삭제가 가능하므로 패스워드 설정 시 패스워드 복잡도를 만족해야 한다.

진단 기준

양호

계정명과 동일한 패스워드, default 패스워드를 사용하지 않으며 패스워드 복잡도 설정을 만족하는 경우

취약

계정명과 동일한 패스워드, default 패스워드를 사용하거나 패스워드 복잡도 설정을 만족하지 않는 경우

진단 방법

■ 사용자 계정 패스워드 사용 여부 확인

1) csql〉 SELECT name, password FROM db_user;

2) csql〉 SELECT * FROM db_password;

```
csql> SELECT * FROM db_password;

=== <Result of SELECT Command in Line 2> ===

  password
======================
  'D4045599F602EAB6FD602AC76B0DACBFAADD13630335E951F097AF3900E9DE176B6DB28512F2E000B9D04FBA5133E8B1C6E8DF59083A8AB9D60BE4B97CC9E81DB'

1 row selected. (0.000147 sec) Committed. (0.000012 sec)

1 command(s) successfully processed.
```

조치 방법

■ 사용자 계정 패스워드 변경

1) csql〉 ALTER USER “사용자 계정명” PASSWORD ‘변경 패스워드’;

```
csql> ALTER USER TESTER PASSWORD '12345';
Execute OK. (0.002387 sec) Committed. (0.002972 sec)

1 command(s) successfully processed.
csql>
```

※ 패스워드 복잡도 : 영문(대문자, 소문자), 숫자, 특수문자 조합 중 2가지 조합 10자리 이상, 3가지 조합 8자리 이상

타 사용자에 권한 부여 옵션 사용 제한

항목설명

with grant option과 함께 권한을 받은 사용자는 해당 권한을 다른 사용자에게도 권한을 부여할 수 있다. 그러므로 사용 권한 부여는 DBA만 가능하도록 제한해야 한다.

진단 기준

양호

grant_priv권한이 적절한 사용자에게 부여되어 있는 경우

취약

grant_priv권한이 적절한 사용자에게 부여되어 있지 않은 경우

진단 방법

■ grant_priv 권한을 부여받은 사용자 계정 조회

1) csql〉 SELECT * FROM db_auth WHERE is_grantable='YES';

```
csql> SELECT * FROM db_auth WHERE is_grantable='YES';

=== <Result of SELECT Command in Line 4> ===

There are no results.
0 row selected. (0.039999 sec) Committed. (0.000367 sec)

1 command(s) successfully processed.
```

조치 방법

■ 권한 부여 해제

1) csql〉 REVOKE 특정 권한 on 테이블 FROM 계정;

■ with grant option을 제외하고 권한 부여

1) csql〉 GRANT 특정 권한 테이블 FROM 계정;

root 권한으로 서버 구동 제한

항목설명

root 권한은 데이터베이스의 최고 상위 권한으로 소수의 관리자만이 제한적으로 사용해야 한다.

진단 기준

양호

데몬이 root 계정 또는 root 권한으로 구동되고 있지 않은 경우

취약

데몬이 root 계정 또는 root 권한으로 구동되고 있는 경우

진단 방법

■ 실행 중인 프로세스 확인

1) # ps -ef | egrep 'cub_master|cub_broker|cub_manager' | egrep -v egrep

```
root@ubuntu:~# ps -ef | egrep 'cub_master|cub_broker|cub_manager' | egrep -v egrep
[redacted]  2478     1  0 11:22 pts/0    00:00:00 cub_master
[redacted]  2715     1  0 11:22 ?        00:00:14 cub_broker
[redacted]  2726     1  0 11:22 ?        00:00:14 cub_broker
[redacted]  2741     1  0 11:22 ?        00:00:01 cub_manager start
root       13042 13008  0 13:22 pts/0    00:00:00 grep -E --color=auto cub_master|cub_broker|cub_manager
```

※ cub_master, cub_broker, cub_manager 데몬이 root 또는 root 권한으로 구동되었는지 확인

조치 방법

■ 사용자 계정으로 데몬 실행

1) 삭제 후, cubrid 계정으로 재설치

2) 같은 DB를 생성 후에 언로드 / 로드를 통해 기존 데이터를 이관

환경 설정 파일 접근 권한

항목설명

Cubrid 중요 파일 중 하나인 환경설정 파일이 비인가자에 의해 변경된다면 시스템 장애를 발생시킬 수 있으므로 비인가자의 접근을 제한해야 한다.

진단 기준

양호

환경 설정 파일 접근 권한이 640(-rw-r-----) 이하로 설정된 경우

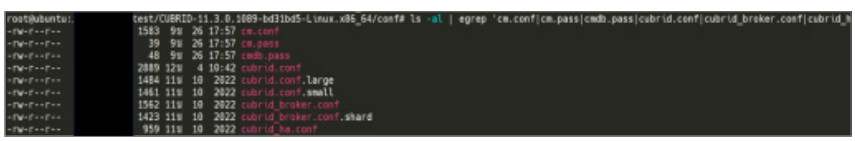
취약

환경 설정 파일 접근 권한이 640(-rw-r-----) 이하로 설정되지 않은 경우

진단 방법

■ 환경 설정 파일 접근 권한 확인

1) # ls -al | egrep 'cm.conf|cm.pass|cmdb.pass|cubrid.conf|cubrid_broker.conf|cubrid_ha.conf'



※ 환경 설정 파일 : cm.conf, cm.pass, cmdb.pass, cubrid.conf, cubrid_broker.conf, cubrid_ha.conf

조치 방법

■ 환경 설정 파일 접근 권한 변경

1) # chmod 640 [환경 설정 파일]

demodb 제거

항목설명

Cubrid 설치 시 자동으로 생성되는 demodb 데이터베이스가 구동 중인 경우, 불필요한 자원을 낭비하게 되며 해당 데이터베이스를 사용하여 데이터를 저장한 경우에 공격자에 의해 해당 데이터베이스의 데이터가 탈취될 위험이 존재한다.

진단 기준

양호

demodb가 존재하지 않는 경우

취약

demodb가 존재하거나 구동 중인 경우

진단 방법

■ demodb 운영 여부 확인

1) # cub_common –P

```
[redacted]@ubuntu:~$ cub_commdb -P
Server testdb (rel 11.3, pid 2481)
```

■ demodb 존재 확인

1) # cat [Cubrid 설치 디렉터리]/databases.txt | grep demodb

```
[redacted]@ubuntu:~/test/CUBRID-11.3.0.1089-bd31bd5-Linux.x86_64/databases$ cat databases.txt | grep demodb
[redacted]@ubuntu:~/test/CUBRID-11.3.0.1089-bd31bd5-Linux.x86_64/databases$
```

※ demodb가 존재하지 않으면 출력되지 않음

조치 방법

■ demodb 제거

1) # cubrid deletedb demodb

안전한 암호화 알고리즘 사용

항목설명

패스워드를 암호화할 때 취약점이 발견된 SHA-1 암호화 알고리즘을 사용하지 말고 SHA-256 이상의 안전한 암호화 알고리즘을 사용하여 암호화해야 한다.

진단 기준

양호

SHA-256 이상의 암호화 알고리즘을 사용하고 있는 경우

취약

SHA-256 이상의 암호화 알고리즘을 사용하고 있지 않은 경우

진단 방법

■ 사용자 계정 패스워드 조회

1) csql〉 SELECT * FROM db_password;

```
csql> SELECT * FROM db_password;

=== <Result of SELECT Command in Line 2> ===

  password
======================
  '3627909A29C313B1A071EC27F7C9CA97726182AED29A7DDD2E54353322CFB30ABB9E3A6DF2AC2C20FE23436311D678564D0C

1 row selected. (0.009484 sec) Committed. (0.000025 sec)

1 command(s) successfully processed.
```

조치 방법

■ SHA-256 이상의 암호화 알고리즘 사용

※ Cubrid v9.3.7 이상부터 패스워드 암호화 알고리즘 SHA-512 적용

로그 기능 활성화

항목설명

로그 파일을 남김으로써 데이터베이스의 변경 이력들을 관리할 수 있으며 침해 사고 및 장애 발생 시 로그 자료를 통해 원인 분석을 할 수 있다.

진단 기준

양호

로그 기능이 활성화되어 있는 경우

취약

로그 기능이 활성화되어 있지 않은 경우

진단 방법

■ 로그 기능 활성화 확인

1) # cat cubrid_broker.conf | grep 'SQL_LOG' -B 8

```
SERVICE                 =ON
SSL                     =OFF
BROKER_PORT             =30000
MIN_NUM_APPL_SERVER     =5
MAX_NUM_APPL_SERVER     =40
APPL_SERVER_SHM_ID      =30000
LOG_DIR                 =log/broker/sql_log
ERROR_LOG_DIR           =log/broker/error_log
SQL_LOG                 =ON
```

조치 방법

■ 로그 기능 활성화

1) # vi [cubrid 설치 디렉터리]/conf/cubrid_broker.conf
SQL_LOG = ON으로 설정

최신 보안 패치 적용

항목설명

취약점이나 버그가 존재하는 버전을 계속 사용하면 공격자가 해당 버전의 취약점 및 버그를 이용하여 침해 사고를 일으킬 가능성이 있으므로 최신 보안 패치를 적용해야 한다.

진단 기준

양호
최신 보안 패치가 적용되어 있는 경우

취약
최신 보안 패치가 적용되어 있지 않은 경우

진단 방법

■ Cubrid 버전 확인

1) $ cubrid_rel

```
CUBRID 11.3 (11.3.0.1089-bd31bd5) (64bit release build for Linux) (Sep 26 2023 17:56:35)
```

조치 방법

■ 보안 패치 적용

1) 보안 취약점이 존재하지 않는 버전으로 보안 패치를 적용해야 함

※ 최신 버전을 사용하도록 권고하고 있으나 시스템 운영상 적용이 어려운 경우 최신이 아닌 취약점이 존재하지 않는 버전도 허용하고 있음

비고

※ 보안 패치를 적용할 경우, 시스템 영향도를 파악하여 충분한 테스트 후 적용 권고

2.17.

CouchDB

2.17. CouchDB

계정 관리(2개 항목), 보안 설정(6개 항목), 패치 및 로그 관리(2개 항목) 총 3개 영역에서 10개 항목으로 구성된다.

[표 17] CouchDB 진단 체크리스트

구분	진단 항목
가. 계정 관리	불필요한 계정 제거
	Default 관리자 계정 이름 바꾸기
나. 보안 설정	패스워드 암호화 알고리즘 확인
	IP 접근 통제
	SSL 활성화
	세션 타임아웃 설정
	데이터베이스 사용자 정의 설정
	환경설정 파일 권한 관리
다. 패치 및 로그 관리	로그 활성화
	최신 보안 패치 적용

불필요한 계정 제거

항목설명

DB 관리나 운용에 사용하지 않는 불필요한 계정이 존재할 경우 비인가자가 불필요한 계정을 통해 DB에 접근하여 데이터를 열람, 삭제, 수정할 위험이 존재한다.

진단 기준

양호

계정 정보를 확인하여 불필요한 계정이 없는 경우

취약

인가되지 않은 계정, 퇴직자 계정, 테스트 계정 등 불필요한 계정이 존재하는 경우

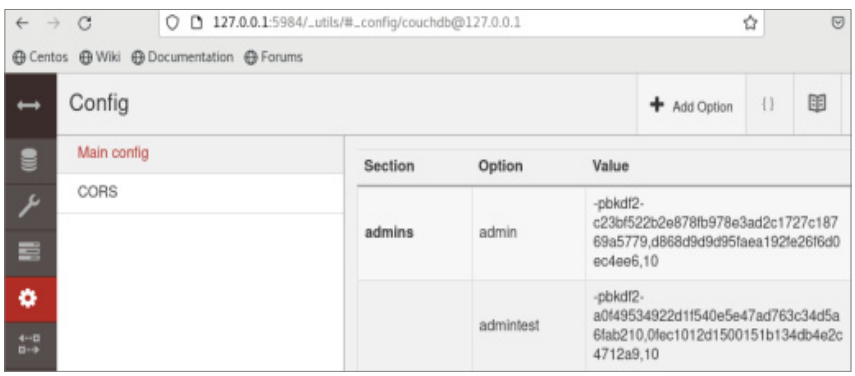
진단 방법

■ 관리자 계정 확인

1) http://127.0.0.1:5984/_utils/에 접속

2) 관리자 계정 로그인 후 Config 메뉴 선택

3) admins Section에서 관리자 계정 확인

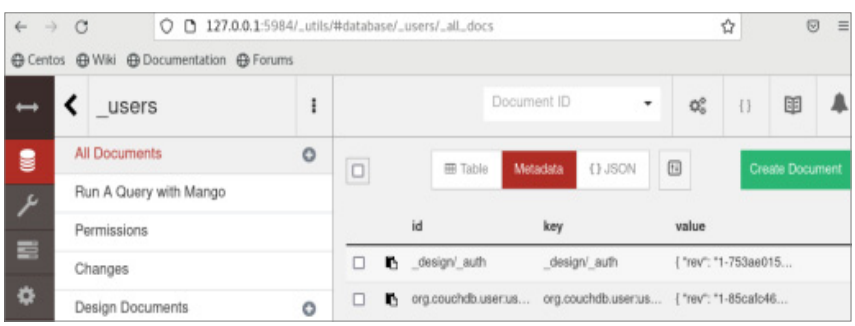


■ 사용자 계정 확인

1) http://127.0.0.1:5984/_utils/에 접속

2) 관리자 계정 로그인 후 Databases 메뉴 선택 후 _users 선택

3) 생성된 사용자 Document 확인



조치 방법

■ 불필요한 관리자 계정 삭제

1) http://127.0.0.1:5984/_utils/에 접속

2) 관리자 계정 로그인 후 Config 메뉴 선택

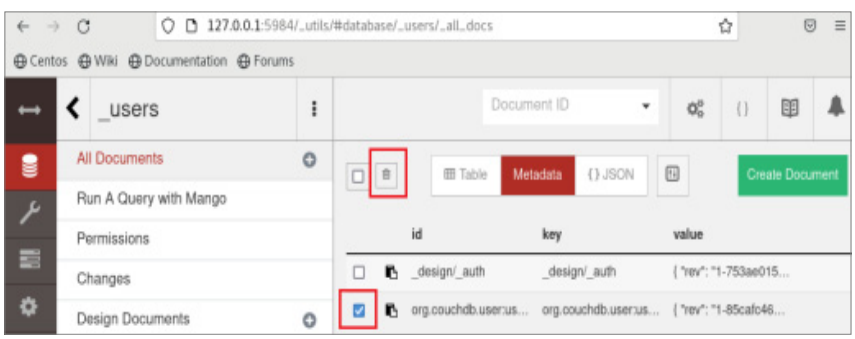
3) admins Section에서 불필요한 관리자 계정 제거

■ 불필요한 사용자 계정 삭제

1) http://127.0.0.1:5984/_utils/에 접속

2) 관리자 계정 로그인 후 Databases 메뉴 선택 후 _users 선택

3) 불필요한 사용자 Document 체크 후 삭제



Default 관리자 계정 이름 바꾸기

항목설명

관리자 계정은 모든 시스템 리소스에 대한 권한을 가지고 있으며, Default 관리자 계정 사용 시 공격자가 예측하기 쉽고 이 계정이 탈취되거나 악용될 경우 시스템 전체에 대한 치명적인 피해가 발생할 수 있는 위험이 존재한다.

진단 기준

양호

Default 관리자 계정을 변경하여 사용하는 경우

취약

Default 관리자 계정을 변경하지 않고 사용하는 경우

진단 방법

■ WEB에서 관리자 계정 확인

1) http://127.0.0.1:5984/_utils/에 접속

2) 관리자 계정 로그인 후 Config 메뉴 선택

3) admins Section에서 관리자 계정 확인(Default 관리자 계정 : admin)

■ local.ini 파일에서 관리자 계정 확인

```
[admins]
;admin = mysecretpassword
admin = -pbkdf2-c23bf522b2e878fb978e3ad2c1727c18769a5779,d868d9d9d95faea192fe26f6d0ec4ee6,10
```

조치 방법

■ local.ini 파일에서 기본 관리자 계정 변경

1) 관리자 계정으로 추측할 수 없는 계정명 사용

```
[admins]
;admin = mysecretpassword
couchdbadmin = -pbkdf2-c23bf522b2e878fb978e3ad2c1727c18769a5779,d868d9d9d95faea192fe26f6d0ec4ee6,10
```

패스워드 암호화 알고리즘 확인

항목설명

패스워드를 취약한 암호 알고리즘으로 암호화 할 경우, 공격자가 사용자 계정의 패스워드를 해독하여, 데이터베이스에 접근 가능한 계정을 탈취할 수 있다.

진단 기준

양호

암호화 알고리즘으로 PBKDF2 및 안전한 암호화 알고리즘이 적용되어 있는 경우

취약

암호화 알고리즘으로 안전하지 않은 암호화 알고리즘이 적용되어 있는 경우

진단 방법

■ 관리자 계정에 적용된 암호화 알고리즘 확인

1) http://127.0.0.1:5984/_utils/에 접속

2) 관리자 계정 로그인 후 Config 메뉴 선택

3) admins Section에서 관리자 계정에 적용된 암호화 알고리즘 확인

■ 일반 사용자 계정에 적용된 암호화 알고리즘 확인

1) http://127.0.0.1:5984/_utils/에 접속

2) 관리자 계정 로그인 후 Databases 메뉴 선택 후 _users 선택

3) 생성된 사용자 Document 선택 후 password_scheme 설정값 확인

조치 방법

■ PBKDF2, bcrypt, Scrypt 등 안전한 암호화 알고리즘 적용

IP 접근 통제

항목설명

인가된 IP만 접근 가능하도록 설정되어 있지 않은 경우, 비인가된 사용자가 해당 데이터베이스에 접근하여 보안 문제가 발생할 위험이 존재한다.

진단 기준

양호

인가된 IP만 접근 가능하도록 설정되어 있는 경우

취약

인가된 IP만 접근 가능하도록 설정되어 있지 않은 경우

진단 방법

■ WEB에서 bind_address 설정 확인

1) http://127.0.0.1:5984/_utils/에 접속

2) 관리자 계정 로그인 후 Config 메뉴 선택

3) chttpd Section에서 bind_address 설정값 확인

■ local.ini 파일에서 bind_address 설정 확인

```
[chttpd]
;port = 5984
;bind_address = 127.0.0.1


; Options for the MochiWeb HTTP server.
;server_options = [{backlog, 128}, {acceptor_pool_size, 16}]

; For more socket options, consult Erlang's module 'inet' man page.
;socket_options = [{sndbuf, 262144}, {nodelay, true}]
```

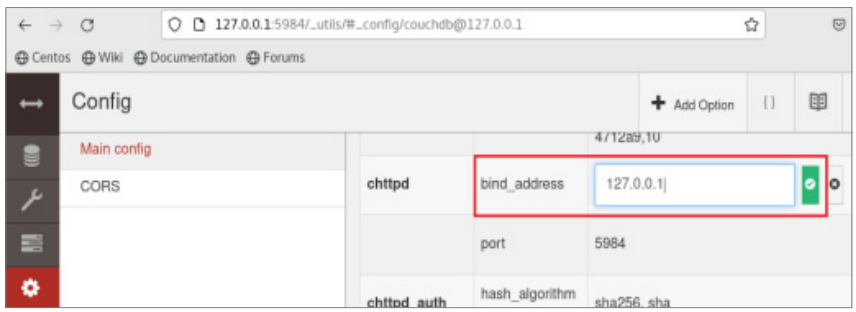
조치 방법

■ WEB에서 bind_address 설정 변경

1) http://127.0.0.1:5984/_utils/에 접속

2) 관리자 계정 로그인 후 Config 메뉴 선택

3) bind_address 설정값에 인가된 IP 설정



■ local.ini 파일에서 bind_address 설정 추가

```
[chttpd]
;port = 5984
;bind_address = 127.0.0.1


; Options for the MochiWeb HTTP server.
;server_options = [{backlog, 128}, {acceptor_pool_size, 16}]

; For more socket options, consult Erlang's module 'inet' man page.
;socket_options = [{sndbuf, 262144}, {nodelay, true}]
bind_address = 192.168.1.190
```

SSL 활성화

항목설명

SSL을 사용하지 않을 경우 데이터는 암호화되지 않아 공격자가 중간에서 네트워크를 가로채거나 도청할 수 있으며, 더 나아가 데이터가 평문으로 전송되어 중간에서 변경될 우려가 있어 데이터의 정확성이 훼손될 위험이 존재한다.

진단 기준

양호

SSL이 활성화되어 있는 경우

취약

SSL이 비활성화되어 있는 경우

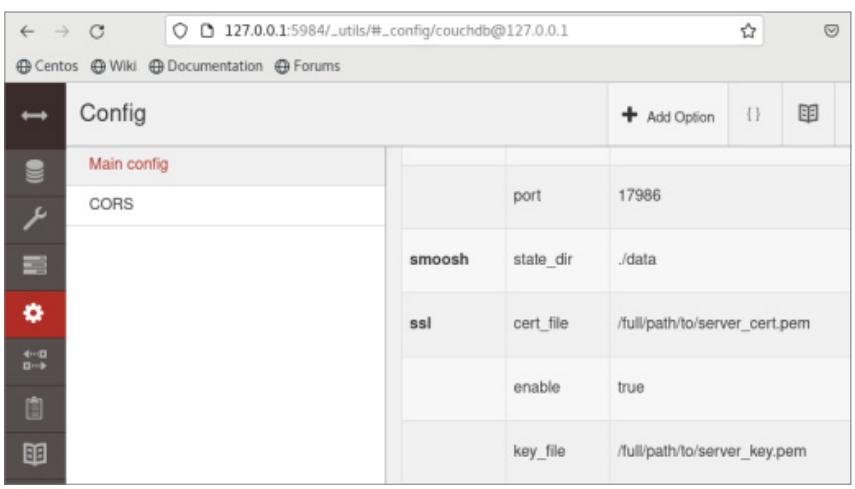
진단 방법

■ WEB에서 ssl 설정 확인

1) http://127.0.0.1:5984/_utils/에 접속

2) 관리자 계정 로그인 후 Config 메뉴 선택

3) ssl Section에서 enable 설정값 확인



■ local.ini 파일에서 ssl 설정 확인

```
[ssl]
;enable = true
;cert_file = /full/path/to/server_cert.pem
;key_file = /full/path/to/server_key.pem
;password = somepassword
```

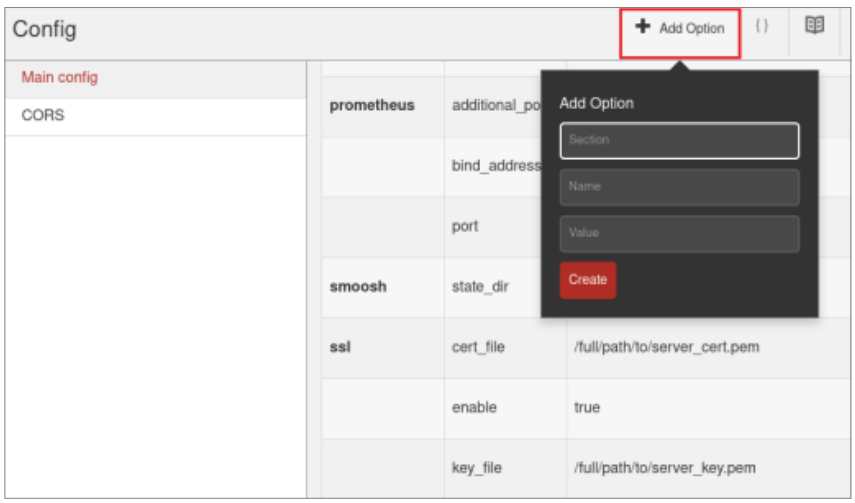
조치 방법

■ WEB에서 ssl 설정 추가

1) http://127.0.0.1:5984/_utils/에 접속

2) 관리자 계정 로그인 후 Config 메뉴 선택

3) Add Option 클릭 후 ssl Section 추가



※ cert_file, key_file 파일 Value에는 해당 파일의 경로를 입력해야 한다.

■ local.ini 파일에서 ssl 설정 추가

1) 주석 해제 또는 cert_file, key_file, enable 설정 추가

```
[ssl]
;enable = true
;cert_file = /full/path/to/server_cert.pem
;key_file = /full/path/to/server_key.pem
;password = somepassword
```

세션 타임아웃 설정

항목설명

사용자의 세션이 로그인 후에도 일정 기간 동안 만료되지 않으면 공격자가 해당 세션을 탈취하여 무단으로 사용자 계정에 접근할 수 있으며 불필요하게 세션이 유지되는 동안 사용자의 정보가 노출될 위험이 존재한다.

진단 기준

양호

timeout 설정이 600(초) 이하인 경우

취약

timeout 설정이 600(초) 이하가 아닌 경우

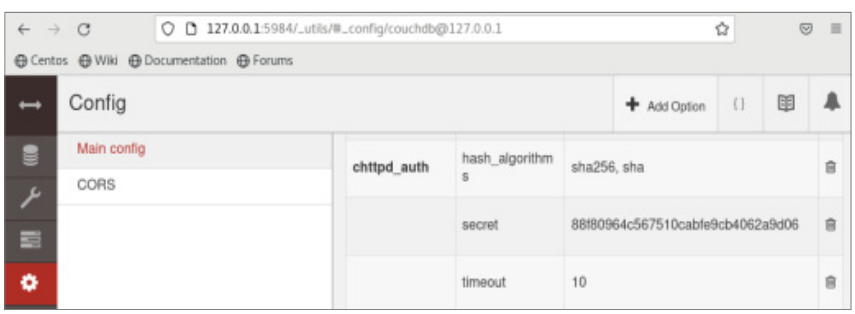
진단 방법

■ WEB에서 timeout 설정 확인

1) http://127.0.0.1:5984/_utils/에 접속

2) 관리자 계정 로그인 후 Config 메뉴 선택

3) chttpd_auth Section에서 timeout 설정값 확인



■ local.ini 파일에서 timeout 설정 확인

```
[chttpd_auth]
secret = 88f80964c567510cabfe9cb4062a9d06
timeout = 600
```

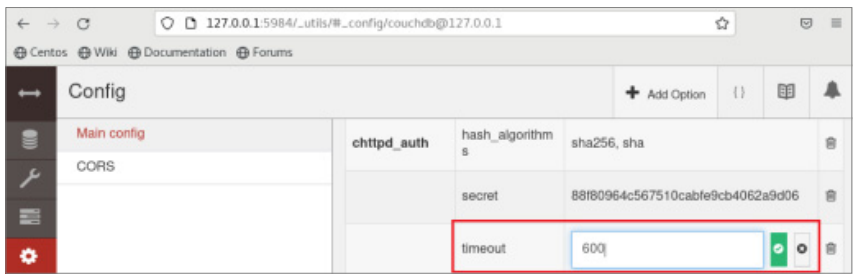
조치 방법

■ WEB에서 timeout 설정값 변경

1) http://127.0.0.1:5984/_utils/에 접속

2) 관리자 계정 로그인 후 Config 메뉴 선택

3) chttpd_auth Section에서 timeout 600(10분) 이하로 설정



■ local.ini 파일에서 timeout 설정값 변경

1) timeout 설정값 600(10분) 이하로 변경

```
[chttpd_auth]
secret = 88f80964c567510cabfe9cb4062a9d06
timeout = 600
```

비고

※ Default : 600

데이터베이스 사용자 정의 설정

항목설명

사용자를 정의하지 않거나 적절한 권한을 부여하지 않으면 모든 사용자가 데이터베이스에 대한 읽기 및 쓰기 권한을 가질 수 있으며 이로 인해 무분별한 데이터 엑세스와 수정 가능한 위험이 존재한다.

진단 기준

양호

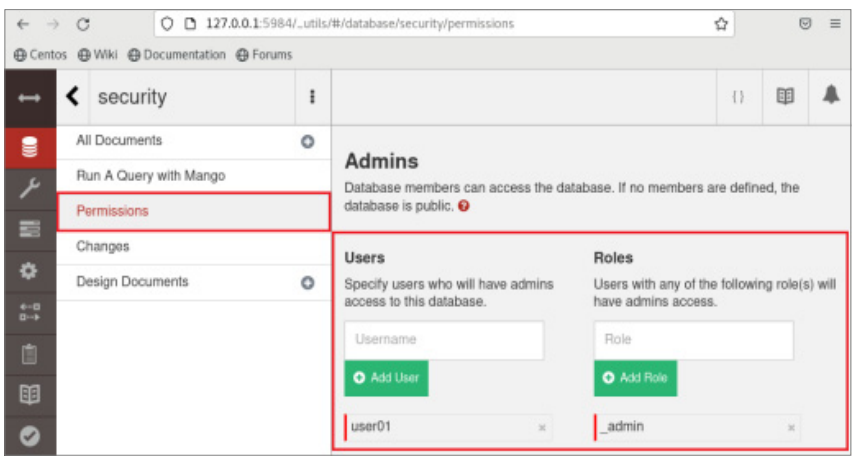
데이터베이스에 정의된 사용자 또는 Roles가 적절한 권한으로 부여되어 있는 경우

취약

데이터베이스에 정의된 사용자 또는 Roles가 적절한 권한으로 부여되어 있지 않은 경우

진단 방법

■ 데이터베이스별 사용자, Roles 설정 확인



조치 방법

■ 적절한 권한의 사용자 또는 Roles 추가

환경설정 파일 권한 관리

항목설명

환경설정 파일에 대한 취약한 접근 권한으로 공격자가 설정 파일을 변경하여 데이터베이스 서비스에 필요한 권한을 획득하여 악용 가능성을 제공하는 위험이 존재한다.

진단 기준

양호

환경설정 파일의 소유자 및 그룹이 관리자 계정이며 권한이 640 이하인 경우

취약

환경설정 파일의 소유자 및 그룹이 관리자 계정이 아니거나 권한이 640 초과인 경우

진단 방법

■ default.ini, local.ini 파일 권한 확인

```
# ls -l [CouchDB 디렉토리]/etc/
```

■ default.d, local.d 디렉토리 내부 파일 권한 확인

```
# ls -l [CouchDB 디렉토리]/etc/default.d/
# ls -l [CouchDB 디렉토리]/etc/local.d/
```

조치 방법

■ 환경 설정 파일 권한을 640으로 변경

```
# chmod 640 [CouchDB 환경 설정 파일]
```

로그 활성화

항목설명

데이터베이스의 감사기록이 기관에서 정의한 감사기록 정책에 적합하도록 설정되어 있어야 하며, 데이터베이스는 데이터, 로그와 응용프로그램에 대한 백업 정책을 수립하여야 한다.

진단 기준

양호

감사 로그 기록을 기관 정책에 맞게 시행하고 있으며, 백업 정책대로 주기적으로 백업을 하고 있는 경우

취약

감사 로그 기록과 관련된 정책이 존재하지 않거나 정책대로 시행하고 있지 않거나 백업 정책 및 시행을 하고 있지 않은 경우

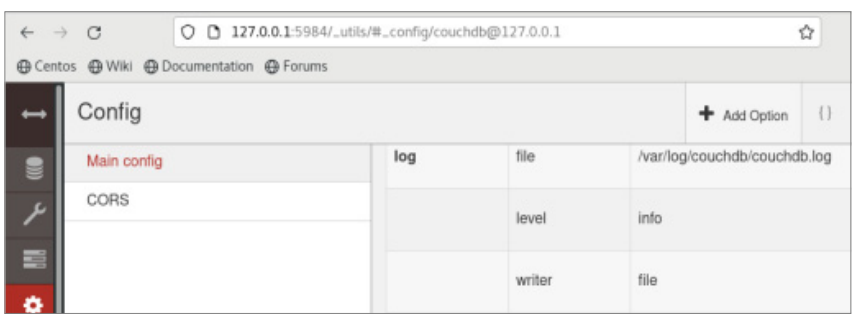
진단 방법

■ WEB에서 log level 설정 확인

1) http://127.0.0.1:5984/_utils/에 접속

2) 관리자 계정 로그인 후 Config 메뉴 선택

3) log Section에서 level 설정값 확인



■ local.ini 파일에서 log level 설정 확인

```
[log]
; Possible log levels:
; ;   debug
; ;   info
; ;   notice
; ;   warning, warn
; ;   error, err
; ;   critical, crit
; ;   alert
; ;   emergency, emerg
; ;   none
level = info
```

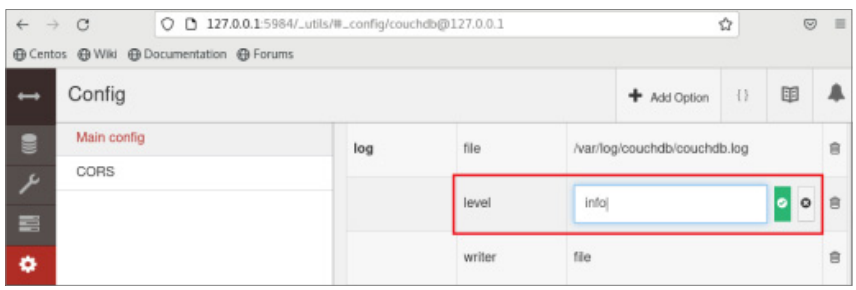
조치 방법

■ WEB에서 log level 변경

1) http://127.0.0.1:5984/_utils/에 접속

2) 관리자 계정 로그인 후 Config 메뉴 선택

3) log Section에서 level을 none이 아닌 다른 값으로 변경



■ local.ini 파일에서 log level 변경

1) level을 none이 아닌 다른 값으로 변경

```
[log]
; Possible log levels:
; ;   debug
; ;   info
; ;   notice
; ;   warning, warn
; ;   error, err
; ;   critical, crit
; ;   alert
; ;   emergency, emerg
; ;   none
level = info
```

비고

※ Default : info

최신 보안 패치 적용

항목설명

데이터베이스의 주요 보안 패치 등을 설치하지 않은 경우 공격자가 알려진 취약점을 이용하여 데이터베이스에 접근 가능하다.

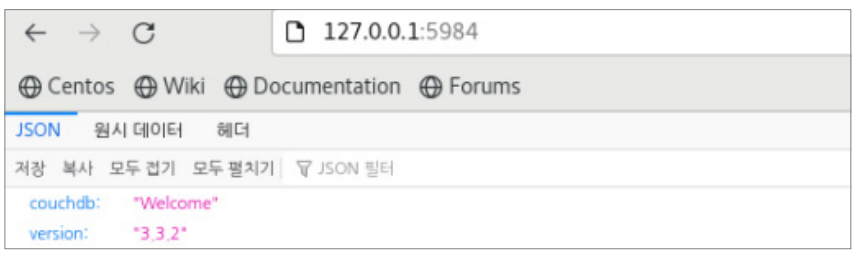
진단 기준

양호
최신 보안 패치를 적용하고 있는 경우

취약
최신 보안 패치를 적용하고 있지 않은 경우

진단 방법

■ 버전 확인 후 최신 패치 적용 여부 확인



조치 방법

■ 최신 보안 패치 확인 후 업그레이드 및 패치 수행

비고

※ 시스템 업데이트는 영향도를 산정하여 진행하여야 한다.

2.18.

SQLite

2.18. SQLite

보안 설정(4개 항목), 로그 및 패치 관리(2개 항목) 총 2개 영역에서 6개 항목으로 구성된다.

[표 18] SQLite 진단 체크리스트

구분	진단 항목
가. 보안 설정	DB 파일 권한
	중요 정보 암호화
	안전한 암호화 알고리즘 사용
	실행 파일 권한
나. 로그 및 패치 관리	로그 설정
	최신 보안 패치 적용

DB 파일 권한

항목설명

비인가자가 DB 파일에 접근 가능하면 데이터 무단 변조, DB 파일 삭제, 외부 노출 등 각종 위험이 존재한다.

진단 기준

양호
DB 파일의 접근 권한이 640 이하인 경우

취약
DB 파일의 접근 권한이 640 초과인 경우

진단 방법

■ DB 파일 접근 권한 확인

```
# ls –al [DB 파일명]
```

조치 방법

■ DB 파일 접근 권한 설정

```
# chmod 640 [DB 파일명]
```

중요 정보 암호화

항목설명

DB 파일 또는 중요 데이터가 암호화되지 않은 상태로 외부 비인가자에게 유출될 경우 침해사고, 개인정보 유출 등 각종 위험이 존재한다.

진단 기준

양호

DB 파일 또는 중요 데이터를 암호화하고 있는 경우

취약

DB 파일 또는 중요 데이터를 암호화하고 있지 않은 경우

진단 방법

■ SQLCipher 설치 확인

```
# dpkg –l | grep –i sqlcipher
```

조치 방법

■ SQLCipher 설치

```
# sudo apt install sqlcipher
```

■ SQLCipher 설치 확인

```
# sqlcipher --version
```

■ 작성된 DB 파일 또는 중요 데이터 암호화 및 복호화 과정

1) DB 파일 암호화를 위한 파일 생성

```
# sqlite3 test.db
SQL〉 .out test_db.sql
SQL〉 .dump
SQL〉 .quit
```

2) 암호화를 위한 파일 생성

```
# cat test_db.sql
# sqlcipher enc.db
```

3) 데이터 암호화

```
SQL〉 PRAGMA key='password';
SQL〉 .read test_db.sql
SQL〉 .quit
```

4) 데이터 암호화 확인

```
# sqlite3 enc.db
# hexdump –C enc.db
```

5) 데이터 복호화

```
# sqlcipher enc.db
SQL〉 SELECT * FROM test;
SQL〉 PRAGMA key='password';
SQL〉 SELECT * FROM test;
```

비고

※ 아래의 프로그램을 통해 SQLCipher 기능을 사용할 수도 있음
- DB Browser for SQLite
- Navicat for SQLite
- SQLiteStudio

※ DB Browser for SQLite의 경우 SQLCipher를 지원하지 않는 버전 존재

안전한 암호화 알고리즘 사용

항목설명

SHA-256 암호화 알고리즘은 단방향 알고리즘으로 평문을 암호화했을 때 다시 평문으로 복호화할 수 없는 암호화 알고리즘이다.

진단 기준

양호

DB 파일 또는 중요 데이터 암호화 시 SHA-256 이상 암호화 알고리즘을 사용하고 있는 경우

취약

DB 파일 또는 중요 데이터 암호화 시 SHA-256 이상 암호화 알고리즘을 사용하고 있지 않은 경우

진단 방법

■ SHA-256 이상의 암호화 알고리즘 사용 여부 확인

조치 방법

■ SHA-256 이상 암호화 알고리즘 사용

비고

※ SQL Cipher 4.0.0 미만 버전에서는 SHA-1 알고리즘이 적용되므로 4.0.0 이상 버전 사용 권고

실행 파일 권한

항목설명

실행 파일에 대한 접근 권한 및 소유자 설정이 취약하면 공격자가 실행 파일을 변경하거나 악성코드 삽입 등으로 인한 침해사고가 발생할 수 있고 이로 인해 중요 데이터의 유출, 데이터의 변조 등 각종 위험이 존재한다.

진단 기준

양호

실행 파일의 소유자 및 소유그룹이 별도의 계정이고 권한이 750 이하인 경우

취약

실행 파일의 소유자 및 소유그룹이 기본 계정이고 권한이 750 초과인 경우

진단 방법

■ 실행 파일 확인

```
# which sqlite3
```

■ 실행 파일 소유자 및 소유그룹, 권한 확인

```
# ls –al [파일명]
```

조치 방법

1) 파일의 소유자 및 소유그룹을 별도의 계정으로 변경

```
# chown dba:dba [파일명]
```

2) Other의 실행 권한 제거

```
# chmod 750 [파일명]
```

로그 설정

항목설명

로그를 활성화하여 정기적으로 침입 여부를 파악하고, 침입 시도 의심 사례를 분석하여 사전에 해당 장비에 대한 접근을 차단하는 등 체계적인 로그 관리 작업이 이루어져야 한다.

진단 기준

양호

WAL mode 설정을 통해 로그를 저장하고 있는 경우

취약

WAL mode 설정을 통해 로그를 저장하고 있지 않은 경우

진단 방법

■ journal_mode 확인

SQL〉 pragma journal_mode;

```
sqlite> pragma journal_mode;
delete
sqlite>
```

조치 방법

■ WAL mode 설정

SQL〉 pragma journal_mode=WAL;

```
sqlite> pragma journal_mode=WAL;
wal
sqlite> pragma journal_mode;
wal
sqlite>
```

최신 보안 패치 적용

항목설명

최신 패치가 적용되어 있지 않은 경우, 데이터베이스가 공격자나 비인가자에 노출될 수 있고 각종 버그 또는 알려진 취약점으로 인해 침해사고가 발생할 수 있다.

진단 기준

양호
최신 보안 패치가 적용되어 있는 경우

취약
최신 보안 패치가 적용되어 있지 않은 경우

진단 방법

■ 최신 보안 패치 적용 여부 확인

```
# sqlite3 --version
```

조치 방법

■ 최신 보안 패치 버전 확인 후 업그레이드 및 패치 수행

※ SQLite 공식사이트에서 최신 버전 확인 가능
https://www.sqlite.org/chronology.html

비고

※ 시스템 업데이트는 영향도를 산정하여 진행하여야 함

2.19.

Tibero

2.19. Tibero

계정 관리(3개 항목), 보안 설정(3개 항목), 패치 및 로그 관리(3개 항목) 총 3개 영역에서 9개 항목으로 구성된다.

[표 19] Tibero 진단 체크리스트

구분	진단 항목
가. 계정 관리	불필요한 계정 제거
	취약한 패스워드 사용 제한
	계정 별 부여된 시스템 권한 확인
나. 접근 관리	홈 디렉터리의 접근 권한
	주요 실행 파일 접근 권한
	환경 설정 파일 접근 권한
다. 옵션 관리	감사 기능 활성화
	아카이브 모드 확인
	최신 보안 패치 적용

불필요한 계정 제거

항목설명

사용하지 않는 불필요한 계정이 존재할 경우 비인가자가 불필요한 계정을 이용하여 DB에 접근 후 데이터를 열람, 삭제, 수정할 위험이 존재한다.

진단 기준

양호

계정 정보를 확인하여 불필요한 계정이 없는 경우

취약

인가되지 않은 계정, 퇴직자 계정, 테스트 계정 등 불필요한 계정이 존재하는 경우

진단 방법

■ 활성화 계정 확인

SQL〉 SELECT USERNAME,ACCOUNT_STATUS FROM DBA_USERS;

조치 방법

■ 활성화 계정 중 불필요한 계정 삭제

SQL〉 DROP USER ‘username’ cascade;

취약한 패스워드 사용 제한

항목설명

취약한 패스워드는 사회공학적인 유추가 가능할 수 있으며 암호화된 패스워드 해시값을 무작위 대입공격, 사전대입 공격 등으로 단시간에 패스워드 크랙이 가능하다.

진단 기준

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

진단 방법

■ 계정별 적용된 프로파일 확인

```
SQL〉 SELECT USERNAME, ACCOUNT_STATUS FROM DBA_USERS;
```

■ 프로파일 설정 내용 확인

```
SQL〉 SELECT * FROM DBA_PROFILES;
```

조치 방법

■ 프로파일 리소스 수정

```
SQL〉 ALTER PROFILE DEFAULT LIMIT PASSWORD_LIFE_TIME 90;
SQL〉 ALTER PROFILE DEFAULT LIMIT PASSWORD_VERIFY_FUNCTION
      NULL_VERIFY_FUNCTION;
SQL〉 ALTER PROFILE DEFAULT LIMIT FAILED_LOGIN_ATTEMPTS 3;
SQL〉 ALTER PROFILE DEFAULT LIMIT PASSWORD_LOCK_TIME 1/1440;
SQL〉 ALTER PROFILE DEFAULT LIMIT PASSWORD_REUSE_TIME UNLIMITED;
SQL〉 ALTER PROFILE DEFAULT LIMIT PASSWORD_REUSE_MAX 10;
SQL〉 ALTER PROFILE DEFAULT LIMIT PASSWORD_GRACE_TIME 10;
SQL〉 ALTER PROFILE DEFAULT LIMIT VERIFY_FUNCTION VERIFY_FUNCTION;
```

■ 취약한 패스워드 변경

```
SQL〉 ALTER USER ‘USERNAME’ IDENTIFIED BY ‘새로운 비밀번호’;
```

비고

※ FAILED_LOGIN_ATTEMPTS : 로그인 시도 허용 횟수
※ PASSWORD_LOCK_TIME : 패스워드 입력 초과로 잠금 상태가 되었을 때 자동으로 잠금 상태를 해제하는 기간
※ PASSWORD_LIFE_TIME : 패스워드 만료 기간
※ PASSWORD_REUSE_TIME : 패스워드 재사용 금지 기간
※ PASSWORD_REUSE_MAX : 설정된 개수만큼 최근 변경한 패스워드 재사용 금지
※ PASSWORD_VERIFY_FUNCTION : 패스워드 문자열을 검사하여 유효성을 확인하는 함수 지정
※ PASSWORD_GRACE_TIME : 패스워드 사용기간 만료 후 패스워드 만료 경고를 보내는 기간
※ LOGIN_PERIOD : 마지막 로그인 후 지정된 시간 지나면 계정 잠금

계정 별 부여된 시스템 권한 확인

항목설명

각 사용자 계정에 시스템 권한이 불필요하게 부여되어 있는 경우 무단 액세스로 인해 인가되지 않은 사용자가 중요한 데이터에 접근할 수 있어 정보 유출이나 손상과 같은 위험이 존재한다.

진단 기준

양호

시스템 권한이 적절한 사용자에게 부여되어 있는 경우

취약

시스템 권한이 적절하지 않은 사용자에게 부여되어 있는 경우

진단 방법

■ 시스템 계정, 일반 계정 확인

SQL〉 SELECT USERNAME, DEFAULT_TABLESPACE FROM DBA_USERS;

■ 시스템 권한을 부여 받은 일반 계정 확인

SQL〉 SELECT * FROM DBA_SYS_PRIVS;

조치 방법

■ 불필요한 사용자 권한 회수

SQL〉 REVOKE '권한' FROM '사용자';

홈 디렉터리의 접근 권한

항목설명

취약한 접근 권한으로 무단 사용자가 홈 디렉터리에 접근할 경우 중요 설정 파일 및 데이터 파일이 유출될 수 있으며 취약한 디렉터리에 악성코드나 악의적인 스크립트가 삽입될 수 있는 위험이 존재한다.

진단 기준

양호

일반 사용자 쓰기 권한이 제거되어 있는 경우

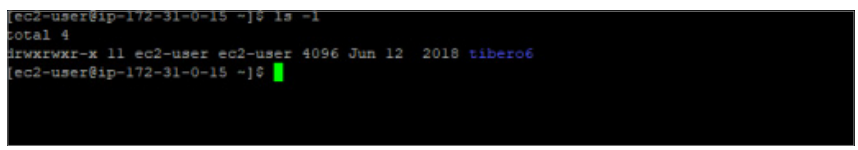
취약

일반 사용자 쓰기 권한이 제거되어 있지 않은 경우

진단 방법

■ 홈 디렉터리 권한 확인

ls -l $TB_HOME



조치 방법

■ 홈 디렉터리 일반 사용자 쓰기 권한 제거

chmod o-w $TB_HOME

주요 실행 파일 접근 권한

항목설명

실행 파일에 대한 접근 권한이 취약하면 공격자가 실행 파일을 변경하거나 악성코드를 삽입할 수 있으며 이로 인해 무단 액세스, 데이터 변조, 중요한 설정 파일의 노출 위험이 존재한다.

진단 기준

양호
일반 사용자 권한이 제거되어 있는 경우

취약
일반 사용자 권한이 제거되어 있지 않은 경우

진단 방법

■ 주요 실행 파일 권한 확인

ls –l $TB_HOME/bin

```
[ec2-user@ip-172-31-0-15 bin]$ ls -l
total 684652
-rwxr-xr-x 1 ec2-user ec2-user      1266 Jan  4  2021 alterdd.sh
-rw-r--r-- 1 ec2-user ec2-user       946 Jan  4  2021 base_env.sh
-rwxrwxr-x 4 ec2-user ec2-user  30391940 Jan  4  2021 cmrctl
-rwxr-xr-x 1 ec2-user ec2-user       225 Jan  4  2021 cm_res_exec.sh
-rwxrwxr-x 4 ec2-user ec2-user  30391940 Jan  4  2021 crfconf
-rwxr-xr-x 1 ec2-user ec2-user       849 Jan  4  2021 dbctl_for_cm.sh
-rwxr-xr-x 2 ec2-user ec2-user      1346 Jan  4  2021 internal_svr_env.sh
```

조치 방법

■ 주요 실행 파일 일반 사용자 권한 제거

chmod –R 640 $TB_HOME/bin

환경 설정 파일 접근 권한

항목설명

환경 설정 파일의 취약한 접근 권한 설정으로 인해 비인가자에 의한 환경 설정 파일 수정, 데이터베이스 권한 획득 등의 위험에 노출될 수 있다.

진단 기준

양호

환경 설정 파일에 일반 사용자 권한이 제거되어 있는 경우

취약

환경 설정 파일에 일반 사용자 권한이 제거되어 있지 않은 경우

진단 방법

■ 환경 설정 파일 권한 확인

ls -l $TB_HOME/config/$TB_SID.tip

```
-rw-r--r-- 1 ec2-user ec2-user  489 May 30  2018 tibero.template
-rw-rw-r-- 1 ec2-user ec2-user  712 Jun 12  2018 tibero.tip
-rw-r--r-- 1 ec2-user ec2-user  689 May 30  2018 tip_dev.template
-rw-r--r-- 1 ec2-user ec2-user  340 May 30  2018 tip_max.template
-rw-r--r-- 1 ec2-user ec2-user  582 May 30  2018 tip.ssa.template
-rw-r--r-- 1 ec2-user ec2-user  525 Jan  4  2021 tip.template
-rw-rw-r-- 1 ec2-user ec2-user    4 Jan  4  2021 variant
[ec2-user@ip-172-31-0-15 config]$
```

ls -l $TB_HOME/client/config/tbdsn.tbr

```
-rwxr-xr-x 1 ec2-user ec2-user 786 Jan  4  2021 gen_esql_cfg.sh
-rw-rw-r-- 1 ec2-user ec2-user 296 Jun 12  2018 tbdsn.tbr
-rw-rw-r-- 1 ec2-user ec2-user 502 Jan  4  2021 tbertl.cfg
-rw-rw-r-- 1 ec2-user ec2-user 323 Jan  4  2021 tbpcb.cfg
-rw-rw-r-- 1 ec2-user ec2-user 598 Jan  4  2021 tbpc.cfg
[ec2-user@ip-172-31-0-15 config]$
```

조치 방법

■ 환경 설정 파일 일반 사용자 권한 제거

chmod 640 $TB_HOME/config/$TB_SID.tip
chmod 640 $TB_HOME/client/config/tbdsn.tbr

감사 기능 활성화

항목설명

감사기록 정책이 설정되어 있지 않을 경우, 데이터베이스에 문제 발생 시 원인을 규명할 수 있는 자료가 존재하지 않아 이에 대한 대처 및 개선방안 수립이 어려움이 있다.

진단 기준

양호

DBMS의 감사 로그 기록 정책이 수립되어 있으며, 정책 설정이 적용되어 있는 경우

취약

DBMS의 감사 로그 기록 정책이 수립되어 있지 않거나, 정책 설정이 적용되어 있지 않은 경우

진단 방법

■ 감사 기록 설정 여부 확인

```
# vi $TB_HOME/config/$TB_SID.tip
```

조치 방법

■ 감사 기록 설정

$TB_HOME/config/$TB_SID.tip 파일 내용 수정
- AUDIT_TRAIL=OS
- AUDIT_SYS_OPERATIONS=Y
- AUDIT_FILE_DEST=$TB_HOME/audit/audit_trail.log
- AUDIT_FILE_SIZE=10M

아카이브 모드 확인

항목설명

아카이브 모드가 비활성화되면 데이터 손실 및 시스템 장애 시 복구 어려움이 발생하고 데이터 변경 감지와 보안 감사도 어려워지게 되므로 비인가된 접근 위험이 증가한다.

진단 기준

양호
아카이브 모드로 설정 되어 있는 경우

취약
아카이브 모드로 설정 되어 있지 않은 경우

진단 방법

■ 아카이브 모드 확인

SQL〉 SELECT LOG_MODE FROM V$DATABASE;

```
SQL> SELECT LOG_MODE FROM V$DATABASE;

LOG_MODE
------------
NOARCHIVELOG

1 row selected.

SQL>
```

조치 방법

■ 아카이브 모드 설정

1) mount 모드로 tibero 재실행
   # tbdown
   # tbboot mount
   # tbsql sys/tibero

2) 아카이브 모드로 변경 후 재실행
   SQL〉 ALTER DATABASE ARCHIVELOG;
   SQL〉 QUIT
   # tbdown
   # tbboot

최신 보안 패치 적용

항목설명

데이터베이스의 주요 보안 패치를 설치하지 않은 경우 공격자가 알려진 취약점을 이용하여 데이터베이스에 접근 가능하다.

진단 기준

양호
최신 보안 패치를 적용하고 있는 경우

취약
최신 보안 패치를 적용하고 있지 않은 경우

진단 방법

■ 버전 확인 후 최신 보안 패치 적용 여부 확인

SQL〉 SELECT * FROM V$VERSION;

조치 방법

■ 최신 보안 패치 확인 후 업그레이드 및 패치 수행

비고

※ 시스템 업데이트는 영향도를 산정하여 진행하여야 한다.

2.20.

InfluxDB

2.20. InfluxDB

보안 설정(4개 항목), 디렉터리 및 파일권한 관리(2개 항목), 패치 및 로그 관리(2개 항목) 총 3개 영역에서 8개 항목으로 구성된다.

[표 20] InfluxDB 진단 체크리스트

구분	진단 항목
가. 보안 설정	인증사용 여부
	사용자 및 권한 관리
	HTTPS 프로토콜 활성화
	IP 접근 권한 설정
나. 디렉터리 및 파일권한 관리	패스워드 파일 권한 변경
	환경설정 파일 접근 권한 설정
다. 패치 및 로그 관리	로그 활성화
	최신 보안 패치 적용

인증사용 여부

항목설명

InfluxDB의 실행 데몬인 influxd를 실행할 때, 인증 설정을 사용하지 않으면 인증 없이 접근이 가능하게 되므로 비인가된 사용자가 데이터베이스에 접근하여 악의적인 행위를 할 위험이 존재한다.

진단 기준

양호
인증 여부가 활성화되어 있는 경우

취약
인증 여부가 비활성화되어 있는 경우

진단 방법

[InfluxDB v1]

■ influxdb.conf 파일 내 auth-enabled 설정 확인

```
# cat /etc/influxdb/influxdb.conf
```

```
# Determines whether user auth
# auth-enabled = false
```

[InfluxDB v2]

■ v2에서는 기본적으로 인증 기능을 사용

조치 방법

[InfluxDB v1]

■ influxdb.conf 파일 내 auth-enabled 설정 변경

```
# vi /etc/influxdb/influxdb.conf
  auth-enabled = true
```

사용자 및 권한 관리

항목설명

DB 관리나 운용에 사용하지 않는 불필요한 계정이나 부적절한 권한이 존재할 경우 비인가자가 불필요한 계정을 이용하여 DB에 접근하여 데이터를 열람, 삭제, 수정할 위험이 존재한다.

진단 기준

양호

계정 정보를 확인하여 불필요한 계정이 없는 경우

취약

인가되지 않은 계정, 퇴직자 계정, 테스트 계정 등 불필요한 계정이 존재하는 경우

진단 방법

[InfluxDB v1]

■ 활성화 계정 및 권한 확인

SQL〉 show users;
SQL〉 show grants for [계정명];

[InfluxDB v2]

■ 활성화 계정 및 권한 확인

influx user list

조치 방법

[InfluxDB v1]

■ 활성화 계정 중 불필요한 계정 삭제

SQL〉 DROP USER 'username';

■ 불필요한 권한 삭제 및 변경

SQL〉 REVOKE [READ,WRITE,ALL] ON 〈database_name〉 FROM 〈username〉

[InfluxDB v2]

■ 활성화 계정 중 불필요한 계정 및 권한 삭제

비고

※ 활성화 계정 중 일부 시스템 계정 제외

HTTPS 프로토콜 활성화

항목설명

HTTP 프로토콜은 암호화가 되지 않는 평문 통신으로, 중간에 패킷을 가로채 DB 정보가 노출될 수 있으므로, HTTPS를 통해 암호화 통신이 되어있는지 확인한다.

진단 기준

양호
HTTPS 프로토콜이 활성화되어 있는 경우

취약
HTTPS 프로토콜이 비활성화되어 있는 경우

진단 방법

[InfluxDB v1]

■ influxdb.conf 파일 내 https-enabled 설정 확인

cat /etc/influxdb/influxdb.conf

```
# Determines whether HTTP
# https-enabled = false
```

[InfluxDB v2]

■ config 파일 및 실행 데몬 옵션값 tls-key, tls-cert 설정 확인

cat /etc/influxdb/config.toml
- tls-key, tls-cert 값 확인

ps -ef | grep influxd

```
ubuntu@server:~$ ps -ef | grep influx | grep -v grep
root        1949    1932  0 01:43 tty1     00:00:00 systemctl status influxd
root       16548    2129  0 03:54 pts/0    00:00:00 vi /etc/influxdb/config.toml
root       19491    2129  0 06:16 pts/0    00:00:00 influxd --tls-key /etc/ssl/influxdb.key
--tls-cert /etc/ssl/influxdb.crt
```

조치 방법

[InfluxDB v1]

■ HTTPS 프로토콜 활성화

vi /etc/influxdb/influxdb.conf
https-enabled = true

[InfluxDB v2]

■ SSL 프로토콜 활성화

vi /etc/influxdb/config.toml
tls-key = "key 파일 경로"
tls-cert = "crt 파일 경로"

influxd --tls-key "key 파일 경로" --tls-cert "crt 파일 경로"

IP 접근 권한 설정

항목설명

인가된 IP만 접근 가능하도록 설정되어 있지 않은 경우, 비인가 사용자가 해당 데이터베이스에 접근할 위험이 존재한다.

진단 기준

양호

인가된 IP만 접근 가능하도록 설정되어 있는 경우

취약

비인가된 IP가 접근 가능하도록 설정되어 있는 경우

진단 방법

■ IP 접근제어 확인

- iptables 설정 확인
  # iptables –L
- /etc/hosts.deny , allow 설정 확인
  # cat /etc/hosts.allow
  # cat /etc/hosts.deny

조치 방법

■ iptables 설정

■ /etc/hosts.deny, allow 설정

vi /etc/hosts.deny
vi /etc/hosts.allow

비고

※ Server의 IP 접근 정책(iptables, tcpwrapper, firewalld 등)이 부재한 경우, 별도의 방화벽 정책 확인 필요

패스워드 파일 권한 변경

항목설명

InfluxDB의 패스워드 파일을 변경하여 시스템 장애를 유발할 수 있으므로, 패스워드 파일에 대한 접근 권한을 제한해야 한다.

진단 기준

양호

패스워드 파일 권한이 640 이하이고,
소유자가 influxdb인 경우

취약

패스워드 파일 권한이 640 초과하거나,
소유자가 influxdb가 아닌 경우

진단 방법

[InfluxDB v1]

■ 'meta.db' 파일 권한 확인

ls –l meta.db

```
ubuntu@server:~$ ls -l /var/lib/influxdb/meta/meta.db
-rw-r--r-- 1 influxdb influxdb 378 Nov 13 23:54 /var/lib/influxdb/meta/meta.db
```

[InfluxDB v2]

■ 'influxd.bolt' 파일 권한 확인

ls –aln influxd.bolt

```
root@server:/var/lib/influxdb# ls -aln influxd.bolt
-rw------- 1 998 998 262144 Nov 17 06:05 influxd.bolt
```

조치 방법

■ 패스워드 파일 권한 변경

chmod 640 [패스워드 파일]

■ 패스워드 파일 소유자 변경

chown influxdb [패스워드 파일]

환경설정 파일 접근 권한 설정

항목설명

InfluxDB의 환경설정 파일을 변경하여 시스템 장애를 유발할 수 있으므로, 환경설정 파일에 대한 접근 권한을 제한해야 한다.

진단 기준

양호

환경설정 파일 권한이 640 이하이고,
소유자가 influxdb인 경우

취약

환경설정 파일 권한이 640 초과하거나,
소유자가 influxdb가 아닌 경우

진단 방법

[InfluxDB v1]

■ "influxdb.cnf" 파일 접근 권한 확인

```
# ls –alL /etc/influxdb/influxdb.conf
```

[InfluxDB v2]

■ "config.toml" 파일 접근 권한 확인

```
# ls –alL /etc/influxdb/config.toml
```

조치 방법

■ 환경설정 파일 권한 변경

```
# chmod 640 [환경설정 파일]
```

■ 환경설정 파일 소유자 변경

```
# chown influxdb [환경설정 파일]
```

로그 활성화

항목설명

로그 파일을 남김으로써 데이터베이스의 변경 이력들을 관리할 수 있으며 침해 사고 및 장애 발생 시 로그 자료를 통해 원인 분석을 할 수 있다.

진단 기준

양호
로그 기능이 활성화 되어 있는 경우

취약
로그 기능이 비활성화 되어 있는 경우

진단 방법

[InfluxDB v1]

■ 'influxdb.conf' 파일 내 설정값 확인

cat /etc/influxdb/influxdb.conf

- query log 설정 확인

```
# query-log-enabled = true
```

- Slow Query 설정 확인

```
# log-queries-after = "0s"
```

- HTTP 요청 트래픽 로그 설정 확인

```
# log-enabled = true
# access-log-path = ""
```

[InfluxDB v2]

■ ps 명령어를 이용한 옵션값 확인

ps –ef | grep influxd

```
ubuntu@server:~$ ps -ef | grep influx | grep -v grep
root        1949    1932  0 01:43 tty1     00:00:00 systemctl status influxd
root       16548    2129  0 03:54 pts/0    00:00:00 vi /etc/influxdb/config.toml
root       19763    2129  3 06:46 pts/0    00:00:00 influxd --flux-log-enabled
```

■ influx CLI를 이용한 설정값 확인

influx server-config
- flux-log-enabled 값 확인
- log-level 값 확인

```
rver:/home/ubuntu# influx server-config | grep lo
 "flux-log-enabled": true,
 "log-level": "info",
 "storage-max-index-log-file-size": 1048576,
```

■ 'config.toml' 파일 내 설정값 확인

cat /etc/influxdb/config.toml
flux-log-enabled 값 확인

조치 방법

[InfluxDB v1]

■ 로그 기능 활성화

vi /etc/influxdb/influxdb.conf

- query log 설정 변경
  query-log-enabled = true
- Slow Query 설정
  log-queries-after 값 설정
- HTTP 요청 트래픽 로그 설정 확인
  [Http]
  log-enabled = true
  access-log-path 경로 설정

[InfluxDB v2]

■ 로그 기능 활성화

vi /etc/influxdb/config.toml
flux-log-enabled = true
log-level = info

influxd —flux-log-enabled

최신 보안 패치 적용

항목설명

데이터베이스의 주요 보안 패치 등을 설치하지 않은 경우 공격자가 알려진 취약점을 이용하여 데이터베이스에 접근 가능하다.

진단 기준

양호
최신 보안 패치를 적용하고 있는 경우

취약
최신 보안 패치를 적용하고 있지 않은 경우

진단 방법

[InfluxDB v1]

■ InfulxDB 버전 확인

influx -version

```
ubuntu@server:~$ influx -version
InfluxDB shell version: 1.6.7~rc0
ubuntu@server:~$
```

[InfluxDB v2]

■ InfulxDB 버전 확인

influxd version

```
root@server:/home/ubuntu# influxd version
InfluxDB v2.7.4 (git: 19e5c0e1b7) build_dat
```

조치 방법

■ 최신 보안 패치 적용

비고

※ InfluxDB v1은 2021년 10월 11일에 v1.8.10을 마지막으로 업데이트 없음

2.21.

Oracle

2.21. Oracle

계정 관리(4개 항목), 접근 관리(4개 항목), 옵션 관리(2개 항목), 패치 관리(2개 항목) 총 4개 영역에서 12개 항목으로 구성된다.

[표 21] Oracle 진단 체크리스트

구분	진단 항목
가. 계정 관리	디폴트 계정 및 패스워드 변경
	불필요한 계정 제거
	기관 보안 정책과 패스워드 정책 일치
	관리자 권한 설정
나. 접근 관리	원격에서 DB 서버로의 접속 제한
	사용자의 시스템 테이블 접근 권한 제거
	리스너의 패스워드 설정
	SYSDBA로그인 제한 설정
다. 옵션 관리	DBA 계정 Role 설정
	OS_ROLES, REMOTE_OS_AUTHENTICATION, REMOTE_OS_ROLES 설정
라. 패치 관리	최신 보안 패치 적용
	로그 활성화

디폴트 계정 및 패스워드 변경

항목설명

DBMS 기본 계정 디폴트 패스워드 및 권한 정책을 변경하지 않을 경우 비인가자가 DBMS 기본 계정과 디폴트 패스워드를 통해 DB에 접근할 수 있으며, 기본 계정에 부여된 권한을 악용하여 DB 정보를 유출할 수 있는 위험이 존재한다.

진단 기준

양호

기본 계정의 디폴트 패스워드 및 권한 정책을 변경하여 사용하는 경우

취약

기본 계정의 디폴트 패스워드 및 권한 정책을 변경하지 않고 사용하는 경우

진단 방법

■ 기본 계정 및 패스워드 정보 확인

User	Password	User	Password
scott	tiger or tigger	system	manager
dbsnmp	dbsnmp	sys	chageon_install
tracesvr	trace	outln	outln
ordplugins	ordplugins	ordsys	ordsys
ctxsys	ctxsys	mdsys	mdsys
adams	wood	blake	papr
clark	clth	jones	steel
lbacsys	lbacsys	–	–

조치 방법

■ 사용되는 계정의 경우 패스워드 변경 후 사용

SQL〉 alter user username identified by new_password;

※ 그 이외에 객체 권한 부여, 기본 role 확인 및 변경 수행
※ DBSNMP 파일의 접근권한 설정이 필요함
chmod 700 snmp_rw.ora

■ 불필요한 계정 삭제

SQL〉 DROP USER 'username';

불필요한 계정 제거

항목설명

DB 관리나 운용에 사용하지 않는 불필요한 계정이 존재할 경우 비인가자가 불필요한 계정을 이용하여 DB의 데이터를 열람, 삭제, 수정할 위험이 존재한다.

진단 기준

양호

계정 정보를 확인하여 불필요한 계정이 없는 경우

취약

인가되지 않은 계정, 퇴직자 계정, 테스트 계정 등 불필요한 계정이 존재하는 경우

진단 방법

■ 활성화 계정 확인

SQL〉 SELECT USERNAME, ACCOUNT_STATUS FROM DBA_USERS WHERE ACCOUNT_STATUS='OPEN';

조치 방법

■ 활성화 계정 중 불필요한 계정 삭제

SQL〉 DROP USER 'username';

비고

■ 활성화 계정 중 일부 시스템 계정 제외

- SYS, SYSTEM, SYSMAN, DBSNMP, MGMT_VIEW

기관 보안 정책과 패스워드 정책 일치

항목설명

패스워드 사용기간 및 복잡도 설정 유무를 점검하여 비인가자의 패스워드 추측 공격(무작위 대입 공격, 사전 대입 공격 등)에 대한 대비가 되어있는지 확인한다.

진단 기준

양호

기관 정책에 맞게 패스워드 사용기간 및 복잡도 설정이 적용되어 있는 경우

취약

기관 정책에 맞게 패스워드 사용기간 및 복잡도 설정이 적용되어 있지 않는 경우

진단 방법

■ 유저 별 적용된 프로파일 확인

SQL〉 SELECT USERNAME, PROFILE FROM DBA_USERS WHERE ACCOUNT_STATUS='OPEN';

```
SQL> SELECT USERNAME, PROFILE FROM DBA_USERS WHERE ACCOUNT_STATUS='OPEN';

USERNAME                       PROFILE
------------------------------ --------------------
SYS                            DEFAULT
SYSTEM                         DEFAULT
CLOUD_USER                     DEFAULT
CLOUD                          CLOUD1
```

■ 프로파일 리소스 확인

SQL〉 SELECT PROFILE, RESOURCE_NAME, LIMIT FROM DBA_PROFILES;

```
PROFILE    RESOURCE_NAME              LIMIT
---------- -------------------------- ----------
CLOUD1     PASSWORD_LIFE_TIME         90
CLOUD1     PASSWORD_REUSE_TIME        DEFAULT
CLOUD1     PASSWORD_REUSE_MAX         DEFAULT
CLOUD1     PASSWORD_VERIFY_FUNCTION   VERIFY_FUN
                                      CTION

CLOUD1     PASSWORD_LOCK_TIME         1
CLOUD1     PASSWORD_GRACE_TIME        DEFAULT
```

조치 방법

■ 프로파일 리소스 수정

SQL〉 ALTER PROFILE ‘profile_name’ LIMIT ‘resource_name’ value

예시)

SQL〉 ALTER PROFILE CLOUD1 LIMIT ‘PASSWORD_LIFE_TIME’ 90; (패스워드 최대 사용일을 90일로 설정)

SQL〉 ALTER PROFILE CLOUD1 LIMIT ‘PASSWORD_VERIFY_FUNCTION’ VERIFY_FUNCTION; (패스워드 점검 함수로 VERIFY_FUNCTION 사용)

비고

■ 활성화된 유저가 적용된 모든 프로파일에 설정해야 함

- PASSWORD_LIFE_TIME : 비밀번호 유효 기간
- PASSWORD_REUSE_TIME : 비밀번호를 재사용할 수 없는 일 수
- PASSWORD_REUSE_MAX : 현재 암호를 재사용하기 전 필요한 암호 변경 횟수
- PASSWORD_VERIFY_FUNCTION : 비밀번호 복잡성 검사 함수 설정
- PASSWORD_LOCK_TIME : 지정된 로그인 실패 횟수 이후 계정이 잠기는 일 수
- PASSWORD_GRACE_TIME : 암호 만기 후 변경까지의 유예 기간

관리자 권한 설정

항목설명

관리자 권한을 최소한의 계정과 그룹에만 부여하였는지를 점검하여, 관리자 권한의 오남용을 방지하고 관리자 계정 유출로 인한 비인가자의 DB접근 가능성을 최소화해야 한다.

진단 기준

양호

관리자 권한이 필요한 계정 및 그룹에만 관리자 권한이 부여된 경우

취약

관리자 권한이 필요 없는 계정 및 그룹에 권한이 부여된 경우

진단 방법

■ 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';
```

※ 계정 출력 시 취약

■ Admin에 부적합 계정 존재 여부 점검

```
SQL> SELECT GRANTEE, PRIVILEGE FROM DBA_SYS_PRIVS WHERE GRANTEE
     NOT IN ('SYS, 'SYSTEM', 'AQ_ADMINISTARTOR_ROLE', 'DBA', 'MDSYS',
     'LBACSYS', 'SCHEDULER_ADMIN', 'WMSHS') AND ADMIN_OPTION='YES'
     AND GRANTEE NOT IN (SELECT GRANTEE FROM DBA_ROLE_PRIVS
     WHERE GRANTED_ROLE='DBA');
```

※ 계정 출력 시 취약

조치 방법

■ 불필요한 계정일 경우 계정 삭제

```
SQL> DROP USER 'username';
```

원격에서 DB 서버로의 접속 제한

항목설명

허용되지 않은 IP 및 포트에 대한 접근 통제가 이루어지지 않을 경우, 원격에서의 DB 접근이 가능해져 공격자에 의해 네트워크 서비스 스캐닝을 통한 DB 사용 여부가 확인되어 DB 내의 데이터 유출 및 공격 대상이 될 수 있다.

진단 기준

양호

DB 원격 접속을 제한하고 있는 경우

취약

DB 원격 접속을 제한하고 있지 않은 경우

진단 방법

■ 방화벽 등 보안 솔루션을 통해 원격에서 Oracle에 원격으로 접속이 가능한지 여부 파악

조치 방법

■ 원격 OS 인증 방식이 불필요한 경우 REMOTE_OS_AUTHENT=FALSE로 설정

1) spfile을 사용하는 경우
SQL〉 ALTER SYSTEM SET REMOTE_OS_AUTHENT=FALSE SCOPE=spfile;

2) pfile을 사용하는 경우 ini〈SID〉.ora 파일 내에 설정
SQL〉 ALTER SYSTEM SET REMOTE_OS_AUTHENT=FALSE;

■ 방화벽 OS 인증이 필요한 경우

1) 방화벽을 통한 원격 접근 IP주소 제한

2) NAT를 사용하여 비공인 IP 주소 부여 후 외부 접근 제한

사용자의 시스템 테이블 접근 권한 제거

항목설명

DBA만 접근 가능한 테이블에 일반 사용자 접근을 허용할 경우 비인가 사용자가 시스템의 주요 정보를 획득하거나, 주요 데이터베이스 설정 변경이 가능하다.

진단 기준

양호

DBA만 접근 가능한 테이블에 일반 사용자 접근이 불가능 할 경우

취약

DBA만 접근 가능한 테이블에 일반 사용자 접근이 가능한 경우

진단 방법

■ 시스템 테이블에 접근할 수 있는 일반 사용자 출력

SQL〉 select grantee, privilege, owner, table_name from dba_tab_privs where (owner='SYS' or table_name like 'DBA_%') and privilege 〈〉 'EXECUTE' and grantee not in ('PUBLIC', 'AQ_ADMINISTRATOR_ROLE', 'AQ_USER_ROLE', 'AURORAJISUTILITY$', 'OSE$HTTP$ADMIN', 'TRACESVR', 'CTXSYS', 'DBA', 'DELETE_CATALOG_ROLE', 'EXECUTE_CATALOG_ROLE', 'EXP_FULL_DATABASE', 'GATHER_SYSTEM_STATISTICS', 'HS_ADMIN_ROLE', 'IMP_FULL_DATABASE', 'LOGSTDBY_ADMINISTRATOR', 'MDSYS', 'ODM', 'OEM_MONITOR', 'OLAPSYS', 'ORDSYS', 'OUTLN', 'RECOVERY_CATALOG_OWNER', 'SELECT_CATALOG_ROLE', 'SNMPAGENT', 'SYSTEM', 'WKSYS', 'WKUSER', 'WMSYS', 'WM_ADMIN_ROLE', 'XDB', 'LBACSYS', 'PERFSTAT', 'XDBADMIN', 'ADM_PARALLEL_EXECUTE_TASK', 'DBFS_ROLE', 'HS_ADMIN_SELECT_ROLE', 'OLAPI_TRACE_USER', 'OLAP_XS_ADMIN', 'OWB$CLIENT', 'SYSMAN') and grantee not in (select grantee from dba_role_privs where granted_role='DBA') and grantee not in (select username from dba_users where account_status !='OPEN') order by grantee;

```
GRANTEE                  PRIVILEGE                OWNER                    TABLE_NAME
------------------------ ------------------------ ------------------------ ------------------------
APPLICATION_TRACE_VIEWER SELECT                   SYS                      V_$DIAG_SESS_OPT_TRACE_RE
                                                                           CORDS

APPLICATION_TRACE_VIEWER SELECT                   SYS                      V_$DIAG_SESS_SQL_TRACE_RE
                                                                           CORDS

APPLICATION_TRACE_VIEWER SELECT                   SYS                      V_$DIAG_OPT_TRACE_RECORDS
APPLICATION_TRACE_VIEWER SELECT                   SYS                      V_$DIAG_SQL_TRACE_RECORDS
APPLICATION_TRACE_VIEWER SELECT                   SYS                      V_$DIAG_APP_TRACE_FILE
AUDIT_ADMIN              READ                     SYS                      V_$ASM_AUDIT_CONFIG_PARAM
                                                                           S

AUDIT_ADMIN              READ                     SYS                      GV_$ASM_AUDIT_LAST_ARCH_T
                                                                           S
```

조치 방법

■ 불필요하게 테이블 접근 권한이 사용자 계정에 할당된 경우 권한 제거

SQL〉 REVOKE 권한 ON 객체 FROM USER

리스너의 패스워드 설정

항목설명

Listener에 패스워드가 설정되지 않은 경우 Dos, 정보 획득, Listener 프로세서를 중지시킬 수 있는 위험이 존재한다.

진단 기준

양호

Listener의 패스워드가 설정되어 있고
디폴트 포트가 변경되어 있는 경우

취약

Listener의 패스워드가 설정되지 않거나
디폴트 포트를 변경없이 사용하는 경우

진단 방법

■ Listener 파일 확인

cat $ORACLE_HOME/network/admin/listener.ora

```
[oracle@localhost admin]$ cat listener.ora
# listener.ora Network Configuration File: /u01/app/oracle/product/19.3.0/db_1/network/admin/listener.ora
# Generated by Oracle configuration tools.

LISTENER =
  (DESCRIPTION_LIST =
    (DESCRIPTION =
      (ADDRESS = (PROTOCOL = TCP)(HOST = test.com)(PORT = 1539))
      (ADDRESS = (PROTOCOL = IPC)(KEY = EXTPROC1521))
    )
  )
```

PASSWORD_LISTENER: 암호화된 패스워드 저장
PORT = 1539: Default Port

Oracle 12c 릴리즈 2부터 리스너 패스워드 기능 지원하지 않음

조치 방법

■ Listener 파일 수정

기본 포트 변경(1539) → 원하는 포트 번호
LOCAL_OS_AUTHENTICATION_LISTENER = OFF 내용 추가

■ Listener 접속 후 패스워드 변경

lsnrctl
LSNRCTL〉 change_password

■ 패스워드 변경 후 저장

LSNRCTL〉 save_config

SYSDBA 로그인 제한 설정

항목설명

SYSDBA 권한을 가진 계정에 대해 로그인 제한 설정이 적용되어 있는지 점검하여 비인가자에 의한 접근 차단할 수 있다.

진단 기준

양호

SYSDBA 로그인 제한 설정이 적용되어 있는 경우

취약

SYSDBA 로그인 제한 설정이 적용되어 있지 않은 경우

진단 방법

■ sqlnet.ora 파일 내용 확인

cat $ORACLE_HOME/network/admin/sqlnet.ora

SQLNET.AUTHENTICATION_SERVICES 옵션 확인

```
[oracle@localhost ~]$ cat $ORACLE_HOME/network/admin/sqlnet.ora
# sqlnet.ora Network Configuration File: /u01/app/oracle/product/19.3.0/d
b_1/network/admin/sqlnet.ora
# Generated by Oracle configuration tools.

NAMES.DIRECTORY_PATH= (TNSNAMES, EZCONNECT)

[oracle@localhost ~]$
```

조치 방법

■ sqlnet.ora 파일 내용 수정

vi $ORACLE_HOME/network/admin/sqlnet.ora

SQLNET.AUTHENTICATION_SERVICES=(NONE) 추가

```
NAMES.DIRECTORY_PATH= (TNSNAMES, EZCONNECT)

SQLNET.AUTHENTICATION_SERVICES=(NONE)
```

DBA 계정 Role 설정

항목설명

응용프로그램 또는 DBA 계정의 Role이 Public으로 설정되어 있으면, 일반 계정에서도 응용프로그램 테이블 및 DBA 테이블로 접근할 수 있어 정보 유출이 발생할 수 있다.

진단 기준

양호

DBA 계정의 Role이 Public으로 설정되어 있지 않은 경우

취약

DBA 계정의 Role이 Public으로 설정되어 있는 경우

진단 방법

■ role 확인

SQL〉 SELECT GRANTED_ROLE FROM DBA_ROLE_PRIVS WHERE GRANTEE='PUBLIC';

```
SQL> SELECT GRANTED_ROLE FROM DBA_ROLE_PRIVS WHERE GRANTEE='PUBLIC';

no rows selected
```

■ Restricted PL/SQL Package 설정 확인

SQL〉 SELECT GRANTEE, TABLE_NAME, PRIVILEGE FROM DBA_TAB_PRIVS WHERE GRANTEE='PUBLIC' AND PRIVILEGE='EXECUTE' AND TABLE_NAME IN('UTL_STMP', 'UTL_TCP', 'UTL_HTTP', 'UTL_FILE', 'DBMS_RANDOM', 'DBMS_LOB', 'DBMS_SQL', 'DBMS_JOB', 'DBMS_BACKUP_RESTORE', 'DBMS_OBFUSCATION_TOOLKIT', 'UTL_INADDR');

```
SQL> SELECT grantee,table_name,privilege FROM dba_tab_privs WHERE grantee='PUB
_RESTORE', 'DBMS_OBFUSCATION_TOOLKIT', 'UTL_INADDR');

GRANTEE                        TABLE_NAME                     PRIVILEGE
------------------------------ ------------------------------ ----------------------------------------
PUBLIC                         DBMS_LOB                       EXECUTE
PUBLIC                         UTL_TCP                        EXECUTE
PUBLIC                         UTL_HTTP                       EXECUTE
PUBLIC                         DBMS_SQL                       EXECUTE
PUBLIC                         UTL_FILE                       EXECUTE
PUBLIC                         UTL_INADDR                     EXECUTE
PUBLIC                         UTL_SMTP                       EXECUTE
PUBLIC                         DBMS_JOB                       EXECUTE
PUBLIC                         DBMS_OBFUSCATION_TOOLKIT       EXECUTE
PUBLIC                         DBMS_RANDOM                    EXECUTE
```

■ Public system privileges 설정 확인

SQL〉 SELECT * FROM DBA_SYS_PRIVS WHERE GRANTEE='PUBLIC';

조치 방법

■ 권한 취소

SQL〉 REVOKE ROLE FROM PUBLIC;

OS_ROLES, REMOTE_OS_AUTHENTICATION, REMOTE_OS_ROLES 설정

항목설명

OS_ROLES가 TRUE로 설정된 경우, 데이터베이스 접근 제어로 컨트롤되지 않는 OS 그룹에 의해 GRANT된 퍼미션이 허락된다. REMOTE_OS_ROLES가 TRUE로 설정된 경우, 원격 사용자가 OS의 다른 사용자로 속여 데이터베이스에 접근할 수 있다.

진단 기준

양호

OS_ROLES, REMOTE_OS_ROLES 설정이 FALSE로 설정되어 있는 경우

취약

OS_ROLES, REMOTE_OS_ROLES 설정이 TRUE로 설정되어 있는 경우

진단 방법

■ OS_ROLES 확인

SQL〉 SHOW PARAMETER OS_ROLES;

■ REMOTE_OS_ROLES 확인

SQL〉 SHOW PARAMETER REMOTE_OS_ROLES;

```
SQL> SHOW PARAMETER OS_ROLES;

NAME                                 TYPE        VALUE
------------------------------------ ----------- -------
os_roles                             boolean     FALSE
remote_os_roles                      boolean     FALSE
```

조치 방법

■ 설정 변경

SQL〉 ALTER SYSTEM SET OS_ROLES=FALSE SCOPE=spfile;
SQL〉 ALTER SYSTEM SET REMOTE_OS_ROLES=FALSE SCOPE=spfile;

최신 보안 패치 적용

항목설명

데이터베이스의 주요 보안 패치 등을 설치하지 않은 경우 공격자가 알려진 취약점을 이용하여 데이터베이스에 접근 가능하다.

진단 기준

양호
최신 보안 패치를 적용하고 있는 경우

취약
최신 보안 패치를 적용하고 있지 않은 경우

진단 방법

■ Oracle 버전 정보 확인

SQL〉 SELECT VERSION, PRODUCT FROM PRODUCT_COMPONENT_VERSION;

■ 릴리즈 확인

SQL〉 SELECT BANNER_FULL FROM V$VERSION;

```
SQL> SELECT BANNER_FULL FROM V$VERSION;

BANNER_FULL
--------------------------------------------------------------------------------
Oracle Database 19c Enterprise Edition Release 19.0.0.0.0 - Production
Version 19.3.0.0.0
```

조치 방법

■ 최신 보안 패치 적용

로그 활성화

항목설명

감사기록 정책이 설정되어 있지 않을 경우, 데이터베이스에 문제 발생 시 원인을 규명할 수 있는 자료가 존재하지 않아 이에 대한 대처 및 개선방안 수립이 어려움이 있다.

진단 기준

양호

DBMS의 감사 로그 저장 정책이 수립되어 있으며, 정책 설정이 적용되어 있는 경우

취약

DBMS의 감사 로그 저장하지 않거나, 정책 설정이 적용되어 있지 않은 경우

진단 방법

■ 데이터베이스 감사기록 정책 및 백업 정책 수립 확인

조치 방법

■ 데이터베이스 감사기록 정책 및 백업 정책 수립

2.22.

Apache

2.22. Apache

보안 설정(4개 항목), 접근 관리(2개 항목), 패치 관리(1개 항목) 총 3개 영역에서 7개 항목으로 구성된다.

[표 22] Apache 진단 체크리스트

구분	진단 항목
가. 보안 설정	웹 서비스 영역의 분리
	불필요한 파일 제거
	링크 사용 금지
	파일 업로드 및 다운로드 제한
나. 접근 관리	디렉터리 리스팅 제거
	웹 프로세스 권한 제한
라. 패치 관리	최신 보안 패치 적용

웹 서비스 영역의 분리

항목설명

Apache 설치 시 httdocs 디렉터리를 Document로 사용하면 공격에 이용될 수 있는 시스템 관련 정보가 노출될 수 있으므로 default DucumentRoot 경로를 변경하여 사용해야 한다.

진단 기준

양호

default Document를 사용하고 있지 않은 경우

취약

default Document를 사용하고 있는 경우

진단 방법

■ 기본 디렉터리 확인 (예시)

1) # cat [Apache 환경 설정 파일] | grep DocumentRoot

```
root@ubuntu:/etc/apache2/sites-available# cat 000-default.conf | grep DocumentRoot
        DocumentRoot /var/www/html
```

※ default : /var/www/html
※ 설치 OS 및 설치 방법에 따라 환경 설정 파일의 위치가 다름

조치 방법

■ 기본 디렉터리 변경

1) DocumentRoot를 별도의 경로로 변경

vi [Apache 환경 설정 파일]

```
        # value is not decisive as it is used as a last resort hos
        # However, you must set it for any further virtual host ex
        #ServerName www.example.com

        ServerAdmin webmaster@localhost
        DocumentRoot /var/test/apache_test

        # Available loglevels: trace8, ..., trace1, debug, info, n
        # error, crit, alert, emerg.
```

불필요한 파일 제거

항목설명

Apache 웹 서버 설치 시 기본으로 생성되는 매뉴얼 파일은 비인가자에게 시스템 정보 및 웹 서버 정보를 제공할 수 있으므로 제거해야 한다.

진단 기준

양호

매뉴얼 파일 및 디렉터리가 제거되어 있는 경우

취약

매뉴얼 파일 및 디렉터리가 제거되어 있지 않은 경우

진단 방법

■ 매뉴얼 디렉터리 존재 여부 확인 (예시)

1) # cd [Apache 설치 디렉터리]
2) # find . -name manual 명령어
3) httpd.conf 파일에 manual에 관련 설정 존재 여부 확인
4) # vi [Apache2 설정 디렉터리]/httpd.conf

조치 방법

■ 매뉴얼 디렉터리 삭제

1) # rm –rf [Apache2 설치 디렉터리/manual]
2) Apache 설정 파일에 매뉴얼에 관한 설정이 존재할 경우 삭제 또는 주석처리
3) # vi [Apahce 설정 파일]

링크 사용 금지

항목설명

심볼릭 링크가 활성화되어 있으면 기존의 웹 문서 이외의 파일 시스템 접근이 가능하기 때문에 편의성을 제공하는 반면 보안적으로 취약하므로 심볼릭 링크 사용을 금지해야 한다.

진단 기준

양호

심볼릭 링크, aliases 사용이 제한되어 있는 경우

취약

심볼릭 링크, aliases 사용이 제한되어 있지 않은 경우

진단 방법

■ 심볼릭 링크 사용 제한 여부 확인 (예시)

1) # cat /etc/apache2/apache2.conf | grep FollowSymLinks

```
root@ubuntu:/etc/apache2# cat apache2.conf | grep FollowSymLinks
        Options FollowSymLinks
        Options Indexes FollowSymLinks
#       Options Indexes FollowSymLinks
root@ubuntu:/etc/apache2#
```

■ aliases 사용 제한 여부 확인 (예시)

1) # cat [Apahce Alias 설정 파일] | grep Alias

```
root@ubuntu:/etc/apache2/mods-enabled# cat alias.conf | grep Alias
        # Aliases: Add here as many aliases as you need (with no limit). The format is
        # Alias fakename realname
        Alias /icons/ "/usr/share/apache2/icons/"
```

※ Options FollowSymLinks 존재 = 활성화 (취약)

조치 방법

■ 심볼릭 링크 사용 제한

1) 환경 설정 파일 내에 FollowSymLinks Options 중 Indexes 제거

```
root@ubuntu:/etc/apache2# cat apache2.conf | grep FollowSymLinks
        Options FollowSymLinks
        Options Indexes FollowSymLinks
#       Options Indexes FollowSymLinks
root@ubuntu:/etc/apache2#
```

■ Alias 사용 제한

1) Alias 환경 설정 파일 내에 Alias 사용 제한 (주석처리)

파일 업로드 및 다운로드 제한

항목설명

파일 업로드, 다운로드 시에 불필요한 파일 또는 대용량의 파일로 인해 서비스가 불능 상태에 빠질 수 있다. 따라서 가능한 파일 업로드, 다운로드 용량을 제한해야 한다.

진단 기준

양호

파일 업로드 및 다운로드 용량을 제한하고 있는 경우

취약

파일 업로드 및 다운로드 용량을 제한하고 있지 않은 경우

진단 방법

■ 파일 업로드 및 다운로드 용량 제한

1) # cat /etc/apache2/apache2.conf | grep LimitRequestBody

※ 출력되는 값이 없으면 용량을 제한하고 있지 않은 상태 (취약)

조치 방법

■ 파일 업로드 및 다운로드 용량 제한 설정

1) # vi /etc/apache2/apache2.conf

```
<Directory />
        Options FollowSymLinks
        AllowOverride None
        Require all denied
        LimitRequestBody 10240000
</Directory>

<Directory /usr/share>
        AllowOverride None
        Require all granted
        LimitRequestBody 20480000
</Directory>

<Directory /var/www/>
        Options Indexes FollowSymLinks
        AllowOverride None
        Require all granted
        LimitRequestBody 20480000
```

디렉터리 리스팅 제거

항목설명

디렉터리 검색 기능이 활성화되어 있는 경우 외부에서 디렉터리 내 모든 파일에 접근이 가능하여 WEB 서버 구조를 파악하여 공격을 시도할 수 있으며 백업 파일이나 소스 파일 등 공개되면 안 되는 중요 파일이 노출될 수 있다.

진단 기준

양호
디렉터리 검색 기능을 사용하지 않는 경우

취약
디렉터리 검색 기능을 사용하는 경우

진단 방법

■ 디렉터리 검색 기능 사용 여부 확인

1) 환경 설정 파일에서 indexes 옵션이 설정되어 있는지 확인

```
<Directory />
        Options FollowSymLinks
        AllowOverride None
        Require all denied
</Directory>

<Directory /usr/share>
        AllowOverride None
        Require all granted
</Directory>

<Directory /var/www/>
        Options Indexes FollowSymLinks
        AllowOverride None
        Require all granted
</Directory>
```

조치 방법

■ 디렉터리 검색 기능 제거

1) 환경 설정 파일 Options Indexes FollowSymLinks에서 'Indexes'를 제거하거나, '-indexex' 옵션 설정

```
<Directory /var/www/>
        Options FollowSymLinks
```

```
<Directory /var/www/>
        Options -Indexes FollowSymLinks
```

2) Options Indexes FollowSymLinks 주석처리

```
<Directory /var/www/>
#       Options Indexes FollowSymLinks
        AllowOverride None
        Require all granted
</Directory>
```

웹 프로세스 권한 제한

항목설명

Unix 시스템에서 apache 서버 데몬이 root 권한으로 운영되는 경우 Web Application 취약점 또는 버퍼 오버플로우로 인하여 root 권한을 획득할 수 있으므로 apache 서버 데몬이 root 권한으로 운영되지 않도록 별도 계정으로 실행해야 한다.

진단 기준

양호
데몬이 root 권한으로 구동되지 않는 경우

취약
데몬이 root 권한으로 구동되는 경우

진단 방법

■ 웹 서버 프로세스 소유자의 권한 확인

1) # ps –ef | grep apache2

```
root@ubuntu:/etc/apache2# ps -ef | grep apache2
root        4163       1  0 15:22 ?        00:00:00 /usr/sbin/apache2 -k start
www-data    4166    4163  0 15:22 ?        00:00:00 /usr/sbin/apache2 -k start
www-data    4167    4163  0 15:22 ?        00:00:00 /usr/sbin/apache2 -k start
www-data    4284       1  0 15:22 ?        00:00:00 /usr/bin/htcacheclean -d 120 -p /var/cache/apache2/mod_cache_disk -l 300M -n
root        8124    4643  0 16:38 pts/0    00:00:00 grep --color=auto apache2
root@ubuntu:/etc/apache2#
```

※ 별도의 계정이 아닌 root 또는 root 권한으로 구동 (취약)

조치 방법

■ apache 데몬 user/group 변경 (예시)

1) # vi [Apache 설정 디렉터리]/envvars

2) APACHE_RUN_USER, APACHE_RUN_GROUP을 별도의 계정으로 변경

```
export APACHE_RUN_USER=www-data
export APACHE_RUN_GROUP=www-data
# temporary state file location. This migh
```

3) 웹 프로세스 구동 사용자 계정을 변경했을 경우, 로그인이 되지 않도록 계정에 nologin 설정

vi /etc/passwd

```
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
```

비고

※ 설치 OS, 설치 방법에 따라 설정 파일 이름, 위치가 다름

최신 보안 패치 적용

항목설명

최신 보안 패치를 적용하지 않으면 해당 버전의 취약점으로 인해 침해사고가 발생할 수 있으므로 주기적으로 공식 릴리즈 사이트를 방문하여 보안 패치를 적용해야 한다.

진단 기준

양호

최신 보안 패치를 적용한 경우

취약

최신 보안 패치를 적용하지 않은 경우

진단 방법

■ 현재 버전 확인

1) # apache2 –v

```
root@ubuntu:/etc/apache2# apache2 -v
Server version: Apache/2.4.52 (Ubuntu)
Server built:   2023-10-26T13:44:44
root@ubuntu:/etc/apache2#
```

조치 방법

■ 보안 패치 적용

1) 보안 취약점이 존재하지 않는 버전으로 보안패치를 적용해야 함

※ 최신 버전을 사용하도록 권고하고 있으나 시스템 운영상 적용이 어려운 경우 최신이 아닌 취약점이 존재하지 않는 버전도 허용하고 있음

비고

※ 보안 패치를 적용할 경우, 시스템 영향도를 파악하여 충분한 테스트 후 적용 권고

2.23.

Nginx

2.23. Nginx

보안 설정(4개 항목), 접근 관리(2개 항목), 패치 관리(1개 항목) 총 3개 영역에서 7개 항목으로 구성된다.

[표 23] Nginx 진단 체크리스트

구분	진단 항목
가. 보안 설정	웹 서비스 영역의 분리
	불필요한 파일 제거
	링크 사용 금지
	파일 업로드 및 다운로드 제한
나. 접근 관리	디렉터리 리스팅 제거
	웹 프로세스 권한 제한
라. 패치 관리	최신 보안 패치 적용

웹 서비스 영역의 분리

항목설명

Nginx 설치 시 html 디렉터리를 DocumentRoot로 사용하고 있는데 html 디렉터리는 공격에 이용될 수 있는 시스템 관련 정보도 포함하고 있으므로 이를 다른 경로로 변경하여 사용해야 한다.

진단 기준

양호

default DocumentRoot를 사용하고 있는 경우

취약

default DocumentRoot를 사용하고 있지 않은 경우

진단 방법

■ 기본 디렉터리 위치 확인 (예시)

1) # cat [Nginx 환경 설정 파일] | grep root

```
root@ubuntu:/etc/nginx/sites-available# cat default | grep root
        root /var/www/html;
        # deny access to .htaccess files, if Apache's document root
#       root /var/www/example.com;
root@ubuntu:/etc/nginx/sites-available#
```

※ default : /var/www/html
※ 설치 OS 및 설치 방법에 따라 환경 설정 파일의 위치가 다름

조치 방법

■ 기본 디렉터리 위치 변경 (예시)

1) # vi [Nginx 환경 설정 파일]

```
        root /var/test/nginx_test
```

불필요한 파일 제거

항목설명

Nginx 설치 시 기본으로 생성되는 매뉴얼 파일 및 테스트 파일은 외부 침입자에게 시스템에 대한 정보를 제공할 수 있으므로 반드시 제거해야 한다.

진단 기준

양호

매뉴얼 파일 및 디렉터리가 제거되어 있는 경우

취약

매뉴얼 파일 및 디렉터리가 제거되어 있지 않은 경우

진단 방법

■ 불필요한 디렉터리 존재 여부 확인

1) 불필요한 파일 존재 여부 확인 (*.old, *.bak, 테스트 파일 등)

ls –al [Nginx 설정 디렉터리]

```
root@ubuntu:/etc/nginx# ls -al
합 계  80
drwxr-xr-x   8 root root  4096 12월   6 17:38 .
drwxr-xr-x 143 root root 12288 12월   6 17:32 ..
drwxr-xr-x   2 root root  4096  5월  31  2023 conf.d
-rw-r--r--   1 root root  1125  5월  31  2023 fastcgi.conf
-rw-r--r--   1 root root  1055  5월  31  2023 fastcgi_params
-rw-r--r--   1 root root  2837  5월  31  2023 koi-utf
-rw-r--r--   1 root root  2223  5월  31  2023 koi-win
-rw-r--r--   1 root root  3957  5월  31  2023 mime.types
drwxr-xr-x   2 root root  4096  5월  31  2023 modules-available
drwxr-xr-x   2 root root  4096 12월   6 17:32 modules-enabled
-rw-r--r--   1 root root  1447  5월  31  2023 nginx.conf
-rw-r--r--   1 root root   180  5월  31  2023 proxy_params
-rw-r--r--   1 root root   636  5월  31  2023 scgi_params
drwxr-xr-x   2 root root  4096 12월   6 17:45 sites-available
drwxr-xr-x   2 root root  4096 12월   6 17:32 sites-enabled
drwxr-xr-x   2 root root  4096 12월   6 17:32 snippets
-rw-r--r--   1 root root   664  5월  31  2023 uwsgi_params
-rw-r--r--   1 root root  3071  5월  31  2023 win-utf
```

조치 방법

■ 불필요한 파일 삭제

1) 주기적으로 Nginx 설정 디렉터리 내 불필요한 파일(test, old, bak 파일 등)을 확인
2) # cd [Nginx 설치 디렉터리]
3) # rm –rf [불필요한 파일명]

비고

※ 파일 삭제 시, 시스템에 영향이 가는지 충분히 테스트를 진행하고 삭제 진행

링크 사용 금지

항목설명

심볼릭 링크 기능은 일반 사용자들이 시스템 중요 파일에 접근할 수 있는 보안 문제를 일으킨다. 따라서 반드시 심볼릭 링크 기능을 제한해야 한다.

진단 기준

양호

심볼릭 링크, aliases 사용을 제한하고 있는 경우

취약

심볼릭 링크, aliases 사용을 제한하고 있지 않은 경우

진단 방법

■ 심볼릭 링크, aliases 사용 제한 여부 확인

1) # car [Nginx 설정 파일] | grep “disable_symlinks

```
root@ubuntu:/etc/nginx# cat nginx.conf | grep "disable_symlinks off"
root@ubuntu:/etc/nginx#
```

※ default : 설정값이 존재하지 않음 (취약)

조치 방법

■ 심볼릭 링크 제한

1) # vi [Nginx 설정 파일]

```
        disable_symlinks off;

        # server_names_hash_bucket_size 64;
```

파일 업로드 및 다운로드 제한

항목설명

공격자가 파일 업로드, 다운로드 기능을 이용하여 불필요한 파일 및 대용량 파일로 서비스 불능 상태를 발생시킬 수 있다. 따라서 불필요한 파일을 관리해야 하며 업로드, 다운로드 용량을 제한해야 한다.

진단 기준

양호

파일 업로드 및 다운로드 용량을 제한한 경우

취약

파일 업로드 및 다운로드 용량을 제한하지 않은 경우

진단 방법

■ 파일 업로드 및 다운로드 용량 제한 설정 확인

1) # cat [Ningx 설정 파일] | grep clien_max_body_size

※ default : 설정값이 존재하지 않음 (취약)

조치 방법

■ 파일 업로드 및 다운로드 용량 제한 설정

1) # vi [Nginx 설정 파일]

```
        disable_symlinks off;
        client_max_body_size 20M
```

디렉터리 리스팅 제거

항목설명

디렉터리 검색 기능이 활성화되어 있는 경우 외부에서 공격자가 디렉터리 내의 모든 파일에 대한 접근이 가능하며 Web 서버의 구조 파악 및 중요 파일도 열람할 수 있으므로 디렉터리 검색 기능을 제한해야 한다.

진단 기준

양호
디렉터리 검색 기능을 사용하지 않는 경우

취약
디렉터리 검색 기능을 사용하는 경우

진단 방법

■ 디렉터리 검색 기능 사용 여부 확인

1) # cat [Ningx 설정 파일] | grep autoindex

※ default : 설정값이 존재하지 않음 (취약)

조치 방법

■ 디렉터리 검색 기능 비활성화

1) # vi [Nginx 설정 파일]

```
        location / {
                # First attempt to serve request as file, then
                # as directory, then fall back to displaying a 404.
                try_files $uri $uri/ =404;
                autoindex off;
```

웹 프로세스 제한

항목설명

Web 서버 데몬이 root 계정 또는 root 권한으로 운영될 경우 Wen Application 취약점 또는 버퍼 오버플로우로 인하여 root 권한을 획득할 수 있다. 따라서 서버 데몬이 root 권한이 아닌 별도의 계정으로 운영되도록 해야 한다.

진단 기준

양호

데몬이 root 또는 root 권한으로 구동되고 있지 않은 경우

취약

데몬이 root 또는 root 권한으로 구동되고 있는 경우

진단 방법

■ Nginx 프로세스 소유자 권한 확인

1) # ps –ef | grep nginx

```
root@ubuntu:/etc/nginx# ps -ef | grep nginx
root        5322       1  0 09:48 ?        00:00:00 nginx: master process /usr/sbin/nginx -g daemon on; master_process on;
www-data    5323    5322  0 09:48 ?        00:00:00 nginx: worker process
www-data    5324    5322  0 09:48 ?        00:00:00 nginx: worker process
www-data    5325    5322  0 09:48 ?        00:00:00 nginx: worker process
www-data    5326    5322  0 09:48 ?        00:00:00 nginx: worker process
root        7194    2631  0 10:24 pts/0    00:00:00 grep --color=auto nginx
```

조치 방법

■ Nginx 데몬 user/group 변경

1) user 지시자에 root가 아닌 별도의 계정으로 변경

vi [Nginx 설정 파일]

```
user www-data;
worker_processes auto;
pid /run/nginx.pid;
include /etc/nginx/modules-enabled/*.conf;
```

2) 설정한 별도의 계정이 로그인할 수 없도록 nologin 설정

```
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
```

최신 보안 패치 적용

항목설명

공격자에 의해 해당 버전 취약점 공격이 발생하여 침해 사고가 발생할 수 있으므로 공식 사이트를 참고하여 제공되는 최신 보안 패치를 적용해야 한다.

진단 기준

양호

최신 보안 패치를 적용한 경우

취약

최신 보안 패치를 적용하지 않은 경우

진단 방법

■ 현재 Nginx 버전 확인

1) # [Nginx 실행 디렉터리]/nginx -v

조치 방법

■ 보안 패치 적용

1) 보안 취약점이 존재하지 않는 버전으로 보안패치를 적용해야 함

※ 최신 버전을 사용하도록 권고하고 있으나 시스템 운영상 적용이 어려운 경우 최신이 아닌 취약점이 존재하지 않는 버전도 허용하고 있음

비고

※ 보안 패치를 적용할 경우, 시스템 영향도를 파악하여 충분한 테스트 후 적용 권고

2.24.

IIS

2.24. IIS

보안 설정(9개 항목), 접근 관리(2개 항목) 총 2개 영역에서 11개 항목으로 구성된다.

[표 24] IIS 진단 체크리스트

구분	진단 항목
가. 보안 설정	서비스 구동 점검
	불필요한 파일 제거
	CGI 실행 제한
	링크 사용 금지
	파일 업로드 및 다운로드 제한
	데이터 파일 ACL 적용
	미사용 스크립트 매핑 제거
	Exec 명령어 쉘 호출 진단
	WebDAV 비활성화
나. 접근 관리	디렉터리 리스팅 제거
	상위 디렉터리 접근 금지

서비스 구동 점검

항목설명

IIS 서비스는 Web, FTP 등의 서비스를 제공해주는 유용한 서비스이지만 프로파일링, 서비스 거부, 불법적인 접근, 임의의 코드 실행, 정보 공개, 바이러스, 웜, 트로이 목마 등의 위협에 노출될 수 있다.

진단 기준

양호

불필요한 웹사이트가 구동 중이지 않은 경우

취약

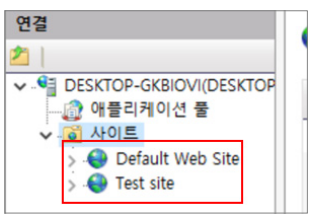
불필요한 웹사이트가 구동 중인 경우

진단 방법

■ 불필요한 웹 사이트 확인

1) Win + R → inermgr 명령어 입력 → 컴퓨터 이름 → 연결 → 사이트

2) 웹 사이트 목록 중 불필요한 사이트가 존재하는지 확인

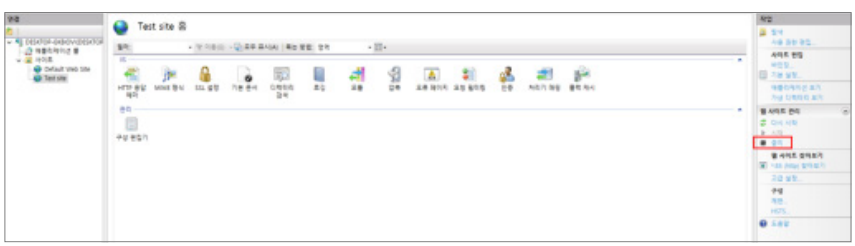


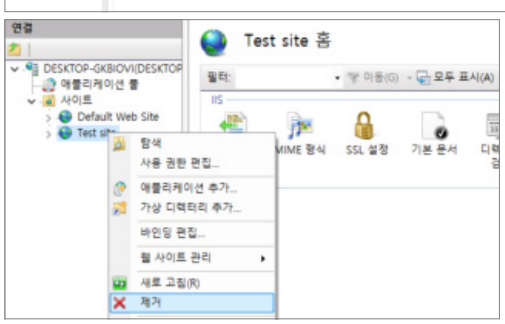
조치 방법

■ 불필요한 웹 사이트 중지 및 제거

1) Win + R → inetmgr 명령어 입력 → 컴퓨터 이름 → 연결 → 사이트

2) 불필요한 웹 사이트 중지 또는 제거





※ 불필요한 웹 사이트가 구동 중일 경우, 웹 사이트 중지/제거 권고

불필요한 파일 제거

항목설명

IIS 초기에 생성되는 샘플 파일과 폴더가 공격자에게 이용될 수 있으므로 해당 디폴트 생성 파일 및 폴더들을 제거하는 것이 안전하다.

진단 기준

양호

해당 웹 사이트에 IISSamples, IISHelp 가상 디렉터리가 존재하지 않는 경우

취약

해당 웹 사이트에 IISSamples, IISHelp 가상 디렉터리가 존재하는 경우

진단 방법

■ 운영 중인 웹 사이트에서 불필요한 파일 확인

1) 운영 중인 웹 사이트에서 샘플 디렉터리가 존재하는지 확인

※ IIS 7.0 이상 버전에서는 가상 디렉터리가 존재하지 않으므로 양호로 처리함

조치 방법

■ 운영 웹 사이트 불필요한 샘플 파일 삭제

1) 샘플 파일이 존재하는 경우 삭제

CGI 실행 제한

항목설명

CGI 스크립트는 정해진 디렉터리에서만 실행되도록 해야 한다. 게시판이나 자료실과 같이 업로드되는 파일이 저장되는 디렉터리에 CGI 스크립트가 실행 가능할 경우, 악의적인 파일을 업로드하고 이를 실행하여 시스템의 중요 정보가 유출될 수 있으며 침해 사고로 이어질 수 있다.

진단 기준

양호

지정하지 않은 CGI 모듈 허용 및 지정하지 않은 ISAPI 모듈 허용을 사용하지 않을 경우

취약

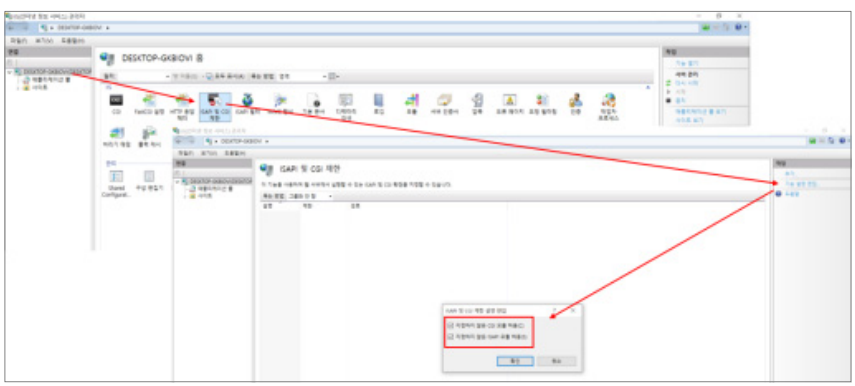
지정하지 않은 CGI 모듈 허용 및 지정하지 않은 ISAPI 모듈 허용을 사용할 경우

진단 방법

■ IIS 관리자에서 확인

1) IIS 관리자 → 서버 선택 → ISAPI 및 CGI 제한 → 기능 열기 → 작업 → 기능 설정 편집

2) 지정하지 않은 CGI/ISAPI 모듈 허용 2개 모두 체크 해체되어 있는지 확인



■ IIS 관리자에서 확인

1) 설정 파일(C:\Windows\System32\inetsrv\config\applicationHost.config)에서 확인 "notListedIsapisAllowed", "notListedCgisAllowed" 두 설정이 존재하지 않거나 false인지 확인

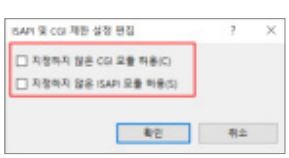
※ 두 설정값이 존재하지 않거나 false인 경우 양호함

조치 방법

■ IIS 관리자에서 설정 변경

1) IIS 관리자 → 서버 선택 → ISAPI 및 CGI 제한 → 기능 열기 → 작업 → 기능 설정 편집

2) 지정하지 않은 CGI/ISAPI 모듈 허용 2개 설정 모두 체크 해제



링크 사용 금지

항목설명

공개적인 웹 콘텐츠 디렉터리 안에서 서버의 다른 디렉터리나 파일들에 접근할 수 있는 심볼릭 링크, alias, 바로 가기 등을 사용하지 않도록 해야 한다.

진단 기준

양호

홈 디렉터리에 바로 가기 등의 링크 파일이 존재하지 않는 경우

취약

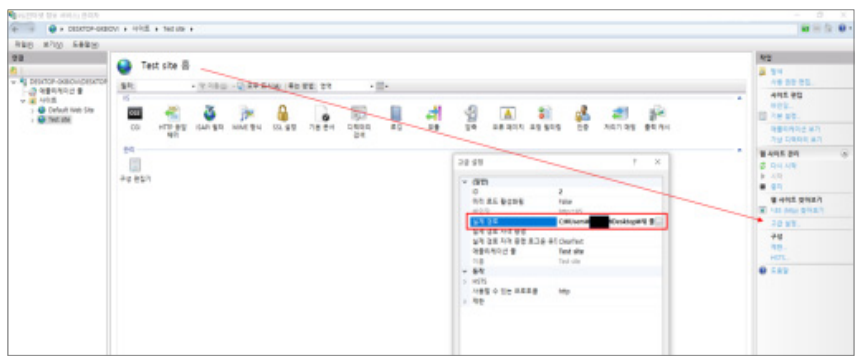
홈 디렉터리에 바로 가기 등의 링크 파일이 존재하는 경우

진단 방법

■ IIS 관리자에서 확인

1) IIS 관리자 → 서버 선택 → 웹 사이트 → 고급 설정 → 실제 경로

2) 해당 경로에 링크 파일이 존재하는지 확인



조치 방법

■ 링크 파일 삭제

1) IIS 관리자 → 서버 선택 → 웹 사이트 → 고급 설정 → 실제 경로
2) 해당 경로 확인
3) 경로로 이동 링크 파일 삭제

파일 업로드 및 다운로드 제한

항목설명

불필요한 파일 업로드, 다운로드 시에, 대량의 업로드, 다운로드로 인한 서비스 불능 상태가 발생한다. 따라서 불필요한 업로드와 다운로드는 허용하지 않으며, 웹서버에 의해 처리되지 못하게 해야 한다. 또한 자동이나 수동으로 파일의 보안성 검토를 하도록 해야 한다.

진단 기준

양호

웹서비스 서버의 업로드, 다운로드 용량을 제한한 경우

취약

웹서비스 서버의 업로드, 다운로드 용량을 제한하지 않은 경우

진단 방법

■ IIS 관리자에서 확인

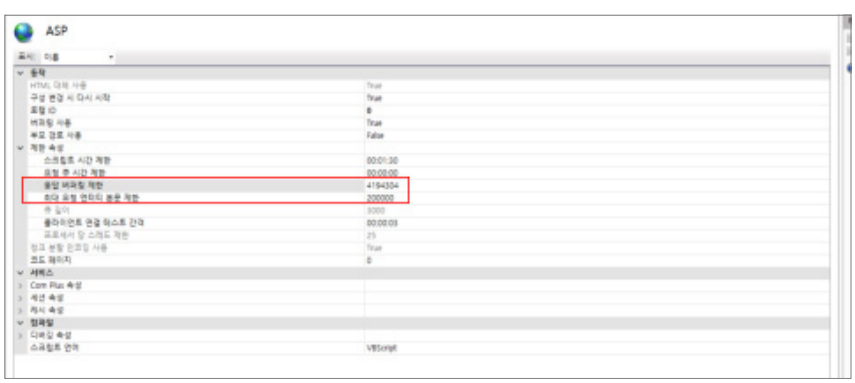
1) IIS 관리자 → 서버 선택 → 웹 사이트 → ASP → 기능 열기 → 제한 속성 → 응답 버퍼링 / 최대 요청 엔터티 본문 제한 설정 2개 설정 모두 확인

2) 파일 업로드 용량 설정 변경
IIS 관리자 → 서버 선택 → 웹 사이트 → 요청 필터링 → 기능 열기 → 기능 설정 편집 → 허용되는 최대 콘텐츠 길이 설정값 변경

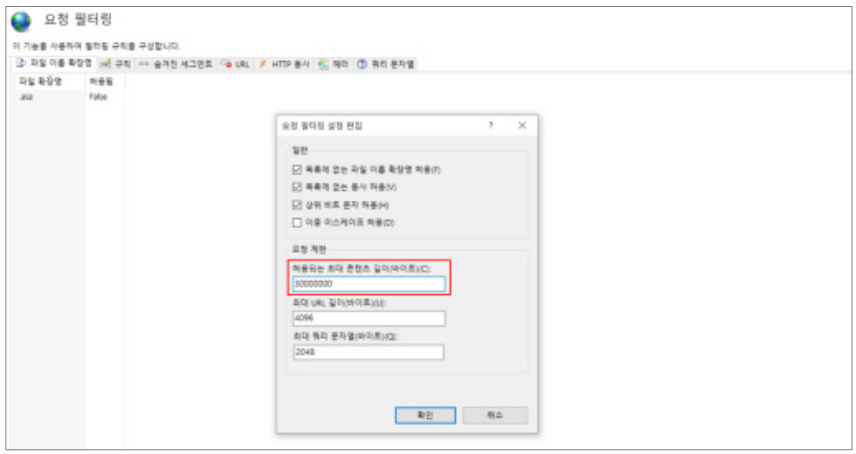
조치 방법

■ IIS 관리자에서 확인

1) 파일 다운로드 용량 설정 변경
IIS 관리자 → 서버 선택 → 웹 사이트 → ASP → 고급 설정 → 제한 속성 → 응답 버퍼링 제한 / 최대 요청 엔터티 본문 제한 2가지 설정값 적용



2) 파일 업로드 용량 설정 변경
IIS 관리자 → 서버 선택 → 웹 사이트 → 요청 필터링 → 기능 열기 → 기능 설정 편집 → 허용되는 최대 콘텐츠 길이 설정값 적용



데이터 파일 ACL 적용

항목설명

웹 데이터 파일에 ACL을 부여함으로써 권한 없는 사용자로부터의 실행 및 읽기 제한을 설정할 수 있다. 향후 필요한 경우 IIS를 설치해 운용한다면 웹 데이터 파일에 대한 ACL을 부여하는 것이 바람직하다. ACL을 설정할 때에는 다음과 같은 사항을 참고하여 설정해야 한다.

진단 기준

양호

홈 디렉터리 내에 있는 하위 파일들에 대해 Everyone 권한이 존재하지 않는 경우

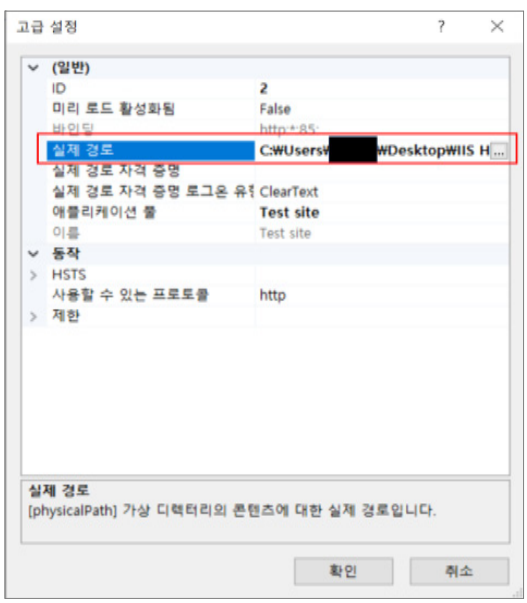
취약

홈 디렉터리 내에 있는 하위 파일들에 대해 Everyone 권한이 존재하는 경우

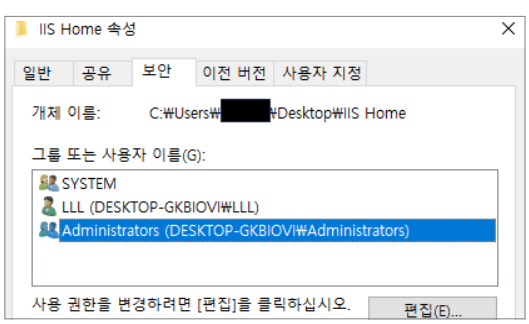
진단 방법

■ IIS 관리자에서 확인

1) IIS 관리자 → 서버 선택 → 웹 사이트 → 고급 설정 → 실제 경로 확인



2) 해당 경로의 데이터 파일 접근 권한 확인



조치 방법

■ 데이터 파일 ACL 적용

1) 실제 경로 → 해당 디렉터리 내 비고란의 파일들의 접근 권한에서 불필요한 Everyone 권한 제거

비고

파일 형식	엑세스 제어 목록
CGI(*.exe,*.dll,*.cmd,*.pl)	Everyone(X), Administrator/System(전체 제어)
스크립트(*.asp)	Everyone(X), Administrator/System(전체 제어)

미사용 스크립트 매핑 제거

항목설명

사용하지 않는 스크립트 매핑은 보안에 위협이 될 수 있으므로 개발자와 협의하여 불필요한 매핑인지 확인한 후에 제거해야 한다. .asp나 .shtm 과 같은 확장자들은 특정 DLL 파일과 매핑되어 있어, 이러한 파일들에 대한 요청이 들어오면 해당 DLL에 의해 처리된다. 이러한 매핑 중에는 사용되지 않는 것들이 있어서 이를 제거해주는 것이 보안에 도움이 된다. ida , .idc, .idq, .printer, .htr, .htw 확장자는 Buffer overflow 공격 위험이 존재하므로 삭제를 권고한다.

진단 기준

양호

취약한 매핑(.htr .idc .stm .shtm .shtml .printer .htw .ida .idq)이 존재하지 않는 경우

취약

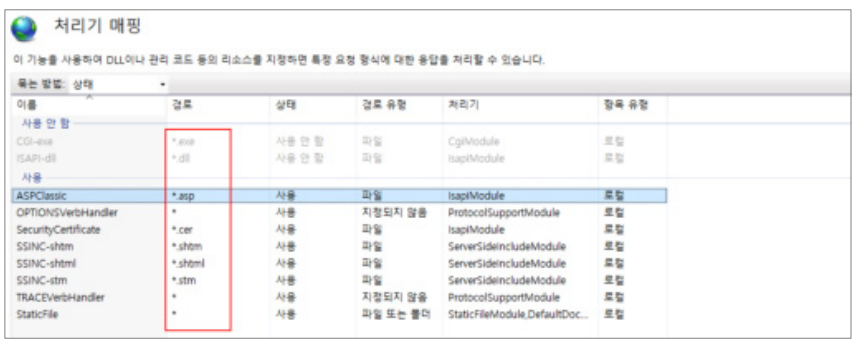
취약한 매핑(.htr .idc .stm .shtm .shtml .printer .htw .ida .idq)이 존재하는 경우

진단 방법

■ IIS 관리자에서 확인

1) IIS 관리자 → 서버 선택 → 웹 사이트→ 처리기 매핑 → 기능 열기

2) 취약한 매핑이 존재하는지 확인

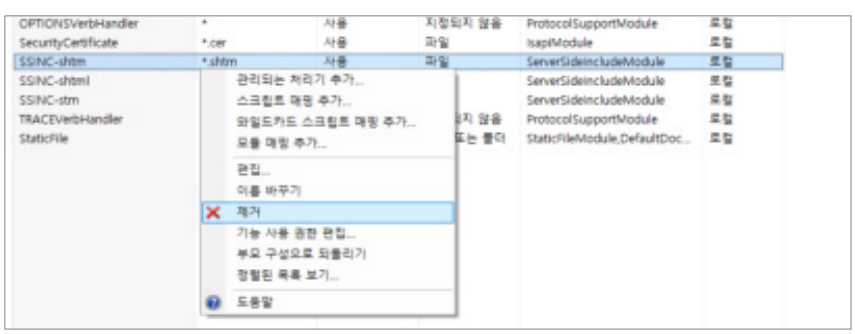


조치 방법

■ 취약한 매핑 제거

1) IIS 관리자 → 서버 선택 → 웹 사이트 → 처리기 매핑 → 기능 열기

2) 취약한 매핑 우클릭 → 제거



Exec 명령어 쉘 호출 진단

항목설명

명령어가 Web 서버에서 임의의 명령을 호출하도록 사용될 수 있다. 임의의 명령을 호출하도록 설정되어 있다면 아래의 조치 방법에 따라서 설정을 변경하여 주는 것이 안전하다. HTML 페이지에서 웹 서버에 명령어 실행은 # exec 명령어를 통해 활용할 수 있다. 기본값으로 IIS 4.0에서는 사용할 수 있으나, IIS 5.0에서는 기본값으로 사용이 불가하다. 기본값은 서버 측의 허가되지 않은 실행 구의 동작을 방지하기 위해 변경되었다.

진단 기준

양호

해당 레지스트리 값이 0인 경우, 또는 IIS 5.0 이상에서 해당 레지스트리 값이 존재하지 않을 경우

취약

해당 레지스트리 값이 1인 경우

진단 방법

■ 레지스트리 편집기에서 확인

1) 시작 → Win + R → regedit

2) HKLM\SYSTEM\CuttentContorlSet\services\W3SVC\Parameters

3) SSIEnableCmdDirective 값이 0으로 존재하는지 확인

이름	종류	데이터
(기본값)	REG_SZ	(값 설정 안 됨)
AccessDeniedMessage	REG_SZ	Error: Access is Denied.
InstallPath	REG_EXPAND_SZ	%windir%₩system32₩inetsrv
MajorVersion	REG_DWORD	0x0000000a (10)
MinorVersion	REG_DWORD	0x00000000 (0)
ServiceDll	REG_EXPAND_SZ	%windir%₩system32₩inetsrv₩iisw3adm.dll

※ defalut : 레지스트리 값이 존재하지 않음 (false로 설정됨)
※ IIS v5.0 이상에서 레지스트리 값은 false

조치 방법

■ 레지스트리값 수정

1) 시작 → Win + R → regedit

2) HKLM\SYSTEM\CuttentContorlSet\services\W3SVC\Parameters

3) 우클릭 → DWORD → SSIEnableCmdDirective 레지스트리 값 0으로 추가
(레지스트리 값이 없는 경우 새로 생성)

이름	종류	데이터
(기본값)	REG_SZ	(값 설정 안 됨)
AccessDeniedMessage	REG_SZ	Error: Access is Denied.
InstallPath	REG_EXPAND_SZ	%windir%₩system32₩inetsrv
MajorVersion	REG_DWORD	0x0000000a (10)
MinorVersion	REG_DWORD	0x00000000 (0)
ServiceDll	REG_EXPAND_SZ	%windir%₩system32₩inetsrv₩iisw3adm.dll
SSIEnableCmdDirective	REG_DWORD	0x00000000 (0)

비고

※ 레지스트리 값 추가 후, 웹 서비스 정지 후 재시작
C:〉 net stop w3svc
C:〉 net start w3svc

WebDAV 비활성화

항목설명

악의적으로 작성된 요청을 이용하여 인증을 우회할 경우 패스워드로 보호된 WebDAV의 자원에 접근할 수 있으며, 매개 변수를 점검하지 않을 경우 버퍼 오버런이 일어날 수 있다.

진단 기준

양호

비고)의 양호 기준 중 한 가지라도 해당하는 경우

취약

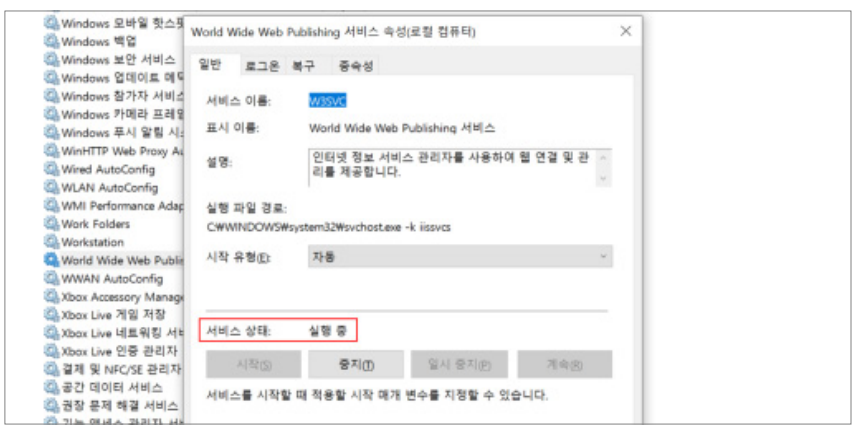
비고)의 양호 기준 중 모두 해당하지 않는 경우

진단 방법

■ 서비스에서 IIS 구동 상태 확인

1) Win + R → services.msc 입력 → World Wide Web Publishing → 우클릭 → 속성

2) 서비스 상태 확인

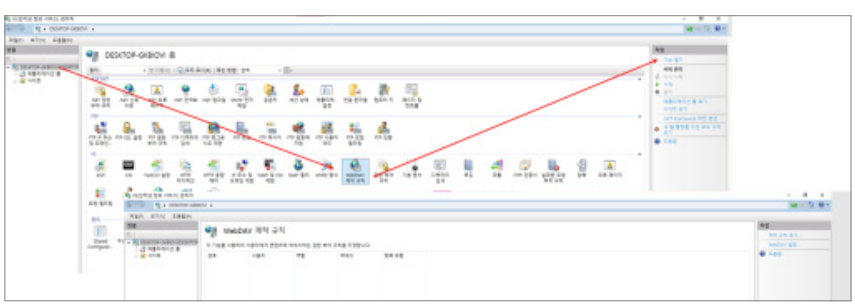


※ WebDAV 레지스트리 값 경로 :
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Service\W3SVC\Parameters

■ IIS 관리자에서 구동 상태 확인

1) IIS 관리자 → 서버 선택 → WebDAV 제작 규칙 → 기능 열기

2) 서비스 상태 확인



조치 방법

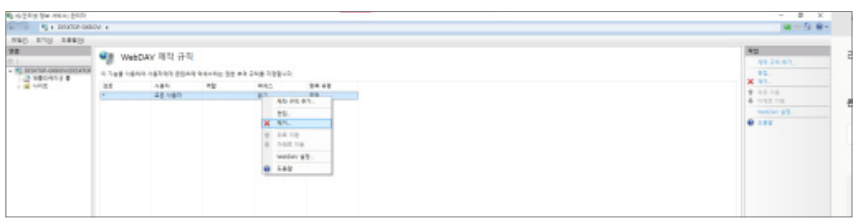
■ 서비스에서 IIS 구동 비활성화

1) Win + R → services.msc 입력 → World Wide Web Publishing → 우클릭 → 속성

2) W3SVC 중지

■ IIS 관리자에서 IIS 구동 비활성화

1) IIS 관리자 → 서버 선택 → WebDAV 제작 규칙 → 기능 열기 → 규칙 우클릭 → 제거



비고

양호	취약
IIS 서비스를 사용하지 않는 경우	양호 기준 중 모두 해당하지 않는 경우 (Win2003, Win2008일 경우 1, 4번만 확인)
레지스트리의 DisableWebDAV 값이 1로 설정된 경우	
Windows NT, 2000 서비스 팩 4 이상이 설치된 경우	
Win2003, Win2008, Win2012에서 WebDAV가 금지된 경우	

디렉터리 리스팅 제거

항목설명

디렉터리 검색 기능이 활성화되어 있으면 IIS 기본파일(default.asp, default.htm)이 서버에 없는 경우 해당 디렉터리에 존재하는 모든 파일의 리스트를 보여주어, Web 서버 구조 노출 및 주요 설정 파일의 내용이 유출될 가능성이 있다.

진단 기준

양호

디렉터리 검색 기능이 활성화되어 있는 경우

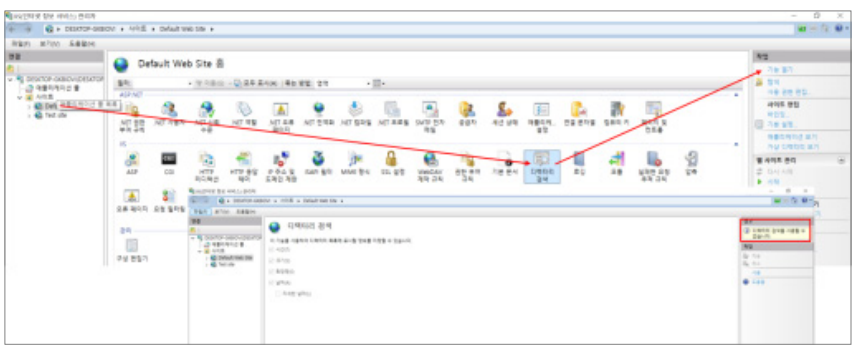
취약

디렉터리 검색 기능이 비활성화되어 있는 경우

진단 방법

■ IIS 관리자에서 확인

1) IIS 관리자 → 해당 웹 사이트 → 디렉터리 검색 → 기능 열기 → 디렉터리 리스팅 활성화 확인



조치 방법

■ IIS 관리자에서 비활성화

1) IIS 관리자 → 해당 웹 사이트 → 디렉터리 검색 → 기능 열기 → 디렉터리 리스팅 비활성화

상위 디렉터리 접근 금지

항목설명

상위경로로 이동하는 것이 가능할 때 하위경로에 접속하여 상위로 이동함으로써 해킹을 당할 위험이 있으며, Unicode 버그 및 서비스 거부 공격에 이용당하기 쉬우므로 “.”와 같은 상위 경로를 사용하지 못하도록 설정하는 것이 바람직하다.
※ “.”는 Unicode 버그, 서비스 거부와 같은 공격에 쉽게 이용되므로 허용하지 않는 것을 권장한다.

진단 기준

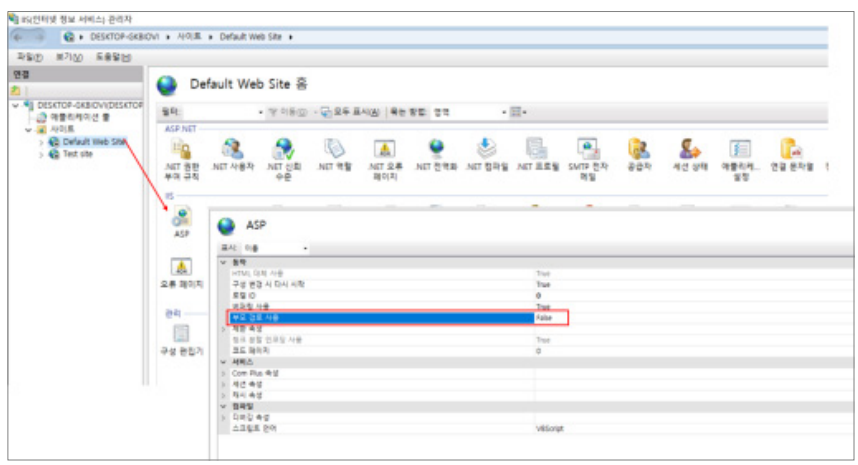
양호
상위 경로 이동 기능을 제거한 경우

취약
상위 경로 이동 기능을 제거하지 않은 경우

진단 방법

■ IIS 관리자에서 확인

1) IIS 관리자 → 해당 웹 사이트 → ASP → 부모 경로 사용 항목 false인지 확인



■ 설정 파일에서 확인

1) 파일 검색 → C:\windows\System32\inetsrv\config\applicationHost.config 열기
2) 사용 중인 웹 사이트 하위 설정에 “enableParenPaths” 값이 false인지 확인

조치 방법

■ IIS 관리자에서 변경

1) IIS 관리자 → 해당 웹 사이트 → ASP → 부모 경로 사용 항목 false로 변경

■ 설정 파일에서 확인

1) 파일 검색 → C:\windows\System32\inetsrv\config\applicationHost.config 열기
2) 사용 중인 웹 사이트 하위 설정에 “enableParenPaths” 값 false로 변경

2.25.

Tomcat

2.25. Tomcat

계정 관리(2개 항목), 보안 설정(5개 항목), 패치 및 로그 관리(2개 항목) 총 3개 영역에서 9개 항목으로 구성된다.

[표 25] Tomcat 진단 체크리스트

구분	진단 항목
가. 계정 관리	default 관리자 계정명 변경
	취약한 패스워드 사용 제한
나. 보안 설정	패스워드 파일 권한 관리
	홈 디렉터리 쓰기 권한 관리
	환경 설정 파일 권한 관리
	디렉터리 리스팅 설정 제한
	에러 메시지 관리
라. 패치 및 로그 관리	로그 파일 관리 및 주기적 백업
	최신 보안 패치 적용

default 관리자 계정명

항목설명

Tomcat의 디폴트 계정을 그대로 사용할 경우 비인가 사용자가 패스워드 추측 공격을 통해 Web Server에 접속할 수 있으므로 패스워드를 유추하기 어려운 계정명으로 변경해야 한다.

진단 기준

양호

계정명이 default 계정명으로 설정되어 있지 않은 경우

취약

계정명이 default 계정명으로 설정되어 있는 경우

진단 방법

■ 계정 사용 여부 확인

1) # cat [Tomcat 설치 디렉터리]/tomcat-users.xml | grep "<user username="

```
root@ubuntu:/usr/share/tomcat9/etc# cat tomcat-users.xml | grep "<user username="
  <user username="admin" password="<must-be-changed>" roles="manager-gui"/>
  <user username="robot" password="<must-be-changed>" roles="manager-script"/>
  <user username="tomcat" password="<must-be-changed>" roles="tomcat"/>
  <user username="both" password="<must-be-changed>" roles="tomcat,role1"/>
  <user username="role1" password="<must-be-changed>" roles="role1"/>
root@ubuntu:/usr/share/tomcat9/etc#
```

■ 관리자 페이지 활성화 확인

1) # cat [Tomcat 설치 디렉터리]/tomcat-users.xml | grep "roles="

```
root@ubuntu:/usr/share/tomcat9/etc# cat tomcat-users.xml | grep "roles="
  <user username="admin" password="<must-be-changed>" roles="manager-gui"/>
  <user username="robot" password="<must-be-changed>" roles="manager-script"/>
  <user username="tomcat" password="<must-be-changed>" roles="tomcat"/>
  <user username="both" password="<must-be-changed>" roles="tomcat,role1"/>
  <user username="role1" password="<must-be-changed>" roles="role1"/>
```

※ roles = manager-gui, manager-script, manager-jmx, manager-status로 설정되어 있으면 관리자 계정 및 페이지 활성화 상태

조치 방법

■ default 계정명 변경 (admin tomcat 등)

1) # vi [Tomcat 설치 디렉터리]/tomcat-users.xml
2) default 계정명 변경 또는
3) 해당 계정 주석 처리

■ 관리자 페이지 비활성화

1) # [Tomcat 설치 디렉터리]/tomcat-users.xml 또는
2) 관리자 계정 주석 처리

※ 관리자 페이지는 default로 비활성화되어 있음(주석 처리)

비고

※ 관리자 페이지를 사용하지 않는다면 양호로 처리함

취약한 패스워드 사용 제한

항목설명

관리자 계정의 패스워드를 취약하게 설정하여 사용하는 경우에 비인가 사용자가 패스워드 유추 공격을 통하여 관리자 권한을 획득할 수 있으므로 패스워드 복잡도를 만족하여 패스워드를 설정해야 한다.

진단 기준

양호

관리자 패스워드가 암호화되어 있거나
패스워드 복잡도 설정을 만족하고 있는 경우

취약

관리자 패스워드가 암호화되어 있지 않거나
패스워드 복잡도 설정을 만족하고 있지 않은 경우

진단 방법

■ 계정 패스워드 확인

1) # [Tomcat 설치 디렉터리]/tomcat-users.xml | grep "〈user username="

2) password 필드 확인

```
root@ubuntu:/usr/share/tomcat9/etc# cat tomcat-users.xml | grep "<user username="
  <user username="admin" password="<must-be-changed>" roles="manager-gui"/>
  <user username="robot" password="<must-be-changed>" roles="manager-script"/>
  <user username="tomcat" password="<must-be-changed>" roles="tomcat"/>
  <user username="both" password="<must-be-changed>" roles="tomcat,role1"/>
  <user username="role1" password="<must-be-changed>" roles="role1"/>
root@ubuntu:/usr/share/tomcat9/etc#
```

※ default 패스워드 : "must-be-changed"

조치 방법

■ 패스워드 변경

1) 패스워드 복잡도를 만족하도록 설정
vi [Tomcat 설치 디렉터리]/tomcat-users.xml

※ 패스워드 복잡도 : 영문(대문자, 소문자), 숫자, 특수문자 조합 중 3가지 8자리 이상, 2가지 조합 10자리 이상

비고

※ 관리자 페이지를 사용하지 않는 경우 양호로 처리함

패스워드 파일 권한 관리

항목설명

패스워드 설정 파일이 비인가 사용자에게 노출되면 패스워드를 이용하여 Web Server에 접속하는 침해사고가 발생할 가능성이 있으므로 패스워드 파일의 접근권한을 제한해야 한다.

진단 기준

양호

패스워드 파일의 접근 권한이 600(-rw-------) 이하로 설정되어 있는 경우

취약

패스워드 파일의 접근 권한이 600(-rw-------) 이하로 설정되어 있지 않은 경우

진단 방법

■ 패스워드 파일 권한 설정 확인

1) # ls [Tomcat 설치 디렉터리] -l

```
root@ubuntu:/usr/share/tomcat9/etc# ls -l
합 계  204
-rw-r--r-- 1 root root   7276  1월  15  2022 catalina.properties
-rw-r--r-- 1 root root   1400  1월  15  2022 context.xml
-rw-r--r-- 1 root root   1149  1월  15  2022 jaspic-providers.xml
-rw-r--r-- 1 root root   2799  7월  20  2022 logging.properties
-rw-r--r-- 1 root root   7578  7월  21  2022 server.xml
-rw-r--r-- 1 root root   2756  1월  15  2022 tomcat-users.xml
-rw-r--r-- 1 root root 172359  1월  15  2022 web.xml
```

조치 방법

■ 패스워드 파일 권한 변경

1) # chmod 600 [Tomcat 설치 디렉터리]/tomcat-users.xml

※ 설정 파일 권한 변경 시, 시스템 영향도를 파악하여 충분한 테스트를 진행 한 후에 접근권한 수정

홈 디렉터리 쓰기 권한 관리

항목설명

일반 사용자가 웹 서버 홈 디렉터리 또는 설정 관리 서버 디렉터리 및 매니지드 구동 서버 디렉터리에 임의의 파일을 생성, 삭제를 할 수 있으면 홈페이지 변조, 중요 파일 삭제, 백도어 삽입 등 피해가 발생할 수 있으므로 홈 디렉터리의 쓰기 권한을 제한 해야 한다.

진단 기준

양호

홈 디렉터리 또는 웹 서버, 관리 서버 디렉터리 권한이 755(-rwx-r-x-r-x) 이하로 설정되어 있는 경우

취약

홈 디렉터리 또는 웹 서버, 관리 서버 디렉터리 권한이 755(-rwx-r-x-r-x) 초과로 설정되어 있는 경우

진단 방법

■ 홈 디렉터리 접근 권한 확인

1) # cat [Tomcat 환경 설정 디렉터리]/server.xml | grep appBase (예시)

```
root@ubuntu:/etc/tomcat9# cat server.xml | grep appBase
      <Host name="localhost"  appBase="webapps"
root@ubuntu:/etc/tomcat9#
```

2) # ls –al [Tomcat 설치 디렉터리]

```
root@ubuntu:/var/lib/tomcat9# ls -al
합계 20
drwxr-xr-x.  5 root   root   4096  1월 26 10:08 .
drwxr-xr-x. 90 root   root   4096  1월  5 14:34 ..
lrwxrwxrwx.  1 root   root     12  7월 21  2022 conf -> /etc/tomcat9
drwxr-xr-x.  2 tomcat tomcat 4096  7월 21  2022 lib
lrwxrwxrwx.  1 root   root     17  7월 21  2022 logs -> ../../log/tomcat9
drwxr-xr-x.  2 root   root   4096  1월 26 10:08 policy
drwxr-xr-x.  3 tomcat tomcat 4096 12월  7 10:56 webapps
lrwxrwxrwx.  1 root   root     19  7월 21  2022 work -> ../../cache/tomcat9
root@ubuntu:/var/lib/tomcat9#
```

조치 방법

■ 홈 디렉터리 접근 권한 변경 (예시)

1) # chmod 755 [Tomcat 설치 디렉터리]/webapps

※ 설정 파일 권한 변경 시, 시스템 영향도를 파악하여 충분한 테스트를 진행한 후에 접근권한 수정

환경 설정 파일 권한 관리

항목설명

일반 사용자가 웹 사이트 소스 파일을 삭제, 변경할 수 있으면, 홈페이지 변조, 작업 실수로 인한 파일 삭제, 백도어 삽입 등의 피해가 발생할 수 있다. 이로 인해 시스템이 오작동하여 사용 불능 상태에 빠질 우려가 있다.

진단 기준

양호

WAS 전용 계정 소유이고 소스파일 접근 권한 644, 설정 파일 접근 권한 600으로 설정되어 있는 경우

취약

WAS 전용 계정 소유이고 소스파일 접근 권한 644, 설정 파일 접근 권한 600으로 설정되어 있지 않은 경우

진단 방법

■ 설정 파일 및 소스 파일 접근 권한 확인

1) # ls –al [Tomcat 설치 디렉터리]

```
root@ubuntu:/usr/share/tomcat9/etc# ls -al
합 계  212
drwxr-xr-x 2 root root   4096 12월   7 11:57 .
drwxr-xr-x 5 root root   4096 12월   7 10:56 ..
-rw-r--r-- 1 root root   7276  1월  15  2022 catalina.properties
-rw-r--r-- 1 root root   1400  1월  15  2022 context.xml
-rw-r--r-- 1 root root   1149  1월  15  2022 jaspic-providers.xml
-rw-r--r-- 1 root root   2799  7월  20  2022 logging.properties
-rw-r--r-- 1 root root   7578  7월  21  2022 server.xml
-rw-r--r-- 1 root root   2756  1월  15  2022 tomcat-users.xml
-rw-r--r-- 1 root root 172359  1월  15  2022 web.xml
root@ubuntu:/usr/share/tomcat9/etc#
```

```
root@ubuntu:/var/lib/tomcat9/policy# ls -al
합 계  24
drwxr-xr-x 2 root root  4096 12월   7 10:56 .
drwxr-xr-x 5 root root  4096 12월   7 10:56 ..
-rw-r--r-- 1 root root 13286 12월   7 10:56 catalina.policy
```

※ 설정 파일 : *.xml, *.properties, *.policy 등

2) # cat [Tomcat 설치 디렉터리]/server.xml | grep appBase (예시)

```
root@ubuntu:/usr/share/tomcat9/etc# cat server.xml | grep appBase
      <Host name="localhost"  appBase="webapps"
```

```
root@ubuntu:/var/lib/tomcat9# ls -al
합 계  20
drwxr-xr-x  5 root   root   4096 12월   7 10:56 .
drwxr-xr-x 88 root   root   4096 12월   7 10:56 ..
lrwxrwxrwx  1 root   root     12  7월  21  2022 conf -> /etc/tomcat9
drwxr-xr-x  2 tomcat tomcat 4096  7월  21  2022 lib
lrwxrwxrwx  1 root   root     17  7월  21  2022 logs -> ../../log/tomcat9
drwxr-xr-x  2 root   root   4096 12월   7 10:56 policy
drwxrwxr-x  3 tomcat tomcat 4096 12월   7 10:56 webapps
lrwxrwxrwx  1 root   root     19  7월  21  2022 work -> ../../cache/tomcat9
root@ubuntu:/var/lib/tomcat9# c dwebapps
```

※ 소스 파일 : server.xml 또는 (appBase 설정 파일)

조치 방법

■ 파일 권한 변경

1) 설정 파일 권한 변경
   # chmod 600 [해당 파일]

2) 소스 파일 권한 변경
   # chmod 644 [해당 파일]

디렉터리 리스팅 설정 제한

항목설명

디렉터리 검색 기능이 설정되어 있는 경우 Web 서버 구조 및 설치 파일이 노출될 수 있으므로 디렉터리 검색 기능을 비활성화해야 한다.

진단 기준

양호
디렉터리 리스팅이 설정되어 있지 않은 경우

취약
디렉터리 리스팅이 설정되어 있는 경우

진단 방법

■ 디렉터리 리스팅 설정 확인

1) # [Tomcat 설치 디렉터리]/web.xml

※ default : false (양호)

조치 방법

■ 디렉터리 리스팅 비활성화

1) # vi [Tomcat 설치 디렉터리]/web.xml

```
        <init-param>
            <param-name>listings</param-name>
            <param-value>false</param-value>
        </init-param>
        <load-on-startup>1</load-on-startup>
    </servlet>
```

에러 메시지 관리

항목설명

공격자가 대상 시스템의 정보를 획득하기 위해 고의적으로 다양한 에러를 유발하여 돌아오는 에러 메시지를 통해 웹 프로그램의 구조 및 환경 설정을 추정할 수 있다.

진단 기준

양호

필수 에러 코드에 대해 일원화된 에러 페이지로 관리하고 있는 경우

취약

필수 에러 코드에 대해 일원화된 에러 페이지로 관리하고 있지 않은 경우

진단 방법

■ 에러 페이지 확인

1) # cat [Tomcat 설치 디렉터리]/web.xml 내 에러 페이지 설정 확인

```
<error-page>
        <error-code>404</error-code>
                <location>/error.html</location>
```

조치 방법

■ 에러 코드 설정 파일 수정

1) 필수 에러 코드(400,401,403,404,500)에 대한 에러 내용을 알 수 없도록 일원화된 에러 페이지로 관리

```
</web-app>

<error-page>
        <error-code>400</error-code>
                <location>/error.html</location>
</error-page>

<error-page>
        <error-code>401</error-code>
                <location>/error.html</location>
</error-page>

<error-page>
        <error-code>403</error-code>
                <location>/error.html</location>
</error-page>

<error-page>
        <error-code>404</error-code>
                <location>/error.html</location>
</error-page>

<error-page>
        <error-code>500</error-code>
                <location>/error.html</location>
</error-page>
```

※ 에러가 발생 시, 일원화된 에러 페이지가 표시되도록 하는 방식이 아닌 로그인 페이지로 리다이렉션되는 방식 또한 양호로 처리함

로그 파일 관리 및 주기적 백업

항목설명

침해 사고 발생 시, 로그 파일은 사고 원인을 분석하는데 사용되는 중요한 자료로써 사용되며 유지보수 및 시스템 업데이트 시에 장애 및 외부 침입 등에 대한 변조가 발생하는 경우를 대비하여 백업 정책을 세워 로그 파일을 관리하고 주기적으로 백업해야 한다.

진단 기준

양호

로그 파일을 관리하고 있으며 주기적으로 백업하고 있는 경우

취약

로그 파일을 관리하고 있으며 주기적으로 백업하고 있지 않은 경우

진단 방법

■ 시스템 담당자와 인터뷰

1) Web 서버의 로그 파일 관리 여부
2) 로그 관리 방식과 백업 방식 및 주기 확인
3) 백업 정책 수립 여부

조치 방법

■ 로그 파일 관리 및 주기적 백업

1) 백업 정책 수립
2) 정책에 따라 로그를 기록하고 주기적으로 백업

최신 보안 패치 적용

항목설명

최신 보안 패치를 적용하지 않으면 해당 버전의 취약점을 이용하여 공격자가 침해사고를 발생시킬 수 있으므로 공식 릴리즈 사이트를 참고하여 최신 보안패치를 적용해야 한다.

진단 기준

양호
최신 보안 패치를 적용하고 있는 경우

취약
최신 보안 패치를 적용하고 있지 않은 경우

진단 방법

■ 현재 버전 확인

1) # [Tomcat 설치 디렉터리]/bin/version.sh 또는
2) # rpm –qa | grep webapps

조치 방법

■ 보안 패치 적용

1) 취약점이 없는 보안 패치가 적용된 버전으로 업데이트해야 함

※ 최신 버전을 사용하도록 권고하고 있으나 시스템 운영상 적용이 어려운 경우 최신이 아닌 취약점이 존재하지 않는 버전도 허용하고 있음

비고

※ 보안 패치를 적용할 경우, 시스템 영향도를 파악하여 충분한 테스트 후 적용 권고

2.26.

Docker

2.26. Docker

Host 설정(8개 항목), 도커 데몬 설정(4개 항목), 도커 데몬 설정 파일(12개 항목), 컨테이너 이미지 및 빌드 파일(2개 항목) 컨테이너 런타임(6개 항목) 총 5개 영역에서 32개 항목으로 구성된다.

[표 26] Docker 진단 체크리스트

구분	진단 항목
가. Host 설정	도커 최신 보안 패치 적용
	도커 그룹에 불필요한 사용자 제거
	Docker daemon audit 설정
	/var/lib/docker audit 설정
	/etc/docker audit 설정
	docker.service audit 설정
	docker.socket audit 설정
	/etc/default/docker audit 설정
나. 도커 데몬 설정	default bridge를 통한 컨테이너간 네트워크 트래픽 제한
	도커 클라이언트 인증 활성화
	legacy registry (v1) 비활성화
	추가 권한 획득으로부터 컨테이너 제한
다. 도커 데몬 설정 파일	docker.service 소유권 설정
	docker.service 파일 접근 권한 설정
	docker.socket 소유권 설정
	docker.socket 파일 접근 권한 설정
	/etc/docker 디렉터리 소유권 설정
	/etc/docker 데릭터리 접근 권한 설정
	/var/run/docker.sock 파일 소유권 설정
	/var/run/docker.sock 파일 접근 권한 설정
	daemon.json 파일 소유권 설정
	daemon.json 파일 접근 권한 설정
	/etc/default/docker 파일 소유권 설정
	/etc/default/docker 파일 접근 권한 설정
라. 컨테이너 이미지 및 빌드 파일	root가 아닌 user로 컨테이너 실행
	도커를 위한 컨텐츠 신뢰성 활성화
마. 컨테이너 런타임	컨테이너 SELinux 보안 옵션 설정
	컨테이너에서 ssh 사용 금지
	컨테이너에 privileged 포트 매핑 금지
	PIDs cgroup 제한
	도커의 default bridge docker() 사용 제한
	Host의 user namespaces 공유 제한

도커 최신 보안 패치 적용

항목설명

Docker 최신 보안 패치를 적용함으로써 Docker 소프트웨어 취약점을 완화할 수 있다. 공격자가 권한을 획득하거나 권한 상승을 시도할 때 보안 취약점을 이용할 수 있으며 그에 따라 권한 상승, 비인가 접근, 기타 보안 침해로 이어질 수 있다.

진단 기준

양호
최신 보안 패치를 적용하고 있는 경우

취약
최신 보안 패치를 적용하고 있지 않은 경우

진단 방법

■ 현재 버전 확인

1) # docker version

```
root@k8s-master:~# docker version
Client: Docker Engine - Community
 Version:           24.0.6
 API version:       1.43
 Go version:        go1.20.7
 Git commit:        ed223bc
 Built:             Mon Sep  4 12:31:44 2023
 OS/Arch:           linux/amd64
 Context:           default

Server: Docker Engine - Community
 Engine:
  Version:          24.0.6
  API version:      1.43 (minimum version 1.12)
  Go version:       go1.20.7
  Git commit:       1a79695
  Built:            Mon Sep  4 12:31:44 2023
  OS/Arch:          linux/amd64
  Experimental:     false
 containerd:
  Version:          1.6.24
  GitCommit:        61f9fd88f79f081d64d6fa3bb1a0dc71ec870523
 runc:
  Version:          1.1.9
  GitCommit:        v1.1.9-0-gccaecfc
 docker-init:
  Version:          0.19.0
  GitCommit:        de40ad0
root@k8s-master:~#
```

2) Ubuntu, Debian 패키지 버전 확인
   # dpkg –l | grep docker.io

3) CentOS 패키지 버전 확인
   # rpm –qa | grep docker.io

조치 방법

■ 보안 패치 적용

1) 보안 취약점이 존재하지 않는 버전으로 보안패치를 적용해야 함

※ 최신 버전을 사용하도록 권고하고 있으나 시스템 운영상 적용이 어려운 경우 최신이 아닌 취약점이 존재하지 않는 버전도 허용하고 있음

비고

※ 보안 패치를 적용할 경우, 시스템 영향도를 파악하여 충분한 테스트 후 적용 권고

도커 그룹에 불필요한 사용자 제거

항목설명

Docker 데몬은 root 권한이 필요하며 Docker 그룹에 추가된 사용자는 root 권한을 부여받게 된다. 따라서 컨테이너를 실행하고 호스트의 root 디렉터리를 컨테이너에 매핑 할 수 있어 컨테이너는 제한 없이 호스트 파일 시스템을 변경할 수 있는 위험이 존재한다. 따라서 도커 그룹에 불필요한 사용자를 제거하여 root 권한 부여를 제한해야 한다.

진단 기준

양호

도커 그룹에 불필요한 사용자가 존재하지 않는 경우

취약

도커 그룹에 불필요한 사용자가 존재하는 경우

진단 방법

■ 도커 그룹에 속한 사용자 계정 조회

1) # cat /etc/group | grep docker

```
root@k8s-master:~# cat /etc/group | grep docker
docker:x:999:test
```

■ 도커 그룹 이름이 dockerroot인 경우

1) 아래의 두 명령어 모두 입력하여 확인
   # cat /etc/group | grep docker
   # cat /etc/group | grep root

조치 방법

■ 도커 그룹에서 불필요한 사용자 제거

1) # vi /etc/group 입력 후, 불필요한 사용자 계정 제거

■ 도커 그룹 이름이 dockerroot인 경우

1) root 그룹, dockerroot 그룹 모두 불필요한 사용자 계정 제거
   # vi /etc/group

Docker daemon audit 설정

항목설명

Docker 데몬은 root 권한으로 실행되기 때문에 그 활동과 용도를 감사해야 한다.

진단 기준

양호

/usr/bin/docker 파일에 감사 설정이 적용되어 있는 경우

취약

/usr/bin/docker 파일에 감사 설정이 적용되어 있지 않은 경우

진단 방법

■ 명령어를 통해 감사 설정 확인

1) # auditctl –l | grep /usr/bin/docker

```
root@k8s-master:/etc/audit/rules.d# auditctl -l | grep /usr/bin/docker
-w /usr/bin/docker -p rwxa
root@k8s-master:/etc/audit/rules.d#
```

■ 명령어를 통해 파일 내용 확인

1) # cat [audit.rules 파일 위치] | grep /usr/bin/docker

```
root@k8s-master:/etc/audit/rules.d# cat audit.rules | grep /usr/bin/docker
-w /usr/bin/docker
root@k8s-master:/etc/audit/rules.d#
```

조치 방법

■ audit 설정 적용

1) auditd 설치

2) /etc/audit/rules.d/audit.rules 파일에 아래의 내용 추가

```
## First rule - delete all
-D

## Increase the buffers to survive stress events.
## Make this bigger for busy systems
-b 8192

## This determine how long to wait in burst of events
--backlog_wait_time 60000

## Set failure mode to syslog
-f 1

-w /usr/bin/docker
```

3) audit 데몬 재시작
service auditd restart

/var/lib/docker audit 설정

항목설명

/var/lib/docker 디렉터리는 컨테이너에 대한 모든 정보를 보유하고 있는 디렉터리이므로 감사 설정을 적용하여 그 기록을 남겨야 한다.

진단 기준

양호

/var/lib/docker 디렉터리에 감사 설정이 적용되어 경우

취약

/var/lib/docker 디렉터리에 감사 설정이 적용되어 있지 않은 경우

진단 방법

■ 명령어를 통해 감사 설정 확인

1) # auditctl –l | grep /var/lib/docker

```
root@k8s-master:/etc/audit/rules.d# auditctl -l | grep /var/lib/docker
-w /var/lib/docker -p rwxa -k docker
```

■ 명령어를 통해 파일 내용 확인

1) # cat [audit.rules 파일 위치] | grep /var/lib/docker

```
root@k8s-master:/etc/audit/rules.d# cat audit.rules | grep /var/lib/docker
-w /var/lib/docker -k docker
```

조치 방법

■ audit 설정 적용

1) auditd 설치

2) /etc/audit/rules.d/audit.rules 파일에 아래의 내용 추가

```
## First rule - delete all
-D

## Increase the buffers to survive stress events.
## Make this bigger for busy systems
-b 8192

## This determine how long to wait in burst of events
--backlog_wait_time 60000

## Set failure mode to syslog
-f 1

-w /usr/bin/docker
-w /var/lib/docker -k docker
-w /etc/docker -k docker
-w /lib/systemd/system/docker.service -k docker
-w /lib/systemd/system/docker.socket -k docker
-w /etc/default/docker -k docker
```

3) audit 데몬 재시작
service auditd restart

/etc/docker audit 설정

항목설명

/etc/docker 디렉터리는 Docker 데몬과 Docker 클라이언트 간의 TLS 통신에 사용되는 다양한 인증서와 키를 보유하고 있으므로 감사 설정을 적용하여 그 기록을 남겨야 한다.

진단 기준

양호

/etc/docker 디렉터리에 감사 설정이 적용되어 있는 경우

취약

/etc/docker 디렉터리에 감사 설정이 적용되어 있지 않은 경우

진단 방법

■ 명령어를 통해 감사 설정 확인

1) # auditctl –l | grep /etc/docker

```
root@k8s-master:/etc/audit/rules.d# auditctl -l | grep /etc/docker
-w /etc/docker -p rwxa -k docker
```

■ 명령어를 통해 파일 내용 확인

1) # cat [audit.rules 파일 위치] | grep /etc/docker

```
root@k8s-master:/etc/audit/rules.d# cat audit.rules | grep /etc/docker
-w /etc/docker -k docker
```

조치 방법

■ audit 설정 적용

1) auditd 설치

2) /etc/audit/rules.d/audit.rules 파일에 아래의 내용 추가

```
## First rule - delete all
-D

## Increase the buffers to survive stress events.
## Make this bigger for busy systems
-b 8192

## This determine how long to wait in burst of events
--backlog_wait_time 60000

## Set failure mode to syslog
-f 1

-w /usr/bin/docker
-w /var/lib/docker -k docker
-w /etc/docker -k docker
-w /lib/systemd/system/docker.service -k docker
-w /lib/systemd/system/docker.socket -k docker
-w /etc/default/docker -k docker
```

3) audit 데몬 재시작
   # service auditd restart

docker.service audit 설정

항목설명

데몬 매개 변수가 관리자에 의해 변경된 경우 docker.service 파일이 존재한다. docker.service 파일은 Docker 데몬을 위한 다양한 파라미터를 보유하고 있으므로 감사 설정을 적용해야 한다.

진단 기준

양호

docker.service 파일에 감사 설정이 적용되어 있는 경우

취약

docker.service 파일에 감사 설정이 적용되어 있지 않은 경우

진단 방법

■ 명령어를 통해 감사 설정 확인

1) # auditctl –l | grep /lib/systemd/system/docker.service

```
root@k8s-master:/etc/audit/rules.d# auditctl -l | grep /lib/systemd/system/docker.service
-w /lib/systemd/system/docker.service -p rwxa -k docker
```

■ 명령어를 통해 파일 내용 확인

1) # cat [audit.rules 파일 위치] | /lib/systemd/system/docker.service

```
root@k8s-master:/etc/audit/rules.d# cat audit.rules | grep /lib/systemd/system/docker.service
-w /lib/systemd/system/docker.service -k docker
```

조치 방법

■ audit 설정 적용

1) auditd 설치

2) /etc/audit/rules.d/audit.rules 파일에 아래의 내용 추가

```
## First rule - delete all
-D

## Increase the buffers to survive stress events.
## Make this bigger for busy systems
-b 8192

## This determine how long to wait in burst of events
--backlog_wait_time 60000

## Set failure mode to syslog
-f 1

-w /usr/bin/docker
-w /var/lib/docker -k docker
-w /etc/docker -k docker
-w /lib/systemd/system/docker.service -k docker
-w /lib/systemd/system/docker.socket -k docker
-w /etc/default/docker -k docker
```

3) audit 데몬 재시작
service auditd restart

docker.socket audit 설정

항목설명

docker.socket 파일은 Docker 데몬 소켓을 위한 다양한 파라미터를 보유하고 있으므로 감사 설정을 적용하여 그 기록을 남겨야 한다.

진단 기준

양호

docker.socket 파일에 감사 설정이 적용되어 경우

취약

docker.socket 파일에 감사 설정이 적용되어 있지 않은 경우

진단 방법

■ 명령어를 통해 감사 설정 확인

1) # auditctl –l | grep /lib/systemd/system/docker.socket

```
root@k8s-master:/etc/audit/rules.d# auditctl -l | grep /lib/systemd/system/docker.service
-w /lib/systemd/system/docker.service -p rwxa -k docker
```

■ 명령어를 통해 파일 내용 확인

1) # cat [audit.rules 파일 위치] | /lib/systemd/system/docker.socket

```
root@k8s-master:/etc/audit/rules.d# cat audit.rules | grep /lib/systemd/system/docker.service
-w /lib/systemd/system/docker.service -k docker
```

조치 방법

■ audit 설정 적용

1) auditd 설치

2) /etc/audit/rules.d/audit.rules 파일에 아래의 내용 추가

```
## First rule - delete all
-D

## Increase the buffers to survive stress events.
## Make this bigger for busy systems
-b 8192

## This determine how long to wait in burst of events
--backlog_wait_time 60000

## Set failure mode to syslog
-f 1

-w /usr/bin/docker
-w /var/lib/docker -k docker
-w /etc/docker -k docker
-w /lib/systemd/system/docker.service -k docker
-w /lib/systemd/system/docker.socket -k docker
-w /etc/default/docker -k docker
```

3) audit 데몬 재시작
   # service auditd restart

/etc/default/docker audit 설정

항목설명

/etc/default/docker 파일은 Docker 데몬을 위한 다양한 파라미터를 보유하고 있으므로 감사 설정을 적용하여 그 기록을 남겨야 한다.

진단 기준

양호

/etc/default/docker 파일에 감사 설정이 적용되어 있는 경우

취약

/etc/default/docker 파일에 감사 설정이 적용되어 있지 않은 경우

진단 방법

■ 명령어를 통해 감사 설정 확인

1) # auditctl –l | grep /etc/default/docker

```
root@k8s-master:/etc/audit/rules.d# auditctl -l | grep /etc/default/docker
-w /etc/default/docker -p rwxa -k docker
```

■ 명령어를 통해 파일 내용 확인

1) # cat [audit.rules 파일 위치] | /etc/default/docker

```
root@k8s-master:/etc/audit/rules.d# cat audit.rules | grep /etc/default/docker
-w /etc/default/docker -k docker
```

조치 방법

■ audit 설정 적용

1) auditd 설치

2) /etc/audit/rules.d/audit.rules 파일에 아래의 내용 추가 (Debian 계열)

```
## First rule - delete all
-D

## Increase the buffers to survive stress events.
## Make this bigger for busy systems
-b 8192

## This determine how long to wait in burst of events
--backlog_wait_time 60000

## Set failure mode to syslog
-f 1

-w /usr/bin/docker
-w /var/lib/docker -k docker
-w /etc/docker -k docker
-w /lib/systemd/system/docker.service -k docker
-w /lib/systemd/system/docker.socket -k docker
-w /etc/default/docker -k docker
```

2) /etc/audit/rules.d/audit.rules 파일에 아래의 내용 추가 (RedHat 계열)
–w /etc/default/docker –k docker

3) audit 데몬 재시작
service auditd restart

default bridege를 통한 컨테이너간 네트워크 트래픽 제한

항목설명

docker의 기본 네트워크 인터페이스인 docker0이 활성화되어 있다면 동일한 호스트 네트워크를 통해 다른 컨테이너와 통신이 가능하며 네트워크 패킷을 모두 확인할 수 있다. 따라서 각 컨테이너간의 통신이 불가하도록 default bridge(docker0) 사용을 제한해야 한다.

진단 기준

양호

컨테이너 간 네트워크 통신이 가능하지 않은 경우

취약

컨테이너 간 네트워크 통신이 가능한 경우

진단 방법

■ 프로세스 확인을 통해 제한 옵션 적용 확인

1) # ps –ef | grep docker

```
root@k8s-master:~# ps -ef | grep docker
root        8115    6791  5 15:38 pts/2    00:00:00 dockerd
root        8271    7765  0 15:38 pts/3    00:00:00 grep --color=auto docker
root@k8s-master:~#
```

※ docker 데몬 프로세스에 --icc=false 인자값이 존재하지 않음 (취약)

■ 명령어를 통해 제한 옵션 적용 확인

1) # docker network ls --quiet | xargs docker network inspect --format '{{ .Name}}: {{ .Options }}'

```
root@k8s-master:/etc/audit/rules.d# docker network ls --quiet | xargs docker network inspect --format '
bridge: map[com.docker.network.bridge.default_bridge:true com.docker.network.bridge.enable_icc:true com.
m.docker.network.bridge.host_binding_ipv4:0.0.0.0 com.docker.network.bridge.name:docker0 com.docker.netw
host: map[]
none: map[]
```

※ com.docker.network.bridge.enable_icc : true (취약)

조치 방법

■ 아래와 같은 옵션으로 데몬 재시작

1) # dockerd --icc=true

■ /etc/default/docker 파일에 아래와 같은 옵션 추가 후 데몬 재시작

1) dockerd, docker.socket, docker.service 중지

2) /etc/default/docker에 DOCKER_OPTS="--icc=false" 문구 추가

3) /lib/systemd/system/docker.service에 아래의 내용 추가

```
# for containers run by docker
EnvironmentFile=/etc/default/docker
ExecStart=/usr/bin/dockerd -H fd:// $DOCKER_OPTS
```

4) docker.socket, docker.service, dockerd 재시작

5) # ps –ef | grep docker 명령어 입력하여 ––icc=false 옵션 적용 확인

```
root@k8s-master:~# ps -ef | grep docker
root        8664    6791  7 15:39 pts/2    00:00:00 dockerd --icc=false
root        8824    7765  0 15:39 pts/3    00:00:00 grep --color=auto docker
root@k8s-master:~#
```

비고

※ /etc/docker/daemon.json을 사용하는 경우 ps 명령어를 통해 옵션 확인을 할 수 없으며 docker 명령어를 통해 옵션 적용 여부를 확인할 수 있음

도커 클라이언트 인증 활성화

항목설명

Docker는 기본적으로 인증 절차를 거치지 않기 때문에 비인가 사용자가 Dockerd에 접근하여 명령을 실행할 수 있다. 따라서 인증 플러그인을 설치하여 Docker 클라이언트 명령을 실행할 때 인증 절차를 거지도록 해야 한다.

진단 기준

양호

Docker 인증 플러그인이 적용되어 경우

취약

Docker 인증 플러그인이 적용되어 있지 않은 경우

진단 방법

■ 명령어를 통해 인증 플러그인 옵션 적용 확인

1) /etc/default/docker를 사용하는 경우
   # ps –ef | grep docker

```
root@k8s-master:~# ps -ef | grep docker
root       10627       1  0 16:53 ?        00:00:00 /usr/bin/dockerd -H fd:// --icc=false
root       14235    8703  0 17:07 pts/2    00:00:00 grep --color=auto docker
```

2) /etc/docker/daemon.json을 사용하는 경우
   # docker plugin ls

```
root@k8s-master:~# docker plugin ls
ID          NAME      DESCRIPTION   ENABLED
```

■ 명령어를 통해 제한 옵션 적용 확인

1) # docker search hello-world

조치 방법

■ 인증 플러그인 설치

■ 다음과 같은 절차로 인증 설정

1) 인증 플러그인 설치

2) 인증 정책 설정

3) 아래와 같은 옵션으로 데몬 시작
   (방법1) docker daemon --authorization-plugin=〈PLUGIN_ID〉
   (방법2) /etc/default/docker 파일에 아래와 같은 옵션 추가 후 데몬 재시작
   DOCKER_OPTS=“ --authorization-plugin-〈PLUGIN_ID〉”
   (방법3) /etc/docker/daemon.json 파일에 아래와 같은 옵션 추가 후 데몬 재시작
   { “authorization-plugins”: [“PLUGIN_ID”]}

비고

※ /etc/docker/daemon.json 파일을 사용하는 경우, ps 명령어를 통해 옵션 확인을 할 수 없으므로 docker 명령어를 통해 확인 할 수 있음

sudo docker plugin ls

legacty registry (v1) 비활성화

항목설명

Docker 레지스트리 v2는 이미지 출처 및 이미지 서명 및 확인과 같은 보안 기능을 지원하는 등 legacy registry v1보다 더 많은 성능 및 보안 향상 기능을 제공한다. 따라서 Docker legacy registry는 사용이 제한되어야 한다.

진단 기준

양호

legacy registry v1이 비활성화되어 있는 경우

취약

legacy registry v1이 활성화되어 있는 경우

진단 방법

■ 명령어를 입력하여 —disable-legacy-registry 옵션 적용 확인

1) # ps –ef | grep docker

※ docker v17.12(CE) 이상을 사용하는 경우 legacy registry v1을 사용할 수 없으므로 양호로 처리함

조치 방법

■ 아래와 같은 옵션으로 데몬 시작

1) # docker daemon —disable-legacy-registry

2) /etc/default/docker 파일에 아래의 옵션 추가 후 데몬 재시작
Docker_OPTS="--disable-legacy-registry"

비고

※ Docker v17.06(CE, EE) 에서는 디폴트로 legacy registry v1이 비활성화되어 있으나 --disable-legacy-registry=false 옵션을 통해 v1 통신이 가능함

※ Docker v17.12(CE) 이상부터는 --disable-legacy-registry 옵션을 사용할 수 없으므로 legacy registry v1을 사용할 수 없음

추가 권한 획득으로부터 컨테이너 제한

항목설명

컨테이너가 suid를 통해 추가 권한을 얻는 것을 제한해야 한다.

진단 기준

양호

컨테이너 추가 권한 획득 제한 설정이 적용되어 있는 경우

취약

컨테이너 추가 권한 획득 제한 설정이 적용되어 있지 않은 경우

진단 방법

■ 추가 권한 획득 제한 설정 적용 확인

1) 컨테이너 목록 확인
   # docker ps —quiet —all

2) # docker inspect 〈CONTAINER ID〉 | grep SecurityOpt

■ 추가 권한 획득 제한 설정 적용 확인

1) # docker ps --quiet --all | xargs docker inspect --format '{{ .Id }}: SecurityOpt={{ .HostConfig.SecurityOpt }}‘

조치 방법

■ 컨테이너 옵션 실행

1) # docker run --security-opt=no-new-privileges

docker.service 소유권 설정

항목설명

docker.service 파일에는 Docker 데몬의 동작을 변경할 수 있는 중요한 매개 변수가 포함되어 있다. 따라서 무결성을 유지하기 위해서는 docker.service 파일의 소유자 및 소유그룹이 root:root로 설정되어 있어야 한다.

진단 기준

양호

docker.service 파일의 소유자 및 소유그룹이 root:root인 경우

취약

docker.service 파일의 소유자 및 소유그룹이 root:root가 아닌 경우

진단 방법

■ docker.service 파일의 소유자 및 소유 그룹 확인

1) # ls -l /lib/systemd/system/docker.service

```
root@k8s-master:~# ls -l /lib/systemd/system/docker.service
-rw-r--r-- 1 root root 1730  9월   4 21:30 /lib/systemd/system/docker.service
```

2) # stat -c %U:%G /lib/systemd/system/docker.service

```
root@k8s-master:~# stat -c %U:%G /lib/systemd/system/docker.service
root:root
```

※ docker.service 파일이 존재하지 않는 경우 해당사항 없음(N/A)으로 처리 함

조치 방법

■ docker.service 파일의 소유자 및 소유 그룹을 root:root로 변경

1) # chown root:root /lib/systemd/system/docker.service

docker.service 파일 접근 권한 설정

항목설명

docker.service 파일에는 Docker 데몬의 동작을 변경할 수 있는 중요한 매개 변수가 포함되어 있다. 따라서 무결성을 유지하기 위해서는 root 이외의 사용자는 권한을 제거해야 한다.

진단 기준

양호

docker.service 파일의 접근 권한이 644(-rw-r--r--) 이하인 경우

취약

docker.service 파일의 접근 권한이 644(-rw-r--r--) 초과인 경우

진단 방법

■ docker.service 파일 경로 확인

1) # systemctl show -p FragmentPath docker.service

```
test@k8s-master:~$  systemctl show -p FragmentPath docker.service
FragmentPath=/lib/systemd/system/docker.service
```

■ docker.service 파일의 접근 권한 확인

1) # ls -l /lib/systemd/system/docker.service

```
root@k8s-master:~# ls -l /lib/systemd/system/docker.service
-rw-r--r-- 1 root root 1730  9월   4 21:30 /lib/systemd/system/docker.service
```

※ docker.service 파일이 존재하지 않는 경우 해당사항 없음(N/A)으로 처리 함

조치 방법

■ docker.service 파일 접근 권한 수정

1) # chmod 644 /lib/systemd/system/docker.service

docker.socket 소유권 설정

항목설명

docker.socket 파일에는 Docker API의 동작을 변경할 수 있는 중요한 매개 변수가 포함되어 있다. 따라서 무결성을 유지하기 위해서는 docket.socket 파일의 소유자 및 소유그룹이 root:root로 설정되어야 한다.

진단 기준

양호

docker.socket 파일의 소유자 및 소유그룹이 root:root인 경우

취약

docker.socket 파일의 소유자 및 소유그룹이 root:root가 아닌 경우

진단 방법

■ docker.socket 파일 경로 확인

1) # systemctl show -p FragmentPath docker.socket

```
root@k8s-master:~# systemctl show -p FragmentPath docker.socket
FragmentPath=/lib/systemd/system/docker.socket
```

■ docker.socket 파일의 소유자 및 소유 그룹 확인

1) # ls -l /lib/systemd/system/docker.socket

```
root@k8s-master:~# ls -l /lib/systemd/system/docker.socket
-rw-r--r-- 1 root root 295  9월   4 21:30 /lib/systemd/system/docker.socket
```

2) # stat -c %U:%G /lib/systemd/system/docker.socket

```
root@k8s-master:~# stat -c %U:%G /lib/systemd/system/docker.socket
root:root
```

조치 방법

■ docker.socket 파일 소유자 및 소유 그룹 수정

1) # chown root:root /lib/systemd/system/docker.socket

docker.socket 파일 접근 권한 설정

항목설명

docker.socket 파일에는 Docker API의 동작을 변경할 수 있는 중요한 매개 변수가 포함되어 있다. 따라서 무결성을 유지하기 위해서는 root 이외의 사용자는 쓰기 권한을 제거해야 한다.

진단 기준

양호

docker.socket파일의 접근 권한이 644(-rw-r--r--) 이하인 경우

취약

docker.socket파일의 접근 권한이 644(-rw-r--r--) 초과인 경우

진단 방법

■ docker.socket 파일 경로 확인

1) # systemctl show -p FragmentPath docker.socket

```
root@k8s-master:~# systemctl show -p FragmentPath docker.socket
FragmentPath=/lib/systemd/system/docker.socket
```

■ docker.socket 파일의 접근 권한 확인

1) # ls -l /lib/systemd/system/docker.socket

```
root@k8s-master:~# ls -l /lib/systemd/system/docker.socket
-rw-r--r-- 1 root root 295  9월   4 21:30 /lib/systemd/system/docker.socket
```

조치 방법

■ docker.socket 파일 접근 권한 수정

1) # chmod 644 /lib/systemd/system/docker.socket

/etc/docker 디렉터리 소유권 설정

항목설명

/etc/docker 디렉터리에는 민감한 파일들 외에도 인증서가 들어 있으므로 디렉터리의 무결성을 유지하기 위해서는 소유자 및 소유그룹이 root:root로 설정되어야 한다.

진단 기준

양호

/etc/docker 디렉터리의 소유자 및 소유그룹이 root:root인 경우

취약

/etc/docker 디렉터리의 소유자 및 소유그룹이 root:root가 아닌 경우

진단 방법

■ /etc/docker 디렉터리 소유자 및 소유 그룹 확인

1) # ls –ld /etc/docker

```
root@k8s-master:~# ls -ld /etc/docker
drwxr-xr-x 2 root root 4096  9월   2 02:35 /etc/docker
```

2) # stat –c %U:%G /etc/docker

```
root@k8s-master:~# stat -c %U:%G /etc/docker
root:root
```

조치 방법

■ /etc/docker 디렉터리 소유자 및 소유 그룹 수정

1) # chown root:root /etc/docker

/etc/docker 디렉터리 접근 권한 설정

항목설명

/etc/docker 디렉터리에는 민감한 파일들 외에도 인증서 및 민감 데이터가 들어 있으므로 디렉터리의 무결성을 유지하기 위해서는 root 이외의 사용자는 쓰기 권한이 제거되어야 한다.

진단 기준

양호

/etc/docker 디렉터리 접근 권한이 755(drwxr-x-r-x) 이하인 경우

취약

/etc/docker 디렉터리 접근 권한이 755(drwxr-x-r-x) 초과인 경우

진단 방법

■ /etc/docker 디렉터리 접근 권한 확인

1) # ls –ld /etc/docker

```
root@k8s-master:~# ls -ld /etc/docker
drwxr-xr-x 2 root root 4096  9월   2 02:35 /etc/docker
```

2) # stat –c %a /etc/docker

```
root@k8s-master:~#
root@k8s-master:~# stat -c %a /etc/docker
755
```

조치 방법

■ /etc/docker 디렉터리 접근 권한 수정

1) # chmod 755 /etc/docker

/var/run/docker.sock 파일 소유권 설정

항목설명

Docker 데몬은 root로 구동된다. 그러므로 해당 소켓은 root가 소유하고 있어야 한다. 다른 사용자나 프로세스가 이 소켓을 소유하고 있는 경우, 권한 없는 사용자나 프로세스가 Docker 데몬과 상호작용할 수 있다.

진단 기준

양호

/var/run/docker.sock 파일의 소유자 및 소유그룹이 root:docker(root)인 경우

취약

/var/run/docker.sock 파일의 소유자 및 소유그룹이 root:docker(root)가 아닌 경우

진단 방법

■ /var/run/docker.sock 파일 소유자 및 소유 그룹 확인

1) # ls –l /var/run/docker.sock

```
root@k8s-master:~# ls -l /var/run/docker.sock
srw-rw---- 1 root docker 0 10월  11 16:39 /var/run/docker.sock
```

2) # stat –c %U:%G /var/run/docker.sock

```
root@k8s-master:~# stat -c %U:%G /var/run/docker.sock
root:docker
```

조치 방법

■ /var/dun/docker.sock 파일 소유자 및 소유 그룹 수정

1) # chown root:docker /var/run/docker.sock (Debian 계열)
2) # chown root:docker /run/docker.sock (RedHat 계열)

/var/run/docker.sock 파일 접근 권한 설정

항목설명

Docker 데몬은 root로 구동된다. 그러므로 root 및 Docker 그룹의 구성원만이 Docker Unix 소켓을 읽고 쓸 수 있어야 한다.

진단 기준

양호

/var/run/docker.sock 파일의 접근 권한이 660(-rw-rw----) 이하인 경우

취약

/var/run/docker.sock 파일의 접근 권한이 660(-rw-rw----) 초과인 경우

진단 방법

■ /var/run/docker.sock 파일 접근 권한 확인

1) # ls -l /var/run/docker.sock

```
root@k8s-master:~# ls -l /var/run/docker.sock
srw-rw---- 1 root docker 0 10월  11 16:39 /var/run/docker.sock
```

2) # stat -c %a /var/run/docker.sock

```
root@k8s-master:~# stat -c %a /var/run/docker.sock
660
```

조치 방법

■ /var/dun/docker.sock 파일 접근 권한 수정

1) # chmod 660 /var/run/docker.sock

daemon.json 파일 소유권 설정

항목설명

daemon.json 파일에는 Docker 데몬의 동작과 관련된 중요한 매개 변수가 포함되어 있다. 따라서 파일의 무결성을 유지하기 위해서 소유자 및 소유그룹은 root로 설정되어야 한다.

진단 기준

양호

/etc/docker/daemon.json 파일의 소유자 및 소유그룹이 root인 경우

취약

/etc/docker/daemon.json 파일의 소유자 및 소유그룹이 root가 아닌 경우

진단 방법

■ /etc/docker/daemon.json 파일 소유자 및 소유 그룹 확인

1) # ls –l /etc/docker/daemon.json

```
root@k8s-master:~# ls -l /etc/docker/daemon.json
-rw-r--r-- 1 root root 156  9월   2 02:35 /etc/docker/daemon.json
```

2) # stat –c %U:%G /etc/docker/daemon.json

```
root@k8s-master:~# stat -c %U:%G /etc/docker/daemon.json
root:root
```

조치 방법

■ daemon.json 파일 소유자 및 소유 그룹 수정

1) # chown root:root /etc/docker/daemon.json

daemon.json 파일 접근 권한 설정

항목설명

daemon.json 파일에는 Docker 데몬의 동작과 관련된 중요한 매개 변수가 포함되어 있다. 따라서 파일의 무결성을 유지하기 위해서 root 이외의 사용자는 쓰기 권한이 제거되어야 한다.

진단 기준

양호

/etc/docker/daemon.json 파일의 접근 권한이 644(-rw-r--r--) 이하인 경우

취약

/etc/docker/daemon.json 파일의 접근 권한이 644(-rw-r--r--) 초과인 경우

진단 방법

■ /etc/docker/daemon.json 파일 접근 권한 확인

1) # ls –l /etc/docker/daemon.json

```
root@k8s-master:~# ls -l /etc/docker/daemon.json
-rw-r--r-- 1 root root 156  9월   2 02:35 /etc/docker/daemon.json
```

2) # stat –c %a /etc/docker/daemon.json

```
root@k8s-master:~# stat -c %a /etc/docker/daemon.json
644
```

조치 방법

■ daemon.json 파일 접근 권한 수정

1) # chmod 644 /etc/docker/daemon.json

/etc/default/docker 파일 소유권 설정

항목설명

/etc/default/docker 파일에는 Docker 데몬의 동작과 관련된 중요한 매개 변수가 포함되어 있다. 따라서 파일의 무결성을 유지하기 위해서 소유자 및 소유그룹은 root로 설정되어야 한다.

진단 기준

양호

/etc/default/docker 파일의 소유자 및 소유그룹이 root:root인 경우

취약

/etc/default/docker 파일의 소유자 및 소유그룹이 root:root가 아닌 경우

진단 방법

■ /etc/default/docker 파일 소유자 및 소유 그룹 확인

1) # ls –l /etc/default/docker

```
root@k8s-master:~# ls -l /etc/default/docker
-rw-r--r-- 1 root root 642  7월  22 05:33 /etc/default/docker
```

2) # stat –c %U:%G /etc/default/docker

```
root@k8s-master:~# stat -c %U:%G /etc/default/docker
root:root
```

조치 방법

■ /etc/default/docker 파일 소유자 및 소유 그룹 수정

1) # chown root:root /etc/default/docker (Debian 계열)
2) # chown root:root /etc/sysconfig/docker (RedHat 계열)

비고

※ /etc/default/docker 파일이 존재하지 않으면 해당사항 없음(N/A)로 처리 함

/etc/default/docker 파일 접근 권한 설정

항목설명

/etc/default/docker 파일에는 Docker 데몬의 동작과 관련된 중요한 매개 변수가 포함되어 있다. 따라서 파일의 무결성을 유지하기 위해서 root 이외의 사용자는 쓰기 권한이 제거되어야 한다.

진단 기준

양호

/etc/default/docker 파일의 접근 권한이 644(-rw-r--r--) 이하인 경우

취약

/etc/default/docker 파일의 접근 권한이 644(-rw-r--r--) 초과인 경우

진단 방법

■ /etc/default/docker 파일 접근 권한 확인

1) # ls –l /etc/default/docker

```
root@k8s-master:~# ls -l /etc/default/docker
-rw-r--r-- 1 root root 642  7월  22 05:33 /etc/default/docker
```

2) # stat –c %a /etc/default/docker

```
root@k8s-master:~# stat -c %a /etc/default/docker
644
```

조치 방법

■ /etc/default/docker 파일 접근 권한 수정

1) # chmod 644 /etc/default/docker (Debian 계열)
2) # chmod 644 /etc/sysconfig/docker (RedHat 계열)

비고

※ /etc/default/docker 파일이 존재하지 않으면 해당사항 없음(N/A)로 처리 함

root가 아닌 user로 컨테이너 실행

항목설명

기본적으로 컨테이너의 user namespace는 호스트의 namespace와 동일하다. 즉, 컨테이너 내부의 root 사용자는 호스트 시스템의 root 사용자이므로 root로 실행되는 컨테이너 프로세스의 손상으로 Docker 호스트 또한 손상될 수 있다. 일반적으로 컨테이너에는 root 권한이 필요하지 않으므로 컨테이너에 있는 애플리케이션은 root 권한으로 실행하지 않아야 한다.

진단 기준

양호

컨테이너가 root 계정으로 실행되고 있지 않은 경우

취약

컨테이너가 root 계정으로 실행되고 있는 경우

진단 방법

■ 컨테이너를 실행시킨 계정 확인

1) # docker ps --quiet --all | xargs docker inspect --format '{{ .Id }}: User={{.Config.User }}'

조치 방법

■ Dockerfile에 아래의 내용 추가

1) RUN useradd -d /home/username -m s /bin/bash username
USER username

도커를 위한 컨텐츠 신뢰성 활성화

항목설명

Content Trust 설정은 원격 Docker 레지스트리와 주고받는 데이터에 디지털 서명을 허용할 수 있는 기능을 제공한다. 이미지 서명은 데이터 전송 도중에 발생할 수 있는 컨테이너 조작을 방지할 수 있으므로 콘텐츠 신뢰성 설정을 적용해야 한다.

진단 기준

양호

Docker 컨텐츠 신뢰성 설정이 활성화되어 있는 경우

취약

Docker 컨텐츠 신뢰성 설정이 활성화되어 있지 않은 경우

진단 방법

■ 아래 명령어를 입력하여 '1'을 반환하는지 확인

1) # echo $DOCKER_CONTENT_TRUST

```
root@k8s-master:~# echo $DOCKER_CONTENT_TRUST

root@k8s-master:~#
```

※ default : disabled (아무런 출력 없음)

조치 방법

■ 사용하는 shell에 아래의 내용을 추가

1) # export DOCKER_CONTENT_TRUST=1

```
root@k8s-master:~# export DOCKER_CONTENT_TRUST=1
root@k8s-master:~# echo $DOCKER_CONTENT_TRUST
1
root@k8s-master:~#
```

비고

※ bash shell 전체 적용을 위해서는 /etc/bash.bashrc(Ubuntu 계열) 또는 /etc/bashrc(CentOS 계열)에 작성 후 적용

컨테이너 SELinux 보안 옵션 설정

항목설명

SELinux는 효과적인 Linux 애플리케이션 보안 시스템으로 MAC(Mandatory Access Control) 시스템을 제공한다. 네트워크의 보안 수준 향상을 위해서 SELinux를 사용해야 한다.

진단 기준

양호

SELinux 보안 옵션이 활성화되어 있는 경우

취약

SELinux 보안 옵션이 활성화되어 있지 않은 경우

진단 방법

■ 프로세스 확인을 통해 SELinux 옵션 적용 확인

1) # ps –ef | grep docker | grep selinux-enabled

```
root@k8s-master:~# ps -ef | grep docker | grep selinux-enabled
root@k8s-master:~#
```

■ 명령어를 입력하여 SELinux 옵션 적용 확인

2) # docker ps --quiet --all | xargs docker inspect --format '{{ .Id }}: SecurityOpt={{ .HostConfig.SecurityOpt }}'

조치 방법

■ SELinux 활성화

1) /etc/default/docker 파일 내 DOCKER_OPTS="--selinux-enabled" 설정

2) /lib/systemd/system/docker.service 파일에 아래의 내용 수정

```
# for containers run by docker
EnvironmentFile=/etc/default/docker
ExecStart=/usr/bin/dockerd -H fd:// $DOCKER_OPTS
```

3) docker 데몬 재시작

4) --selinux-enabled 옵션 활성화 확인

```
root@k8s-master:~# ps -ef | grep docker
root        5019       1  0 00:39 ?        00:00:00 /usr/bin/dockerd -H fd:// --selinux-enabled
root       10387    3167  0 00:44 pts/0    00:00:00 grep --color=auto docker
```

컨테이너에서 ssh 사용 금지

항목설명

대부분 백업, 로그 확인, 프로세스 재시작, 설정 변경과 같은 작업을 위해 SSH를 사용한다. 하지만 Docker 컨테이너에서의 이러한 작업은 SSH가 없어도 가능하다. SSH 접속을 위해 사용하는 키와 패스워드는 이미지와 같이 만들거나 불륨에 넣는다. 키와 패스워드를 갱신해야 할 때, 이미지 안에 넣는 경우, 이미지를 다시 만들어 배포한 후 컨테이너를 재시작해야 한다. 인증정보를 볼륨에 넣어두고 관리하는 경우에는 컨테이너가 인증정보를 파손시킬 수 있으므로 컨테이너에 쓰기 권한을 부여해서는 안 된다.

진단 기준

양호

컨테이너에 SSH가 비활성화되어 있는 경우

취약

컨테이너에 SSH가 활성화되어 있는 경우

진단 방법

■ ssh 목록 확인

1) # docker ps —quiet
2) # docker exec 〈컨테이너 ID〉 ps -el

조치 방법

■ 컨테이너에서 ssh를 제거하고 docker exec, docker attach 명령어 통해 컨테이너 접속

1) # docker exec —interactive —tty $INSTANCE_ID sh
2) # docker attach $INSTANCE_ID

컨테이너에 PREVILEGED 포트 매핑 금지

항목설명

TCP/IP 포트 중 1024 미만의 포트는 권한이 있는 포트로 특정한 목적을 위해서 IANA에서 할당한 포트 번호이다. Docker를 사용하면 컨테이너 포트를 privileged 포트에 매핑할 수 있는데, 이때 일반 사용자와 프로세스는 다양한 보안상의 이유로 privileged 포트를 사용하지 않는 것이 좋다. 따라서 privileged 포트 이외의 별도 포트를 지정하여 매핑하도록 한다.

진단 기준

양호

컨테이너 포트가 privileged 포트에 매핑되지 않은 경우

취약

컨테이너 포트가 privileged 포트에 매핑된 경우

진단 방법

■ privileged 포트 매핑 확인

1) # docker ps —quiet —all
2) # docker inspect 〈CONTAINER ID〉 | grep -A 50 NetworkSettings | grep Ports

■ 컨테이너 전체 목록 출력 옵션을 통해 포트 매핑 확인

1) # docker ps -a

조치 방법

■ privileged가 아닌 포트로 매핑

1) 컨테이너 시작 시, 컨테이너 포트를 호스트의 privileged 포트가 아닌 포트로 매핑
2) Docker 파일에서 privileged 포트 매핑 선언을 호스팅하는 컨테이너가 없는지 확인

PIDs cgroup 제한

항목설명

공격자는 컨테이너 내부에서 포크 폭탄을 실행할 수 있다. 이 포크 폭탄으로 인해 전체 시스템이 손상될 수 있으므로 컨테이너 내부에서 발생할 수 있는 포크의 수를 제한함으로써 이러한 공격을 방지하여야 한다.

진단 기준

양호

PIDs cgroup 제한 설정이 적용된 경우

취약

PIDs cgroup 제한 설정이 적용되어 있지 않은 경우

진단 방법

■ PIDs cgroup 제한 설정 적용 확인

1) # docker ps --quiet --all | xargs docker inspect --format '{{ .Id }}:PidsLimit={{ .HostConfig.PidsLimit }}'

※ PidsLimit 값이 0 또는 -1이면 컨테이너 매부에서 동시에 모든 수의 프로세스를 fork 할 수 있음

조치 방법

■ 컨테이너 시작 시 —pids-limit 플래그를 사용 (예시)

1) # docker run -it —pids-limit 100 〈image_id〉

도커의 default bridge docker() 사용 제한

항목설명

Docker는 브리지 모드에서 생성된 가상 인터페이스를 docker0라는 공통 브리지에 연결한다. 이 네트워크 모델은 필터링이 적용되지 않기 때문에 ARP Spoofing 및 MAC Flooding 등의 공격에 취약하다.

진단 기준

양호

Default bridge docker0를 사용하고 있지 않은 경우

취약

Default bridge docker0를 사용하고 있는 경우

진단 방법

■ ifconfig 명령어를 통해 Default bridge docker0를 사용하고 있는지 확인

1) # ifconfig | grep docker

```
root@k8s-master:~# ifconfig | grep docker
docker0: flags=4099<UP,BROADCAST,MULTICAST>  mtu 1500
```

■ docker 명령어로 Default bridge docker0를 사용하고 있는지 확인

1) docker network ls --quiet | xargs xargs docker network inspect --format '{{.Name }}: {{ .Options }}' | grep name

```
root@k8s-master:~# docker network ls --quiet | xargs xargs docker network inspect --format '{{.Name }}: {{
bridge: map[com.docker.network.bridge.default_bridge:true com.docker.network.bridge.enable_icc:true com.d
st binding ipv4:0.0.0.0 com.docker.network.bridge.name:docker0 com.docker.network.driver.mtu:1500]
```

조치 방법

■ Default bridge docker() 비활성화

1) /etc/default/docker 파일 내 DOCKER_OPTS="--icc=false" 설정

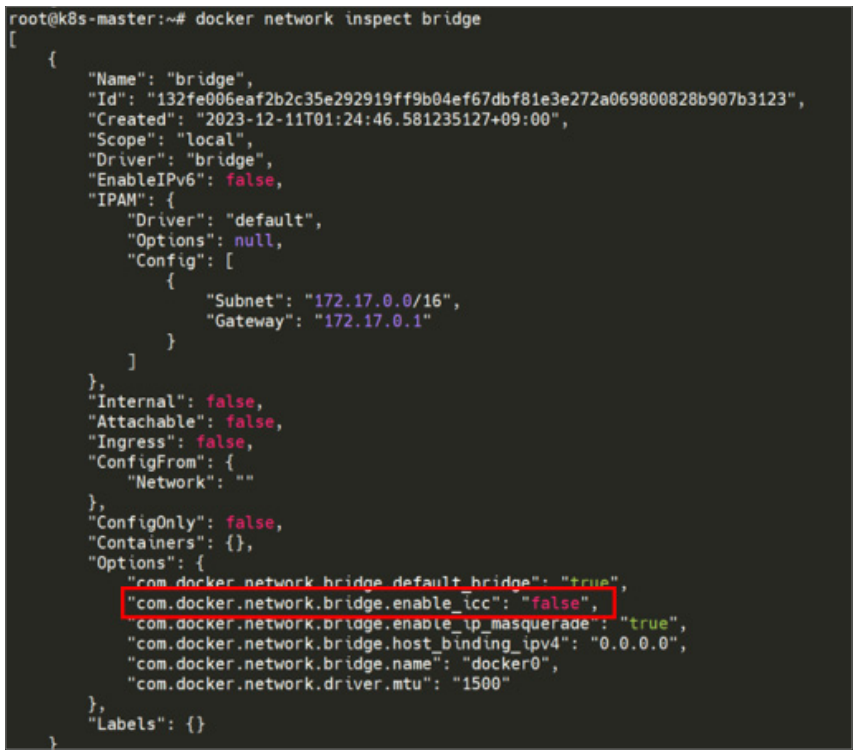
2) /lib/systemd/system/docker.service 파일에 아래의 내용 수정

```
# for containers run by docker
EnvironmentFile=/etc/default/docker
ExecStart=/usr/bin/dockerd -H fd:// $DOCKER_OPTS
```

3) docker 데몬 재시작

```
root@k8s-master:~# ps -ef | grep docker
root        8060       1  7 01:24 ?        00:00:00 /usr/bin/dockerd -H fd:// --icc=false
root        8246    6801  0 01:24 pts/2    00:00:00 grep --color=auto docker
```

4) # docker network inspect bridge



```
root@k8s-master:~# docker network inspect bridge
[
    {
        "Name": "bridge",
        "Id": "132fe006eaf2b2c35e292919ff9b04ef67dbf81e3e272a069800828b907b3123",
        "Created": "2023-12-11T01:24:46.581235127+09:00",
        "Scope": "local",
        "Driver": "bridge",
        "EnableIPv6": false,
        "IPAM": {
            "Driver": "default",
            "Options": null,
            "Config": [
                {
                    "Subnet": "172.17.0.0/16",
                    "Gateway": "172.17.0.1"
                }
            ]
        },
        "Internal": false,
        "Attachable": false,
        "Ingress": false,
        "ConfigFrom": {
            "Network": ""
        },
        "ConfigOnly": false,
        "Containers": {},
        "Options": {
            "com.docker.network.bridge.default_bridge": "true",
            "com.docker.network.bridge.enable_icc": "false",
            "com.docker.network.bridge.enable_ip_masquerade": "true",
            "com.docker.network.bridge.host_binding_ipv4": "0.0.0.0",
            "com.docker.network.bridge.name": "docker0",
            "com.docker.network.driver.mtu": "1500"
        },
        "Labels": {}
    }
```

5) 사용자 정의 네트워크 생성, 지정 (예시) / daemon.json 작성 시, “icc=false” 옵션 추가
   # docker network create my-net

6) 아래 명령어를 입력하여 docker() 제거 확인 및 사용자 정의 네트워크 확인
   # docker network ls

호스트의 user namespaces 공유 제한

항목설명

user namespaces는 컨테이너 내부의 루트 프로세스가 컨테이너 외부의 루트가 아닌 프로세스에 매핑되도록 한다. 따라서 호스트의 use namespaces을 컨테이너와 공유하면 호스트의 사용자와 컨테이너의 사용자가 분리되지 않는다.

진단 기준

양호

호스트의 user namespace를 컨테이너와 공유하고 있지 않은 경우

취약

호스트의 user namespace를 컨테이너와 공유하고 있는 경우

진단 방법

■ UsrnsMode 값 반환 확인

1) # docker ps --quiet --all | xargs docker inspect --format '{{ .Id }} :UsernsMode={{ .HostConfig.UsernsMode }}'

※ host 값을 반환하는 경우 호스트 user namespaces가 컨테이너와 공유되고 있는 상태

조치 방법

■ 호스트, 컨테이너 user namespaces 공유 제한

1) # docker run --rm -it --userns=host ubuntu bash (취약)
2) # docker run --rm -it ubuntu bash (양호)

2.27.

Kubernetes(Master)

2.27. Kubernetes(Master)

API Server Configuration(7개 항목), Controller Manager Configuration(2개 항목), etcd Configuration(2개 항목), PodSecurityAdmission Configuration(2개 항목), 파일 권한 설정(3개 항목), 패치 관리(1개 항목) 총 6개 영역에서 17개 항목으로 구성된다.

[표 27] Kubernetes(Master) 진단 체크리스트

구분	진단 항목
가. API Server Configuration	API sever 비인증 접근 차단
	API sever 취약한 방식의 인증 사용 제한
	API server 서비스 API 외부 오픈 금지
	API server 권한 제어
	Admission Control Plugin 설정
	API server SSL/TLS 적용
	API server 로그 관리
나. Controller Manager Configuration	Controller 인증 제어
	Controller Manager SSL/TLS 적용
다. etcd Configuration	etcd 암호화 적용
	etcd SSL/TLS 적용
라. PodSecurityAdmission Configuration	컨테이너 권한 제어
	네임스페이스 공유 금지
마. 파일 권한 설정	환경설정 파일 권한 설정
	인증서 파일 권한 설정
	etcd 데이터 디렉터리 권한 설정
바. 패치 관리	최신 보안 패치 적용

API sever 비인증 접근 차단

항목설명

API Server 비인증 접근 차단이 허용될 경우, 익명 요청이 활성화되며 비인가자가 서버에 접근하여 Kubernetes 시스템 환경에 영향을 줄 수 있다.

진단 기준

양호

API server 비인증 접근을 차단한 경우

취약

API server 비인증 접근을 허용한 경우

진단 방법

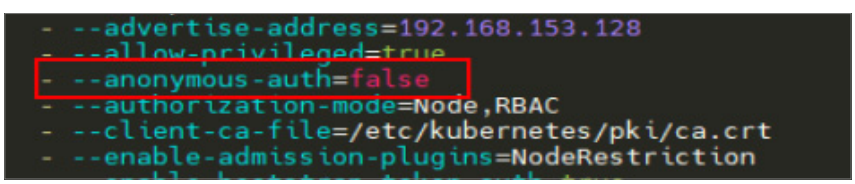
■ Master Node에서 /etc/kubernetes/manifests/kube-apiserver.yaml 파일 내 아래의 파라미터 존재 및 적절한 인자 값 설정 여부 확인

1) - --anonymous-auth
2) - --service-account-lookup

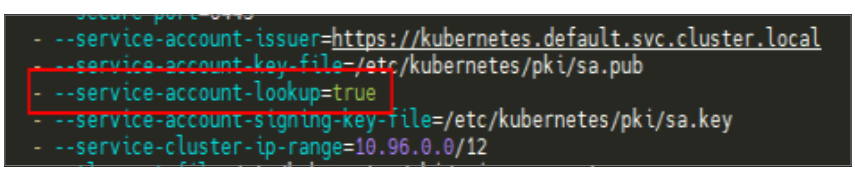
조치 방법

■ 비인증 접근 차단

1) /etc/kubernetes/manifests/kube-apiserver.yaml 파일 내 아래와 같이 설정
   - --anonynous-auth=false



2) /etc/kubernetes/manifests/kube-apiserver.yaml 파일 내 아래와 같이 설정
   - --service-account-lookup=true



API server 취약한 방식의 인증 사용 제한

항목설명

API sever에서 취약한 방식의 인증을 사용할 경우, 비인가자의 접근으로 인해 Kubernetes 시스템의 모든 요소에 영향을 줄 수 있다.

진단 기준

양호

API sever 취약한 방식의 인증 사용을 제한한 경우

취약

API sever 취약한 방식의 인증 사용을 허용한 경우

진단 방법

■ 취약한 방식의 인증 사용

1) /etc/kubernetes/manifests/kube-apiserver.yaml 파일 내 아래의 파라미터 존재 여부 확인
   - --token-auth-file

조치 방법

■ 취약한 방식의 인증 사용 제한

1) /etc/kubernetes/manifests/kube-apiserver.yaml 파일 확인
   - --token-auth-file 파라미터가 존재할 경우, 해당 파라미터 삭제

API sever 서비스 API 외부 오픈 금지

항목설명

API Server의 서비스 API가 외부에서 접근 가능할 경우, Kubernetes 시스템의 모든 요소에 영향을 줄 수 있으므로 클러스터의 공격을 최소화하기 위해 로컬호스트 인터페이스에만 바인딩 설정을 해야 한다.

진단 기준

양호

API server 서비스 API가 외부에서 접근 불가능한 경우

취약

API server 서비스 API가 외부에서 접근 가능한 경우

진단 방법

■ 서비스 API 외부 오픈 금지

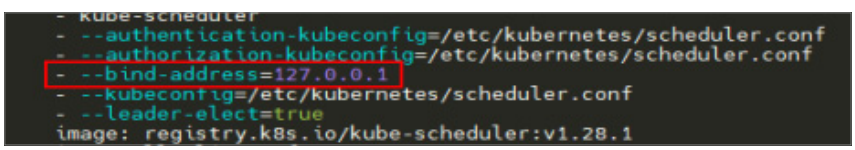
1) /etc/kubernetes/manifests/kube-scheduler.yaml 파일 내 아래의 파라미터 값 존재 및 적절한 인자값 설정 여부 확인
   - --bind-address

2) /etc/kubernetes/manifests/kube-controller-manager.yaml 파일 내 아래의 파라미터 값 존재 및 적절한 인자값 설정 여부 확인
   - --bind-address

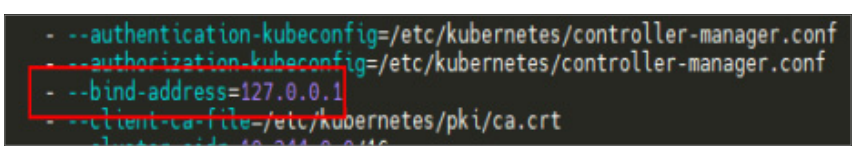
조치 방법

■ 서비스 API 외부 오픈 금지

1) scheduler API 서비스
   etc/kubernetes/manifests/kube-scheduler.yaml 파일 내 아래와 같이 설정



2) controller manager API 서비스
   etc/kubernetes/manifests/kube-controller-manager.yaml 파일 내 아래와 같이 설정



비고

※ 설정값이 비어있거나 0.0.0.0(::)으로 설정된 경우, 모든 인터페이스가 접근 가능하다는 의미이므로 설정 변경이 필요하다.

API server 권한 제어

항목설명

API sever가 모든 요청에 대하여 허용하도록 설정되어 있거나 필요한 권한 이상으로 사용자 또는 그룹에 부여될 경우 악의적인 사용자나 부주의한 사용자에 의해 Kubernetes에서 관리하는 다른 컨테이너의 작업에 영향을 줄 수 있다. 따라서 특정 호스트, 컨테이너 및 이미지에서 특정 작업을 수행할 수 있는 최소한의 권한만을 부여한다.

진단 기준

양호

API server 권한이 AlwaysAllow 값으로 설정되어 있지 않은 경우

취약

API server 권한이 AlwaysAllow 값으로 설정되어 있는 경우

진단 방법

■ API server 권한 제어 설정 확인

1) /etc/kubernetes/manifests/kube-apiserver.yaml 파일 내 AlwaysAllow 설정 확인

```
root@k8s-master:~# cat /etc/kubernetes/manifests/kube-apiserver.yaml | grep authorization
    - --authorization-mode=AlwaysAllow
root@k8s-master:~#
```

※ --authorization-mode=AlwaysAllow인 경우 취약

조치 방법

■ API server 권한 제어 설정

1) authorization-mode 인자 값을 AlwaysAllow가 아닌 값으로 수정
   - --authorization-mode=Node, RBAC (예시)

```
    - --allow-privileged=true
    - --authorization-mode=Node,RBAC
    - --client-ca-file=/etc/kubernetes/pki/ca.crt
    - --enable-admission-plugins=NodeRestriction
```

비고

--authorization-mode 인수	
ABAC	속성 기반 접근제어, 로컬 파일을 사용하여 정책 구성
RBAC	역할 기반 접근제어, 쿠버네티스 API를 사용하여 정책을 구성
Webhook	원격 REST 엔드포인트를 사용하여 인가를 관리
Node	Kubelet이 생성한 API 요청을 특별히 인가시키는 특수 목적 인가 모드
AlwaysDeny	모든 요청을 차단하며 테스트에만 사용
AlwaysAllow	모든 요청을 허용하며 API 인가가 필요하지 않을 경우에만 사용

Admission Control Plugin 설정

항목설명

Kubernetes 고급 기능을 지원하기 위해 Admission Controller를 활성화한다. 적절한 플러그인을 사용하지 않을 경우, Kubernetes API Server가 불안정해질 수 있으므로 반드시 필요한 Plugin만 활성화해야 한다.

진단 기준

양호

Admission Control Plugin 설정이 적절하게 적용된 경우

취약

Admission Control Plugin 설정이 적용되지 않은 경우

진단 방법

■ Admission Control 설정 검토

1) /etc/kubernetes/manifests/kube-apiserver.yaml 파일 내 아래의 파라미터 존재 및 적절한 인자값 설정 여부 확인
- --admission-control-config-file
- --enable-admission-plugins
- --disable-admission-plugins

조치 방법

■ Admission Control 설정 검토

1) /etc/kubernetes/manifests/kube-apiserver.yaml 파일 내 아래와 같이 설정
--enable-admission-plugins=AlwaysAdmin (제거)
--enable-admission-plugins=AlwaysPullImages (추가)
--enable-admission-plugins=NodeRestriction (추가)
--enable-admission-plugins=SecurityContextDeny (추가)

--enable-admission-plugins=PodSecurityPolicy
--disable-admission-plugins=NamespaceLifecycle (제거)
--enable-admission-plugins=EventRateLimit (추가)
--admission-control-config-file = <path> (추가)

비고

※ Kubernetes 1.25 버전 이상부터 PodSecurityPolicy 지원이 중단됨에 따라 PodSecuritAdmission을 통해 PodSecurityStandard 적용이 필요함

API server SSL/TLS 적용

항목설명

SSL/TLS 통신 적용을 통해 네트워크 스니핑과 같은 공격으로 주요 정보가 노출되지 않도록 안전한 통신을 해야 하며, API server에 접근하는 대상에 대해 검증할 수 있도록 설정해야 한다. 또한 SSL/TLS 통신 적용 시에는 주기적으로 인증서를 변경하고 안전한 버전의 암호화 방식을 사용하는 방법을 통해 위험을 최소화할 수 있는 정책 설정이 필요하다.

진단 기준

양호

API server SSL/TLS가 적용된 경우

취약

API server SSL/TLS가 적용되지 않은 경우

진단 방법

■ SSL/TLS 적용을 통한 네트워크 구간 데이터 보호

1) /etc/kubernetes/manifests/kube-apiserver.yaml 파일 내 아래의 파라미터 존재 및 적절한 인자값 설정 여부 확인
   - --secure-port

■ 인증서 관리 (API Server to kubelet)

1) /etc/kubernetes/manifests/kube-apiserver.yaml 파일 내 아래의 파라미터 존재 및 적절한 인자값 설정 여부 확인
   - --kubelet-certificate-authority
   - --kubelet-client-certificate
   - --kubelet-client-key
   - --kubelet-account-key-file

■ 인증서 관리 (API Server)

1) /etc/kubernetes/manifests/kube-apiserver.yaml 파일 내 아래의 파라미터 존재 및 적절한 인자값 설정 여부 확인
   - --tls-cert-file
   - --tls-private-key-file
   - --client-ca-file

■ 안전한 SSL/TLS 버전 사용

1) /etc/kubernetes/manifests/kube-apiserver.yaml 파일 내 아래의 파라미터 존재 및 적절한 인자값 설정 여부 확인
   - --tls-cipher-suites

조치 방법

■ SSL/TLS 적용을 통한 네트워크 구간 데이터 보호

1) /etc/kubernetes/manifests/kube-apiserver.yaml 파일 내 아래의 파라미터를 제거 또는 0이 아닌 값으로 설정
- --secure-port

■ 인증서 관리 (API Server to kubelet)

1) /etc/kubernetes/manifests/kube-apiserver.yaml 파일 내 아래의 파라미터에 파일 추가
- --kubelet-certificate-authority=〈인증서 파일〉
- --kubelet-client-certificate=〈client 인증서 파일〉
- --kubelet-client-key=〈client 키 파일〉
- --kubelet-account-key-file=〈servive account 키 파일〉

■ 인증서 관리 (API Server)

1) /etc/kubernetes/manifests/kube-apiserver.yaml 파일 내 아래의 파라미터에 파일 추가
- --tls-cert-file=〈tls 인증서 파일〉
- --tls-private-key-file=〈tls 키 파일〉
- --client-ca-file=〈client ca 인증서 파일〉

■ 안전한 SSL/TLS 버전 사용 (예시)

1) /etc/kubernetes/manifests/kube-apiserver.yaml 파일 내 아래의 파라미터에 추가
- --tls-cipher-suites=TLS_ECDSA_WITH_AED_128_GCM_SHA256,TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256

API Server 로그 관리

항목설명

로그 정보는 침해 사고 발생시 해킹의 흔적 및 공격기법을 확인할 수 있는 중요 자료로 정기적인 로그 분석을 통하여 시스템 침입 흔적을 확인할 수 있다.

진단 기준

양호

API server 로그가 활성화된 경우

취약

API server 로그가 비활성화되어 있는 경우

진단 방법

■ 로그 관리

1) /etc/kubernetes/manifests/kube-apiserver.yaml 파일 내 아래의 파라미터 존재 및 적절한 인자값 설정 여부 확인
   - --auditlog-path
   - --audit-policy-file
   - --audit-log-maxage
   - --audit-log-maxbackup
   - --audit-log-maxsize

조치 방법

■ 로그 설정

1) /etc/kubernetes/manifests/kube-apiserver.yaml 파일 내 아래의 파라미터에 설정
   - --auditlog-path
   - --audit-policy-file
   - --audit-log-maxage
   - --audit-log-maxbackup
   - --audit-log-maxsize

Controller 인증 제어

항목설명

Controller는 클러스터의 상태를 감시하고 현재 상태와 원하는 상태가 일치하도록 관리하는 작업을 한다. 각 컨트롤러에 대해 개별 서비스 계정 자격증명을 사용해 인가된 계정만이 클러스터를 제어할 수 있도록 설정해야한다.

진단 기준

양호

Controller 인증 제어 설정이 적용된 경우

취약

Controller 인증 제어 설정이 적용되지 않은 경우

진단 방법

■ 컨트롤러에 대해 개별 서비스 계정 자격증명

1) /etc/kubernetes/manifests/kube-controller-manager.yaml 파일 내 아래의 파라미터 존재 및 적절한 인자값 설정 여부 확인
- --use-service-account-credentials

■ 컨트롤러 계정 자격증명에 사용되는 인증서 관리

1) /etc/kubernetes/manifests/kube-controller-manager.yaml 파일 내 아래의 파라미터 존재 및 적절한 인자값 설정 여부 확인
- --service-account-private-key-file

조치 방법

■ 컨트롤러에 대해 개별 서비스 계정 자격증명

1) /etc/kubernetes/manifests/kube-controller-manager.yaml 파일 내 아래의 파라미터에 설정
- --use-service-account-credentials=true

■ 컨트롤러 계정 자격증명에 사용되는 인증서 관리

1) /etc/kubernetes/manifests/kube-controller-manager.yaml 파일 내 아래의 파라미터에 파일 추가
- --service-account-private-key-file= 〈 〉

비고

※ default 설정
user-service-account-credentials : true
service-account-private-key-file : /etc/kubernetes/pki/sa.key

Controller Manager SSL/TLS 적용

항목설명

Kubernetes에서는 SSL/TLS를 이용하여 네트워크상의 DATA 보호 및 각 구성 요소에 접하는 클라이언트에 대한 검증을 위해 사용할 수 있다. SSL/TLS 통신 적용을 통해 네트워크 스니핑과 같은 방법으로 주요 정보가 노출되어 다른 공격에 이용되지 않도록 하고, API server에 접근하는 대상에 대해 검증할 수 있도록 설정해야 한다. 또한, SSL/TLS 통신 적용 시에는 주기적으로 인증서를 변경하고 안전한 버전의 암호화 방식을 사용하는 방법을 통해 위험을 최소화할 수 있는 정책 설정이 필요하다.

진단 기준

양호

Controller Manager SSL/TLS 설정이 적용된 경우

취약

Controller Manager SSL/TLS 설정이 적용되지 않은 경우

진단 방법

■ SSL/TLS 적용을 통한 클라이언트 인증

1) /etc/kubernetes/manifests/kube-controller-manager.yaml 파일 내 아래의 파라미터 존재 및 적절한 인자값 설정 여부 확인
- --root-ca-file

■ 인증서 관리

1) /etc/kubernetes/manifests/kube-controller-manager.yaml 파일 내 아래의 파라미터 존재 및 적절한 인자값 설정 여부 확인
- --feature-gates

조치 방법

■ SSL/TLS 적용을 통한 클라이언트 인증

1) /etc/kubernetes/manifests/kube-controller-manager.yaml 파일 내 아래의 파라미터에 파일 추가
- --root-ca-file=〈〉

■ 인증서 관리

1) /etc/kubernetes/manifests/kube-controller-manager.yaml 파일 내 아래의 파라미터 문구 추가
- --feature-gates=RotateKubeletServerCertificate=true

etcd 암호화 적용

항목설명

etcd는 Kubernetes와 같은 분산시스템에서 중요한 데이터를 저장할 때 사용할 수 있는 키 값 분산 저장소 역할을 하고 있다. 따라서 etcd에 저장되는 데이터는 매우 민감하므로 공개되지 않도록 저장 시 암호화되어야 한다.

진단 기준

양호

etcd 암호화 방식이 aescbc 이상으로 설정된 경우

취약

etcd 암호화 방식이 적용되지 않거나 취약한 방식으로 설정된 경우

진단 방법

■ etcd 암호화 적용

1) /etc/kubernetes/manifests/kube-apiserver.yaml 파일 내 아래의 파라미터 존재 및 적절한 인자값 설정여부 확인
   - --encryption-provider-config

■ 안전한 암호화 방식 사용

1) 아래 명령어 실행 후, --encryption-provider-config 값 확인
   # ps -ef | grep kube-apiserver
2) - --encryption-provider-config 내 설정된 경로의 암호화 설정 파일 분석을 통해 안전한 암호화 방식 사용 여부 확인

조치 방법

■ etcd 암호화 적용

1) /etc/kubernetes/manifests/kube-apiserver.yaml 파일 내 아래의 파라미터에 파일 추가
   - --encryption-provider-config=〈〉

■ 안전한 암호화 방식 사용

1) 아래 명령어 실행 후, --encryption-provider-config 값 확인
   # ps -ef | grep kube-apiserver

etcd SSL/TLS 적용

항목설명

etcd는 중요한 데이터에 대한 액세스를 안정적이고 신속하게 보존하고 제공하도록 설계된 분산된 키 값 저장소로 Kubernetes에서 설정, 네임스페이스 등의 pod/service 상태 저장과 DNS 데이터 저장에 사용되고 있다. etcd에 저장되는 DATA는 민감하므로 네트워크 구간 암호화 및 접근하는 클라이언트에 대한 인증을 통한 DATA 보호가 이루어져야 한다. SSL/TLS 통신 적용을 통해 네트워크 스니핑과 같은 방법으로 etcd 내 주요 정보가 노출되어 다른 공격에 이용되지 않도록 하고, etcd에 접근하는 대상에 대해 검증할 수 있도록 설정해야 한다.

진단 기준

양호

etcd SSL/TLS 설정이 적용된 경우

취약

etcd SSL/TLS 설정이 적용되지 않은 경우

진단 방법

■ SSL/TLS 적용을 통한 클라이언트 인증(etcd peer 및 클라이언트)

1) /etc/kubernetes/manifests/etcd.yaml 파일 내 아래의 파라미터 존재 및 적절한 인자값 설정 여부 확인
   - --client-cert-auth
   - --perr-client-cert-auth (etcd server의 경우 적용 필요 없음)

■ 인증서 관리(etcd peer 및 클라이언트) (인증서 설정)

1) /etc/kubernetes/manifests/etcd.yaml 파일 내 아래의 파라미터 존재 및 적절한 인자값 설정 여부 확인
   - --cert-file
   - --key-file
   - --peer-cert-file
   - --peer-key-file

2) /etc/kubernetes/manifests/etcd.yaml 파일 내 아래의 파라미터 존재 및 적절한 인자값 설정 여부 확인
   - --etcd-certfile
   - --etcd-keyfile
   - --etcd-cafile

■ 인증서 관리(자체 서명인증서 사용금지)

1) /etc/kubernetes/manifests/etcd.yaml 파일 내 아래의 파라미터 존재 및 적절한 인자값 설정 여부 확인
   - --auto-tls
   - --peer-auto-tls
   - --trusted-ca-fiile

조치 방법

■ SSL/TLS 적용을 통한 클라이언트 인증(etcd peer 및 클라이언트)

1) /etc/kubernetes/manifests/etcd.yaml 파일 내 아래와 같이 설정
--client-cert-auth=true 추가
--peer-client-cert-auth=true 수정 (etcd server의 경우 적용 필요 없음)

■ 인증서 관리(etcd peer 및 클라이언트) (인증서설정 예시)

1) /etc/kubernetes/manifests/etcd.yaml 파일 내 아래와 같이 설정
--cert-file=〈인증서 파일〉 추가
--key-file=〈키 파일〉 추가
--peer-cert-file=〈peer 인증서 파일〉
--peer-key-file=〈peer 키 파일〉 추가

2) /etc/kubernetes/manifests/kube-apiserver.yaml 파일 내 아래와 같이 설정
--etcd-certfile=〈etcd cert 인증서 파일〉 추가
--etcd-keyfile=〈etcd 키 파일〉 추가
--etcd-cafile=〈etcd ca 인증서 파일〉 추가

■ 인증서 관리(자체 서명인증서 사용금지)

1) /etc/kubernetes/manifests/etcd.yaml 파일 내 아래와 같이 설정
--auto-tls=false
--peer-auto-tls=false or 제거 (etcd server의 경우 적용 필요 없음)
--trusted-ca-file=〈인증서 파일〉 추가

컨테이너 권한 제어

항목설명

PodSecurityAdmission(이하 PSA)는 클러스터 및 네임스페이스 수준의 리소스로, 파드에 대해 서로 다른 격리 수준을 정의한다. PodSecurityStandard(이하 PSS)를 적용하기 위해 내장된 PSA Controller를 통해 수행된다. PSS 수준에 맞지 않은 Pod를 생성할 경우 설정된 PSS 수준에 따라 내장된 PSA Controller가 유효성을 검사한다. 따라서, 파드 내 컨테이너가 불필요한 권한을 가지지 않도록 PSA를 통해 PSS를 적용하여 운용해야 한다.

진단 기준

양호

PodSecurityAdmission 정책을 통해 컨테이너 권한을 제어한 경우

취약

PodSecurityAdmission 정책을 통해 컨테이너가 불필요한 권한을 사용한 경우

진단 방법

■ 컨테이너 권한 제어

1) pod 생성 *.yaml 파일 내 securityContext 필드 아래의 설정값 유무 확인
   -allowPrivilegeEscalation
   -runAsUser
   -runAsNonRoot
   -capabilities.drop
   -seccompProfile

조치 방법

■ 컨테이너 권한 제어

1) pod 생성 *.yaml 파일 내에 SecurityContext 설정값 수정 (예시)
   -allowPrivilegeEscalation: false (추가)
   -runAsUser: 0이 아닌 값 (추가)
   -runAsNonRoot: true (추가)
   -capabilities.drop: (추가)
   drop: [“ALL”]
   -seccomprofiles: (추가)
   type: “ReuntimeDefault”

```
- name: test-deployment
  image: nginx:1.7.9
  securityContext:
    allowPrivilegeEscalation: false
    runAsUser: 1000
    runAsNonRoot: true
    capabilities:
      drop: ["ALL"]
    seccompProfile:
      type: "RuntimeDefault"
```

2) namespace 생성 시, namespace에 PodSecurityAdmission 정책을 아래와 같이 적용(enforce, warn 인수는 privileged가 아닌 restricted로 설정)
   # kubectl label —overwrite ns test-restricted pod-security.kubernetes.io/enforce=restricted pod-security.kubernetes.io/warn=restricted

네임스페이스 공유 금지

항목설명

파드의 컨테이너는 일반적으로 별도의 리눅스 네임스페이스에서 실행되므로 프로세스가 다른 컨테이너 또는 노드의 기본 네임스페이스에서 실행 중인 프로세스와 분리된다. 파드의 스펙에서 hostNetwork 옵션을 true로 설정하여 가상 네트워크 어댑터 대신 노드의 실제 네트워크 어댑터를 사용할 수 있으며 그 결과 해당 파드는 노드의 인터페이스를 사용하게 된다. 또한, hostNetwork 옵션과 유사한 파드 스펙 속성으로 hostPID와 hostIPC가 있다. 이를 true로 설정하면 파드의 컨테이너는 노드의 PID와 IPC 네임스페이스를 사용해 컨테이너에서 실행 중인 프로세스가 노드의 다른 프로세스를 보거나 IPC로 이들과 통신할 수 있다. 따라서, PSA(Pod Security Admission) 설정을 통해 호스트 IPC, PID, 네트워크 네임스페이스 사용을 방지하여 불필요한 권한을 제거해야 한다.

진단 기준

양호

네임스페이스 공유 금지 설정이 적용된 경우

취약

네임스페이스 공유 금지 설정이 적용되지 않은 경우

진단 방법

■ 네임스페이스 공유 금지

1) pod 생성 *.yaml 파일 내 spec 필드에서 아래의 설정값 유무 확인
   - hostNetwork
   - hostPID
   - hostIPC

```
    app: test-deployment
template:
  metadata:
    labels:
      app: test-deployment
  spec:
    hostNetwork: false
    hostPID:  false
    hostIPC: false
    containers:
    - name: test-deployment
```

조치 방법

■ 네임스페이스 공유 금지

1) pod 생성 *.yaml 파일 내 spec 필드에서 아래의 설정값 유무 확인
   - hostNetwork: false 또는 파라미터 제거
   - hostPID: false 또는 파라미터 제거
   - hostIPC: false 또는 파라미터 제거

환경설정 파일 권한 설정

항목설명

Kubernetes 환경설정 파일의 접근 권한이 과도하게 설정된 경우, 비인가자가 다양한 방법으로 Kubernetes 설정을 변경해 침해 사고를 일으킬 가능성이 있다. 따라서 비인가자가 파일을 수정할 수 없도록 파일의 접근 권한을 제한해 파일의 무결성을 유지해야 한다.

진단 기준

양호

환경설정 파일의 소유자 및 소유 그룹이 root이고, 접근 권한이 644 이하로 설정된 경우

취약

환경설정 파일의 소유자 및 소유 그룹이 root가 아니거나, 접근 권한이 644 초과로 설정된 경우

진단 방법

- kube-apiserver.yaml 접근 권한 확인

  # ls -al /etc/kubernetes/manifests/kube-apiserver.yaml

- kube-controller-manager.yaml 접근 권한 확인

  # ls -al /etc/kubernetes/manifests/kube-controller-manager.yaml

- kube-scheduler.yaml 접근 권한 확인

  # ls -al /etc/kubernetes/manifests/kube-scheduler.yaml

- etcd.yaml 접근 권한 확인

  # ls -al /etc/kubernetes/manifests/etcd.yaml

- admin.conf 접근 권한 확인

  # ls -al /etc/kubernetes/manifests/admin.conf

- scheduler.conf 접근 권한 확인

  # ls -al /etc/kubernetes/manifests/scheduler.conf

- controller-manager.conf 접근 권한 확인

  # ls -al /etc/kubernetes/manifests/controller-manager.conf

조치 방법

■ kube-apiserver.yaml 소유자 및 소유 그룹은 root, 접근 권한은 644 이하로 설정

ls -al /etc/kubernetes/manifests/kube-apiserver.yaml

```
-rw------- 1 root root 4047  9월   2 04:10 kube-apiserver.yaml
```

■ kube-controller-manager.yaml 소유자 및 소유 그룹은 root, 접근 권한은 644 이하로 설정

ls -al /etc/kubernetes/manifests/kube-controller-manager.yaml

```
-rw------- 1 root root 3543  9월   2 04:10 kube-controller-manager.yaml
```

■ kube-scheduler.yaml 소유자 및 소유 그룹은 root, 접근 권한은 644 이하로 설정

ls -al /etc/kubernetes/manifests/kube-scheduler.yaml

```
-rw------- 1 root root 1463  9월   2 04:10 kube-scheduler.yaml
```

■ etcd.yaml 소유자 및 소유 그룹은 root, 접근 권한은 644 이하로 설정

ls -al /etc/kubernetes/manifests/etcd.yaml

```
-rw-------- 1 root root 2419  9월   2 04:10 etcd.yaml
```

■ admin.conf 소유자 및 소유 그룹은 root, 접근 권한은 644 이하로 설정

ls -al /etc/kubernetes/manifests/admin.conf

```
-rw-------   1 root root 5651  9월   2 04:10 admin.conf
```

■ scheduler.conf 소유자 및 소유 그룹은 root, 접근 권한은 644 이하로 설정

ls -al /etc/kubernetes/manifests/scheduler.conf

```
-rw-------   1 root root 5627  9월   2 04:10 scheduler.conf
```

■ controller-manager.conf 소유자 및 소유 그룹은 root, 접근 권한은 644 이하로 설정

ls -al /etc/kubernetes/manifests/controller-manager.conf

```
-rw-------   1 root root 5679  9월   2 04:10 controller-manager.conf
```

인증서 파일 권한 설정

항목설명

인증서와 인증서가 포함된 디렉터리의 접근 권한이 과도하게 설정될 경우, SSL 구성을 통한 네트워크상 데이터 보호 및 사용자 인증을 위해 사용되는 인증서가 비인가자에 의해 유출될 위험이 존재한다. 따라서 root 이외 다른 사용자가 접근할 수 없도록 파일의 권한을 제한해야 한다.

진단 기준

양호

파일의 소유자 및 소유 그룹이 root이고, 인증서 파일의 접근 권한은 644, 키 파일의 접근 권한은 600 이하로 설정된 경우

취약

파일의 소유자 및 소유 그룹이 root가 아니거나, 인증서 파일의 접근 권한은 644, 키 파일의 접근 권한은 600 초과로 설정된 경우

진단 방법

■ pki 인증서 파일 접근 권한 확인

```
# ls –al /etc/kubernetes/pki/*.crt
```

■ pki 키 파일 접근 권한 확인

```
# ls –al /etc/kubernetes/pki/*.key
```

■ Hardway로 설치된 경우(예시)

```
# ls –al /var/;ib/kubernetes/ 내 pem 파일 접근 권한 확인
```

조치 방법

■ pki 인증서 파일 접근 권한 확인

```
# chmod 644 /etc/kubernetes/pki/*.crt
```

```
-rw-r--r-- 1 root root 1155  9월  2 04:10 /etc/kubernetes/pki/apiserver-etcd-client.crt
-rw-r--r-- 1 root root 1164  9월  2 04:10 /etc/kubernetes/pki/apiserver-kubelet-client.crt
-rw-r--r-- 1 root root 1285  9월  2 04:10 /etc/kubernetes/pki/apiserver.crt
-rw-r--r-- 1 root root 1107  9월  2 04:10 /etc/kubernetes/pki/ca.crt
-rw-r--r-- 1 root root 1123  9월  2 04:10 /etc/kubernetes/pki/front-proxy-ca.crt
-rw-r--r-- 1 root root 1119  9월  2 04:10 /etc/kubernetes/pki/front-proxy-client.crt
```

■ pki 키 파일 접근 권한 확인

```
# chmod 600 /etc/kubernetes/pki/*.key
```

```
-rw------- 1 root root 1679  9월  2 04:10 /etc/kubernetes/pki/apiserver-etcd-client.key
-rw------- 1 root root 1675  9월  2 04:10 /etc/kubernetes/pki/apiserver-kubelet-client.key
-rw------- 1 root root 1679  9월  2 04:10 /etc/kubernetes/pki/apiserver.key
-rw------- 1 root root 1675  9월  2 04:10 /etc/kubernetes/pki/ca.key
-rw------- 1 root root 1679  9월  2 04:10 /etc/kubernetes/pki/front-proxy-ca.key
-rw------- 1 root root 1675  9월  2 04:10 /etc/kubernetes/pki/front-proxy-client.key
-rw------- 1 root root 1679  9월  2 04:10 /etc/kubernetes/pki/sa.key
```

■ Hardway로 설치된 경우(예시)

```
# chmod 600 /var/lib/kubernetes/*.pem
```

etcd 데이터 디렉터리 권한 설정

항목설명

etcd 데이터 디렉터리의 접근 권한이 과도하게 설정된 경우, 비인가자가 다양한 방법으로 etcd 설정을 변경해 침해 사고를 일으킬 가능성이 있다. 또한, etcd 내에는 kubernetes 설정, 네임스페이스, pod 상태 등과 같은 민감한 데이터가 존재한다. 따라서 비인가자가 파일을 수정할 수 없도록 파일의 접근 권한을 제한해 파일의 무결성을 유지해야 한다.

진단 기준

양호

etcd 데이터 디렉터리의 소유자 및 소유 그룹이 root 또는 전용 계정이고, 접근 권한이 700 이하로 설정된 경우

취약

etcd 데이터 디렉터리의 소유자 및 소유 그룹이 root 또는 전용 계정이 아니거나, 접근 권한이 700 초과로 설정된 경우

진단 방법

■ etcd 디렉터리 접근 권한 확인

```
# ls –ald /var/lib/etcd
```

조치 방법

■ etcd 디렉터리 소유자 및 소유자 그룹 root, 접근 권한 700 이하로 설정

```
# chmod 700 /var/lib/etcd
# chown root:root /var/lib/etcd
```

최신 보안 패치 적용

항목설명

주기적인 패치 적용을 통하여 보안성 및 시스템 안전성을 확보하는 것이 시스템 운용의 중요한 요소이다. 서비스 중인 시스템에서 패치 적용에 따라 발생하는 서비스 영향도를 확인하고 패치 적용 시 많은 부분을 고려해야 한다.

진단 기준

양호

최신 보안 패치가 적용되거나 보안 취약점이 존재하지 않는 버전을 사용하는 경우

취약

보안 취약점이 존재하거나 지원이 종료된 버전을 사용하는 경우

진단 방법

■ 최신 업데이트 설치 여부 확인

1) #kubectl version

```
test@k8s-master:/var/lib$ kubectl version
Client Version: v1.28.1
Kustomize Version: v5.0.4-0.20230601165947-6ce0bf390ce3
Server Version: v1.28.1
test@k8s-master:/var/lib$
```

조치 방법

■ 최신 보안 업데이트 적용 여부 확인

1) # kubectl version
2) 기간 산정해서 보안 패치 적용(정기 PM 등)

※ 최신 버전을 사용하도록 권고하고 있으나 시스템 운영상 적용이 어려운 경우 최신이 아닌 취약점이 존재하지 않는 버전도 허용하고 있음

비고

※ 보안 패치 적용 시, 시스템 영향도를 파악하여 충분한 테스트 후 적용 권고

2.28.

Kubernetes(Worker)

2.28. Kubernetes(Worker)

Kubelet Configuration(4개 항목), 파일 권한 설정(2개 항목), 패치 관리(1개 항목) 총 3개 영역에서 7개 항목으로 구성된다.

[표 28] Kubernetes(Worker) 진단 체크리스트

구분	진단 항목
가. Kubelet Configuration	kubelet 인증 제어
	kubelet 권한 제어
	kubelet SSL/TLS 적용
	kernel 파라미터 설정
나. 파일 권한 설정	환경설정 파일 권한 설정
	인증서 파일 권한 설정
다. 패치 관리	최신 보안 패치 적용

Kubelet 인증 제어

항목설명

Kubelet은 각 노드에서 실행되는 에이전트로 Pod에 대해 정의된 PodSpec(yaml 또는 Json 형태)에 따라 컨테이너를 실행하고 동작하도록 관리하는 역할을 한다. 따라서 Kubelet의 비인증 접근은 Pod와 컨테이너의 정보 노출, 리소스 수정 등에 대해 영향을 줄 수 있으므로 Kubelet 인증 후 접근할 수 있도록 해야 한다.

진단 기준

양호
비인증 접근이 차단된 경우

취약
비인증 접근이 허용된 경우

진단 방법

■ Kubelet service 파일을 사용하는 경우

1) service 파일에 —anoymous-auth 설정이 false로 되어 있고 —read-only-port 설정이 0(비활성화)으로 되어 있는지 확인
$ cat [kubelet service 파일 경로] | grep “anonymous-auth\|read-only-port” | grep –v “#”

```
[root@k8s-node1 /]# cat /usr/lib/systemd/system/kubelet.service.d/10-kubeadm.conf  | grep "anonymous-auth\|
read-only-port" | grep -v "#"
[root@k8s-node1 /]#
```

■ Kubelet config 파일을 사용하는 경우

1) config 파일에 —anonymous-auth 설정이 false로 되어 있고, --read-only-port 설정이 0(비활성화)으로 되어 있는지 확인
$ cat [kubelet config 파일 경로]

조치 방법

■ Kubelet service 파일을 사용하는 경우

1) vi 명령어를 통해 —anonymous-auth 설정을 false로 —read-only-port 설정을 0으로 설정
$ vi [kubelet service 경로]
Environment="KUBELET_SYSTEM_PODS_ARGS=--anonymous-auth=false --read-only-prot=0" 설정 추가

```
# Note: This dropin only works with kubeadm and kubelet v1.11+
[Service]
Environment="KUBELET_KUBECONFIG_ARGS=--bootstrap-kubeconfig=/etc/kubernetes/bootstrap-kubelet.conf --kubeconfig=/etc/kubernetes/kubelet.conf"
Environment="KUBELET_CONFIG_ARGS=--config=/var/lib/kubelet/config.yaml"
Environment="KUBELET_SYSTEM_PODS_ARGS=--anonymous-auth=false --read-only-prot=0 --protect-kernel-defaults=true"
Environment="KUBELET_AUTHZ_ARGS=--authorization-mode=Webhook"
# This is a file that "kubeadm init" and "kubeadm join" generates at runtime, populating the KUBELET_KUBEADM_ARGS variable dynamically
EnvironmentFile=-/var/lib/kubelet/kubeadm-flags.env
# This is a file that the user can use for overrides of the kubelet args as a last resort. Preferably, the user should use
# the .NodeRegistration.KubeletExtraArgs object in the configuration files instead. KUBELET_EXTRA_ARGS should be sourced from this file.
EnvironmentFile=-/etc/sysconfig/kubelet
ExecStart=
ExecStart=/usr/bin/kubelet $KUBELET_KUBECONFIG_ARGS $KUBELET_CONFIG_ARGS $KUBELET_KUBEADM_ARGS $KUBELET_EXTRA_ARGS
```

2) kubelet 서비스 재시작
$ systemctl daemon-reload
$ systemctl restart kubelet.service

■ Kubelet config 파일을 사용하는 경우

1) vi 명령어를 통해 --anonymous-auth 설정을 false로 --read-only-port 설정을 0으로 설정
$ vi [kubelet config 파일 경로]

```
root@k8s-worker01:/var/lib/kubelet# cat config.yaml
apiVersion: kubelet.config.k8s.io/v1beta1
authentication:
  anonymous:
    enabled: false
  webhook:
    cacheTTL: 0s
    enabled: true
  x509:
    clientCAFile: /etc/kubernetes/pki/ca.crt
authorization:
  mode: Webhook
  webhook:
    cacheAuthorizedTTL: 0s
    cacheUnauthorizedTTL: 0s
readOnlyPort: 0
```

2) kubelet 서비스 재시작
$ systemctl daemon-reload
$ systemctl restart kubelet.service

Kubelet 권한 제어

항목설명

Kubelet은 기본적으로 API server 요청을 권한 인증 없이 모두 허용하고 있어 설정 변경을 통해 권한 인증 후 API server 요청을 처리하도록 해야 한다.

진단 기준

양호

API server 권한이 AlwaysAllow 값으로 설정되지 않은 경우

취약

API server 권한이 AlwaysAllow 값으로 설정된 경우

진단 방법

■ Kubelet service 파일을 사용하는 경우

1) service 파일에 --authorization-mode 설정이 되어 있는지 확인
$ cat [kubelet service 파일 경로] | grep "authorization-mode" | grep -v "#"

```
[root@k8s-node1 /]# cat /usr/lib/systemd/system/kubelet.service.d/10-kubeadm.conf | grep "authorizati
on-mode" | grep -v "#"
[root@k8s-node1 /]#
```

■ Kubelet config 파일을 사용하는 경우

1) config 파일에 --authorization-mode 설정이 되어 있는지 확인
$ cat [kubelet config 파일 경로]

```
address: 0.0.0.0
apiVersion: kubelet.config.k8s.io/v1beta1
authentication:
  anonymous:
    enabled: false
  webhook:
    cacheTTL: 2m0s
    enabled: true
  x509:
    clientCAFile: /etc/kubernetes/pki/ca.crt
authorization:
  mode: AlwaysAllow
```

조치 방법

■ Kubelet service 파일을 사용하는 경우

1) vi 명령어를 통해 --authorization-mode 설정에 모드 설정
$ vi [kubelet service 파일 경로]
Environment="KUBELET_SYSTEM_PODS_ARGS=--anonymous-auth=false --read-only-prot=0" 설정 추가

```
[ Note: This dropin only works with kubeadm and kubelet v1.11+
[Service]
Environment="KUBELET_KUBECONFIG_ARGS=--bootstrap-kubeconfig=/etc/kubernetes/bootstrap-kubelet.conf --kubeconfig=/etc/kubernetes/kubelet.conf"
Environment="KUBELET_CONFIG_ARGS=--config=/var/lib/kubelet/config.yaml"
Environment="KUBELET_SYSTEM_PODS_ARGS=--anonymous-auth=false --read-only-prot=0 --protect-kernel-defaults=true"
Environment="KUBELET_AUTHZ_ARGS=--authorization-mode=Webhook"
# This is a file that "kubeadm init" and "kubeadm join" generates at runtime, populating the KUBELET_KUBEADM_ARGS variable dynamically
EnvironmentFile=-/var/lib/kubelet/kubeadm-flags.env
# This is a file that the user can use for overrides of the kubelet args as a last resort. Preferably, the user should use
# the .NodeRegistration.KubeletExtraArgs object in the configuration files instead. KUBELET_EXTRA_ARGS should be sourced from this file.
EnvironmentFile=-/etc/sysconfig/kubelet
ExecStart=
ExecStart=/usr/bin/kubelet $KUBELET_KUBECONFIG_ARGS $KUBELET_CONFIG_ARGS $KUBELET_KUBEADM_ARGS $KUBELET_EXTRA_ARGS
```

2) kubelet 서비스 재시작
$ systemctl daemon-reload
$ systemctl restart kubelet.service

■ Kubelet config 파일을 사용하는 경우

1) vi 명령어를 통해 --authorization-mode 설정에 모드 설정
$ vi [kubelet config 파일 경로]

```
  webhook:
    cacheTTL: 0s
    enabled: true
  x509:
    clientCAFile: /etc/kubernetes/pki/ca.crt
authorization:
  mode: Webhook
  webhook:
    cacheAuthorizedTTL: 0s
    cacheUnauthorizedTTL: 0s
readOnlyPort: 0
cgroupDriver: systemd
clusterDNS:
```

2) kubelet 서비스 재시작
$ systemctl daemon-reload
$ systemctl restart kubelet.service

Kubelet SSL/TLS 적용

항목설명

API server, node 간 통신 시 민감한 데이터들이 평문으로 전송되면 스니핑과 같은 방법으로 민감한 데이터가 노출되므로 SSL/TLS 통신을 적용하여 송수신되는 데이터들을 보호하고 접근하는 대상에 대해 인증해야 한다. SSL/TLS 통신 적용 시 주기적으로 인증서를 변경하고 안전한 cipher suite를 사용해야 한다.

진단 기준

양호

kubelet SSL/TLS 통신을 위한 설정(인증서, 비밀키, 인증서 교환 주기, TLS 버전, cipher suites, hostname 변경 설정 비활성화)이 적용된 경우

취약

kubelet SSL/TLS 통신을 위한 설정(인증서, 비밀키, 인증서 교환 주기, TLS 버전, cipher suites, hostname 변경 설정 비활성화)이 적용되지 않은 경우

진단 방법

■ kubelet config 파일에서 클라이언트 CA 인증서가 설정되어 있는지 확인

1) $ cat [kubelet config 파일 경로]
clientCAFile : [CA 인증서 파일 경로]

■ kubelet config 파일에서 TLS 인증서와 Private key가 설정되어 있는지 확인

1) $ cat [kubelet config 파일 경로]
tlsCertFile : [인증서 파일 경로]
tlsPrivateKeyFile : [Private key 파일 경로]

■ kubelet config 파일에서 인증서 교환주기 설정이 되어 있는지 확인

1) $ cat [kubelet config 파일 경로]
tlsCertFile : [인증서 파일 경로]
tlsPrivateKeyFile : [Private key 파일 경로]

■ kubelet config 파일에서 TLS 통신에 사용되는 TLS 버전 및 cipher suites 확인

1) $ cat [kubelet config 파일 경로]
TLSCipherSuites :

■ kubelet service 파일에서 hostname이 변경되지 않도록 설정되어 있는지 확인

1) $ cat [kubelet service 파일 경로]를 확인하여 --hostname-override 설정이 존재하는지 확인(존재하지 않아야 함)

조치 방법

■ kubelet config 파일에서 클라이언트 CA 인증서 설정

1) $ cat [kubelet config 파일 경로]
clientCAFile : [CA 인증서 파일 경로]

```
address: 0.0.0.0
apiVersion: kubelet.config.k8s.io/v1beta1
authentication:
  anonymous:
    enabled: false
  webhook:
    cacheTTL: 2m0s
    enabled: true
  x509:
    clientCAFile: /etc/kubernetes/pki/ca.crt
authorization:
  mode: Webhook
  webhook:
```

■ kubelet config 파일에서 TLS 인증서와 Private key가 설정되어 있는지 확인

1) $ cat [kubelet config 파일 경로]
tlsCertFile : [인증서 파일 경로]
tlsPrivateKeyFile : [Private key 파일 경로]

```
kind: KubeletConfiguration
apiVersion: kubelet.config.k8s.io/v1beta1
authentication:
  anonymous:
    enabled: false
  webhook:
    enabled: true
  x509:
    clientCAFile: "/var/lib/kubernetes/ca.pem"
authorization:
  mode: Webhook
clusterDomain: "cluster.local"
clusterDNS:
  - "10.32.0.10"
podCIDR: "10.200.0.0/16"
resolvConf: "/run/systemd/resolve/resolv.conf"
runtimeRequestTimeout: "15m"
tlsCertFile: "/var/lib/kubelet/worker01.pem"
tlsPrivateKeyFile: "/var/lib/kubelet/worker01-key.pem"
```

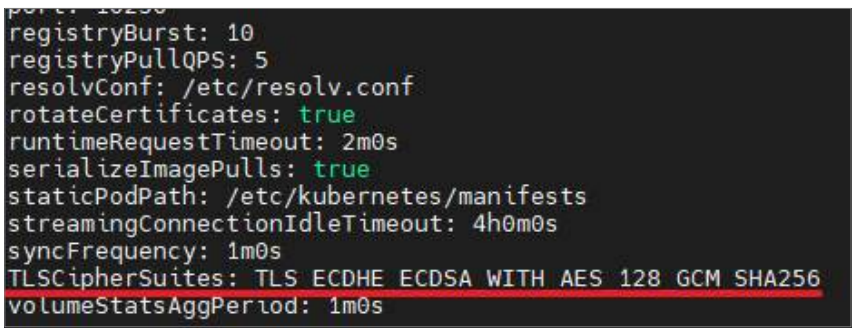
■ kubelet config 파일에서 인증서 교환주기 설정이 되어 있는지 확인

1) $ cat [kubelet config 파일 경로]
tlsCertFile : [인증서 파일 경로]
tlsPrivateKeyFile : [Private key 파일 경로]

```
protectKernelDefaults: true
podPidsLimit: -1
port: 10250
registryBurst: 10
registryPullQPS: 5
resolvConf: /etc/resolv.conf
rotateCertificates: true
runtimeRequestTimeout: 2m0s
serializeImagePulls: true
staticPodPath: /etc/kubernetes/manifests
streamingConnectionIdleTimeout: 4h0m0s
syncFrequency: 1m0s
```

■ kubelet config 파일에서 TLS 통신에 사용되는 TLS 버전 및 cipher suites 확인

1) $ cat [kubelet config 파일 경로]
TLSCipherSuites : TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305
TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
TLS_RSA_WITH_AES_256_GCM_SHA384
TLS_RSA_WITH_AES_128_GCM_SHA256



■ kubelet service 파일에서 hostname이 변경되지 않도록 설정되어 있는지 확인

1) $ cat [kubelet service 파일 경로]를 확인하여 --hostname-override 설정이 존재하는지 확인(존재하지 않아야 함)

Kernel 파라미터 설정

항목설명

OS kernel 매개 변수값과 kubelet에 설정된 기본 kernel 매개 변수값이 다를 경우 kubelet 기본 kernel 매개 변수값이 변경되어 원하지 않는 커널 기능이 존재하는 Pod가 실행될 수 있으므로 각각의 변수값이 다를 경우 kubelet 기본 kernel 매개 변수값이 변경되지 않도록 보호해야 한다.

진단 기준

양호

Kubelet Default Kernel 값을 보호하는 경우

취약

Kubelet Default Kernel 값을 보호하지 않는 경우

진단 방법

■ kubelet service 파일을 사용하는 경우

1) service 파일에 --protect-kernel-defaults 설정이 true로 되어 있는지 확인
$ cat [kubelet service 파일 경로] | grep "authorization-mode" | grep –v "#“

```
[root@k8s-node1 /]# cat /usr/lib/systemd/system/kubelet.service.d/10-kubeadm.conf | grep "authorizati
on-mode" | grep -v "#"
[root@k8s-node1 /]#
```

■ kubelet config 파일을 사용하는 경우

1) config 파일에 --protect-kernel-defaults 설정이 true로 되어 있는지 확인
$ cat [kubelet config 파일 경로]

조치 방법

■ kubelet service 파일을 사용하는 경우

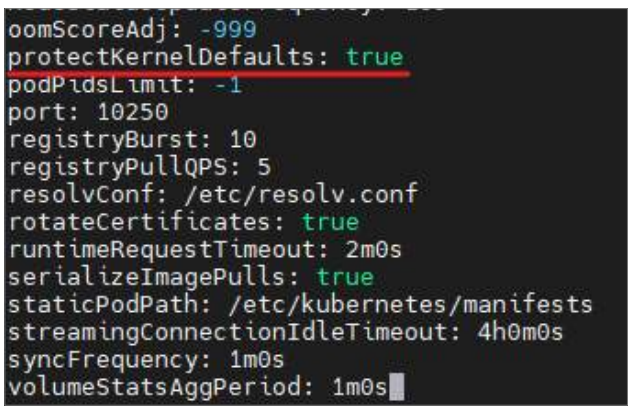
1) --protect-kernel-defaults 설정이 true로 설정
$ vi [kubelet service 파일 경로]
Environment="KUBELET_SYSTEM_PODS_ARGS=--protect-kernel-defaults=true" 설정 추가

```
# Note: This dropin only works with kubeadm and kubelet v1.11+
[Service]
Environment="KUBELET_KUBECONFIG_ARGS=--bootstrap-kubeconfig=/etc/kubernetes/bootstrap-kubelet.conf --kubeconfig=/etc/kubernetes/kubelet.conf"
Environment="KUBELET_CONFIG_ARGS=--config=/var/lib/kubelet/config.yaml"
Environment="KUBELET_SYSTEM_PODS_ARGS=--anonymous-auth=false --read-only-port=0 --protect-kernel-defaults=true"
Environment="KUBELET_AUTHZ_ARGS=--authorization-mode=Webhook"
# This is a file that "kubeadm init" and "kubeadm join" generates at runtime, populating the KUBELET_KUBEADM_ARGS variable dynamically
EnvironmentFile=-/var/lib/kubelet/kubeadm-flags.env
# This is a file that the user can use for overrides of the kubelet args as a last resort. Preferably, the user should use
# the .NodeRegistration.KubeletExtraArgs object in the configuration files instead. KUBELET_EXTRA_ARGS should be sourced from this file.
EnvironmentFile=-/etc/sysconfig/kubelet
ExecStart=
ExecStart=/usr/bin/kubelet $KUBELET_KUBECONFIG_ARGS $KUBELET_CONFIG_ARGS $KUBELET_KUBEADM_ARGS $KUBELET_EXTRA_ARGS
```

2) kubelet 서비스 재시작
$ systemctl daemon-reload
$ systemctl restart kubelet.service

■ Kubelet config 파일을 사용하는 경우

1) vi 명령어를 통해 protectKernelDefaults 설정을 true로 설정
$ vi [kubelet config 파일 경로]



2) kubelet 서비스 재시작
$ systemctl daemon-reload
$ systemctl restart kubelet.service

환경설정 파일 권한 설정

항목설명

Kubernetes 설정 파일에 비인가자의 접근이 가능한 경우 Kubernetes 설정을 변경하여 침해 사고를 일으킬 가능성이 있다. 따라서 root 외 다른 사용자가 이 파일을 수정할 수 없도록 파일의 권한을 제한해야 한다.

진단 기준

양호

환경설정 파일의 소유자 및 소유 그룹이 root이고, 접근 권한이 644 이하로 설정된 경우

취약

환경설정 파일의 소유자 및 소유 그룹이 root가 아니거나, 접근 권한이 644 초과로 설정된 경우

진단 방법

■ Kubernetes 설정 파일 권한이 안전하게 설정되어 있는지 확인

1) kubelet.conf 설정파일 권한 확인
$ stat -c %a:%U:%G /etc/kubernetes/kubelet.conf

```
[root@k8s-node1 kubelet]# stat -c %a:%U:%G /etc/kubernetes/kubelet.conf
600:root:root
```

■ 10-kubeadm.conf 설정파일 권한 확인

1) config 파일에 --protect-kernel-defaults 설정이 true로 되어 있는지 확인
$ stat -c %a:%U:%G /usr/lib/systemd/system/kubelet.service.d/10-kubeadm.conf

```
[root@k8s-node1 kubelet]# stat -c %a:%U:%G /usr/lib/systemd/system/kubelet.service.d/10-kubeadm.conf
644:root:root
```

■ config.yaml 설정파일 권한 확인

1) config 파일에 --protect-kernel-defaults 설정이 true로 되어 있는지 확인
$ stat -c %a:%U:%G /var/lib/kubelet/config.yaml

```
[root@k8s-node1 kubelet]# stat -c %a:%U:%G /var/lib/kubelet/config.yaml
644:root:root
```

조치 방법

■ 설정파일의 소유자 및 소유 그룹이 root가 아닌 경우 root로 조치

$ chown root:root [변경할 파일명]

■ 설정파일의 접근 권한이 644를 초과하는 경우 644 이하로 조치

$ chmod 644 [변경할 파일명]

인증서 파일 권한 설정

항목설명

SSL/TLS 통신 시 사용자 인증을 위해 사용되는 인증서가 root 외 다른 사용자가 인증서 파일에 접근할 수 없도록 인증서 파일의 권한을 제한하여 인증서가 변조되지 않도록 해야 한다.

진단 기준

양호

인증서 파일의 소유자 및 소유 그룹이 root이고, 접근 권한이 644 이하로 설정된 경우

취약

인증서 파일의 소유자 및 소유 그룹이 root가 아니거나, 접근 권한이 644 초과로 설정된 경우

진단 방법

■ 인증서 파일 권한과 소유자가 root로 되어 있는지 확인

$ ls –al [인증서를 생성한 위치]

```
[root@worker01 kubelet]# ls -al
합계 28
drwxr-xr-x   7 root root  214  5월  3 22:31 .
drwxr-xr-x. 28 root root 4096  5월  3 17:44 ..
-rw-------   1 root root   62  5월  3 17:44 cpu_manager_state
drwxr-xr-x   2 root root   45  5월  3 17:44 device-plugins
-rw-r--r--   1 root root 6384  5월  3 16:31 kubeconfig
-rw-r--r--   1 root root  493  5월  3 17:42 kubelet-config.yaml
drwxr-x---   2 root root    6  5월  3 17:44 plugins
drwxr-x---   2 root root    6  5월  3 17:44 plugins_registry
drwxr-x---   2 root root   26  5월  3 17:44 pod-resources
drwxr-x---   2 root root    6  5월  3 17:44 pods
-rw-r--r--   1 root root 1675  5월  3 15:14 worker01-key.pem
-rw-r--r--   1 root root 1493  5월  3 15:14 worker01.pem
[root@worker01 kubelet]#
[root@worker01 kubelet]# ls -al /var/lib/kubernetes
합계 8
drwxr-xr-x   2 root root   20  5월  3 17:41 .
drwxr-xr-x. 28 root root 4096  5월  3 17:44 ..
-rw-r--r--   1 root root 1318  5월  3 15:14 ca.pem
```

조치 방법

■ 인증서 파일 권한과 소유자가 root로 되어 있는지 확인

$ chown root:root [변경할 파일명]

■ 인증서 파일의 접근 권한이 644를 초과하는 경우 644 이하로 조치

$ chmod 644 [변경할 파일명]

최신 보안 패치 적용

항목설명

버그 또는 보안 취약점으로 인한 침해 사고가 발생할 수 있다. 따라서 주기적으로 최신 패치를 적용하여 취약점을 제거해야 한다.

진단 기준

양호

최신 보안 패치가 적용된 경우

취약

최신 보안 패치가 적용되지 않은 경우

진단 방법

■ 현재 사용 중인 버전 확인

$ kubectl version

```
test@k8s-master:~$ kubectl version
Client Version: v1.28.1
Kustomize Version: v5.0.4-0.20230601165947-6ce0bf390ce3
Server Version: v1.28.1
test@k8s-master:~$
```

조치 방법

■ 최신 보안 패치 확인 후 업데이트 및 패치 수행

※ 최신 버전을 사용하도록 권고하고 있으나 시스템 운영상 적용이 어려운 경우 최신이 아닌 취약점이 존재하지 않는 버전도 허용하고 있음

비고

※ 보안 패치를 적용할 경우, 시스템 영향도를 파악하여 충분한 테스트 후 적용 권고

2.29.

OpenStack

2.29. OpenStack

파일 권한 관리(14개 항목), 암호화(15개 항목), 보안 설정(18개 항목) 총 3개 영역에서 47개 항목으로 구성된다.

[표 29] OpenStack 진단 체크리스트

구분	진단 항목
가. 파일 권한 관리	Identity 설정파일 소유권 설정
	Identity 설정파일 접근권한 설정
	Dashboard 설정파일 소유권 설정
	Dashboard 설정파일 접근권한 설정
	Compute 설정파일 소유권 설정
	Compute 설정파일 접근권한 설정
	블록 스토리지 서비스 설정파일 소유권 설정
	블록 스토리지 서비스 설정파일 접근권한 설정
	이미지 스토리지 설정파일 소유권 설정
	이미지 스토리지 설정파일 접근권한 설정
	공유파일 시스템 설정파일 소유권 설정
	공유파일 시스템 설정파일 접근권한 설정
	네트워킹 서비스 설정파일 소유권 설정
	네트워킹 서비스 설정파일 접근권한 설정
나. 암호화	Identity TLS 활성화
	PKI토큰의 강력한 해시 알고리즘 사용
	Dashboard의 SECURE_PROXY_SSL_HEADER 설정
	Compute 인증을 위한 보안프로토콜 사용
	Nova와 Glance의 안전한 통신
	블록 스토리지 서비스 인증을 위한 TLS 활성화
	cinder와 nova의 TLS 통신
	cinder와 glance의 TLS 통신
	이미지 스토리지 서비스 인증을 위한 TLS 활성화
	공유 파일 시스템 인증을 위한 TLS 활성화
	TLS를 이용한 공유 파일 시스템과 Compute의 통신
	TLS를 이용한 공유 파일 시스템과 네트워킹과의 연결
	TLS를 이용한 공유 파일 시스템과 블록 스토리지 서비스와의 연결
	네트워킹 서비스의 인증을 위한 안전한 프로토콜 사용
	Neutron API 서버의 TLS 활성화

구분	진단 항목
다. 보안 설정	Identity 서비스 max_request_body_size 설정
	admin 토큰 비활성화
	Dashboard의 DISALLOW_IFRAME_EMBED 설정
	Dashboard의 CSRF_COOKIE_SECURE 설정
	Dashboard의 SESSION_COOKIE_SECURE 설정
	Dashboard의 SESSION_COOKIE_HTTPONLY 설정
	Dashboard의 PASSWORD_AUTOCOMPLETE 설정
	Dashboard의 DISABLE_PASSWORD_REVEAL 설정
	Dashboard의 ENFORCE_PASSWORD_CHECK 설정
	Dashboard의 PASSWORD_VALIDATOR 설정
	Compute의 인증을 위한 keystone 사용
	블록 스토리지 서비스의 인증을 위한 keystone 사용
	안전한 환경에서의 NAS 운영
	블록 스토리지 서비스에서 요청 본문 최대 크기 설정
	블록 스토리지 볼륨 암호화
	이미지 스토리지 서비스 인증을 위한 keystone 설정
	공유파일 시스템 인증을 위한 오픈스택 Identity 사용
	공유파일 시스템에서 요청 본문 최대 사이즈 설정

Identity 설정파일 소유권 설정

항목설명

설정 파일들에는 구성 요소의 원활한 기능을 수행하는데 필요한 중요한 매개변수와 정보가 들어있다. 권한이 없는 사용자가 의도적으로 또는 실수로 매개변수나 파일 자체를 수정하거나 삭제하면 심각한 가용성 문제로 인해 다른 사용자에게 서비스가 거부 될 수 있다. 따라서 중요한 설정 파일들의 소유자 및 소유그룹은 해당 구성요소 소유자로 설정해야 한다.

진단 기준

양호

Identity 설정 파일의 소유자 및 소유그룹이 keystone으로 설정되어 있는 경우

취약

Identity 설정 파일의 소유자 및 소유그룹이 keystone이 아닌 다른 소유자 또는 소유그룹으로 설정되어 있는 경우

진단 방법

■ Identity 설정파일의 소유자 소유그룹이 keystone/keystone로 출력되는지 확인

```
# ll /etc/keystone/keystone.conf
# ll /etc/keystone/keystone-paste.ini
# ll /etc/keystone/policy.json
# ll /etc/keystone/logging.conf
# ll /etc/keystone/ssl/certs/signing_cert.pem
# ll /etc/keystone/ssl/private/signing_key.pem
# ll /etc/keystone/ssl/certs/ca.pem
```

ex)

```
# ll /etc/keystone/keystone.conf
```

```
[root@localhost ~]# ll /etc/keystone/keystone.conf
-rw-r-----. 1 root keystone 119838 Oct  5 00:18 /etc/keystone/keystone
.conf
```

조치 방법

■ Identity 설정파일의 소유자 소유그룹을 keystone/keystone로 변경

```
# chown keystone:keystone /etc/keystone/keystone.conf
# chown keystone:keystone /etc/keystone/keystone-paste.ini
# chown keystone:keystone /etc/keystone/policy.json
# chown keystone:keystone /etc/keystone/logging.conf
# chown keystone:keystone /etc/keystone/ssl/certs/signing_cert.pem
# chown keystone:keystone /etc/keystone/ssl/private/signing_key.pem
# chown keystone:keystone /etc/keystone/ssl/certs/ca.pem
```

ex)

```
# chown keystone:keystone /etc/keystone/keystone.conf
```

```
[root@localhost ~]# chown keystone:keystone /etc/keystone/keystone.con
f
[root@localhost ~]# ll /etc/keystone/keystone.conf
-rw-r-----. 1 keystone keystone 119838 Oct  5 00:18 /etc/keystone/keys
tone.conf
```

Identity 설정파일 접근권한 설정

항목설명

설정 파일들에는 구성 요소의 원활한 기능을 수행하는데 필요한 중요한 매개변수와 정보가 들어있다. 권한이 없는 사용자가 의도적으로 또는 실수로 매개변수나 파일 자체를 수정하거나 삭제하면 심각한 가용성 문제로 인해 다른 사용자에게 서비스가 거부 될 수 있다. 따라서 설정 파일들에 엄격한 접근권한을 설정해야 한다.

진단 기준

양호

Identity 설정 파일의 퍼미션이 640 또는 그보다 엄격하게 설정되어 있는 경우

취약

Identity 설정 파일의 퍼미션이 최소 640으로 설정되어 있지 않은 경우

진단 방법

■ Identity 설정파일의 퍼미션을 확인

```
# ll /etc/keystone/keystone.conf
# ll /etc/keystone/keystone-paste.ini
# ll /etc/keystone/policy.json
# ll /etc/keystone/logging.conf
# ll /etc/keystone/ssl/certs/signing_cert.pem
# ll /etc/keystone/ssl/private/signing_key.pem
# ll /etc/keystone/ssl/certs/ca.pem
```

ex)

```
# ll /etc/keystone/keystone.conf
```

```
[root@localhost ~]# ll /etc/keystone/keystone.conf
-rw-r-----. 1 keystone keystone 119838 Oct  5 00:18 /etc/keystone/keys
tone.conf
```

조치 방법

■ Identity 설정파일의 퍼미션을 최소 640으로 설정

```
# chmod 640 /etc/keystone/keystone.conf
# chmod 640 /etc/keystone/keystone-paste.ini
# chmod 640 /etc/keystone/policy.json
# chmod 640 /etc/keystone/logging.conf
# chmod 640 /etc/keystone/ssl/certs/signing_cert.pem
# chmod 640 /etc/keystone/ssl/private/signing_key.pem
# chmod 640 /etc/keystone/ssl/certs/ca.pem
```

ex)

```
# chmod 640 /etc/keystone/keystone.conf
```

```
[root@localhost ~]# chmod 640 /etc/keystone/keystone.conf
[root@localhost ~]# ll /etc/keystone/keystone.conf
-rw-r-----. 1 keystone keystone 119838 Oct  5 00:18 /etc/keystone/keys
tone.conf
```

Dashboard 설정파일 소유권 설정

항목설명

설정 파일들에는 구성 요소의 기능을 수행하는데 중요한 매개변수와 정보가 들어있다. 권한이 없는 사용자가 의도적으로 또는 실수로 매개변수나 파일 자체를 수정하거나 삭제하면 심각한 가용성 문제로 인해 다른 사용자에게 서비스가 거부될 수 있다. 따라서 중요한 설정 파일들의 소유자/소유그룹은 root/horizon으로 설정해야 한다.

진단 기준

양호

Dashboard 설정 파일의 소유자 및 소유그룹이 root/horizon으로 되어있는 경우

취약

Dashboard 설정 파일의 소유자 및 소유그룹이 root/horizon으로 되어있지 않은 경우

진단 방법

■ Dashboard 설정파일의 소유자 소유그룹이 root/horizon으로 출력되는지 확인

ll /etc/openstack-dashboard/local_settings.py

또는

ll /etc/openstack-dashboard/local_settings

```
[root@localhost ~]# ll /etc/openstack-dashboard/local_settings
-rw-r-----. 1 root apache 34212 Oct  5 08:34 /etc/openstack-dashboard/
local_settings
```

조치 방법

■ Dashboard 설정파일의 소유자 소유그룹을 root/horizon로 변경

chown root:horizon /etc/openstack-dashboard/local_settings.py

또는

chown root:horizon /etc/openstack-dashboard/local_settings

```
[root@localhost ~]# chown root:horizon /etc/openstack-dashboard/local_
settings
[root@localhost ~]# ll /etc/openstack-dashboard/local_settings
-rw-r-----. 1 root horizon 34212 Oct  5 08:34 /etc/openstack-dashboard
/local_settings
```

Dashboard 설정파일 접근권한 설정

항목설명

설정 파일들에는 구성 요소의 기능을 수행하는데 중요한 매개변수와 정보가 들어있다. 권한이 없는 사용자가 의도적으로 또는 실수로 매개변수나 파일 자체를 수정하거나 삭제하면 심각한 가용성 문제로 인해 다른 사용자에게 서비스가 거부 될 수 있다. 따라서 중요한 설정 파일의 접근권한을 엄격하게 설정해야 한다.

진단 기준

양호

Dashboard 설정파일의 퍼미션이 640 또는 그보다 엄격하게 적용되어 있는 경우

취약

Dashboard 설정 파일의 퍼미션이 최소 640으로 적용되어 있지 않은 경우

진단 방법

■ Dashboard 설정파일 퍼미션을 확인

ll /etc/openstack-dashboard/local_settings.py

또는
ll /etc/openstack-dashboard/local_settings

```
[root@localhost ~]# ll /etc/openstack-dashboard/local_settings
-rw-r-----. 1 root apache 34212 Oct  5 08:34 /etc/openstack-dashboard/
local_settings
```

조치 방법

■ 설정파일의 퍼미션을 640으로 설정

chmod 640 /etc/openstack-dashboard/local_settings.py

또는
chmod 640 /etc/openstack-dashboard/local_settings

```
[root@localhost ~]# chmod 640 /etc/openstack-dashboard/local_settings
[root@localhost ~]# ll /etc/openstack-dashboard/local_settings
-rw-r-----. 1 root horizon 34212 Oct  5 08:34 /etc/openstack-dashboard
/local_settings
```

Compute 설정파일 소유권 설정

항목설명

설정 파일들에는 구성 요소의 기능을 수행하는데 중요한 매개변수와 정보가 들어있다. 의도적으로 또는 실수로 권한이 없는 사용자가 매개변수나 파일 자체를 수정하거나 삭제하면 심각한 서비스 거부가 발생할 수 있다. 따라서 중요한 설정 파일들의 소유자/소유그룹은 root/nova로 설정해야 한다.

진단 기준

양호

Compute 설정 파일의 소유자 및 소유그룹이 root/nova로 되어 있는 경우

취약

Compute 설정 파일의 소유자 및 소유그룹이 root/nova로 되어있지 않은 경우

진단 방법

■ Compute 설정파일의 소유자 소유그룹이 root/nova으로 출력되는지 확인

```
# ll /etc/nova/nova.conf
# ll /etc/nova/api-paste.ini
# ll /etc/nova/policy.json
# ll /etc/nova/rootwrap.conf
```

ex)

```
# ll /etc/nova/nova.conf
```

```
[root@localhost ~]# ll /etc/nova/nova.conf
-rw-r-----. 1 root nova 391964 Oct  5 01:23 /etc/nova/nova.conf
```

조치 방법

■ Compute 설정파일의 소유자 소유그룹을 root/nova로 변경

```
# chown root:nova /etc/nova/nova.conf
# chown root:nova /etc/openstack-dashboard/local_settings
# chown root:nova /etc/nova/policy.json
# chown root:nova /etc/nova/rootwrap.conf
```

ex)

```
# chown root:nova /etc/nova/nova.conf
```

```
[root@localhost ~]# chown root:nova /etc/nova/nova.conf
[root@localhost ~]# ll /etc/nova/nova.conf
-rw-r-----. 1 root nova 391964 Oct  5 01:23 /etc/nova/nova.conf
```

Compute 설정파일 접근권한 설정

항목설명

설정 파일들에는 구성 요소의 기능을 수행하는데 중요한 매개변수와 정보가 들어있다. 의도적으로 또는 실수로 권한이 없는 사용자가 매개변수 또는 파일 자체를 수정하거나 삭제하면 심각한 서비스 거부가 발생할 수 있다. 따라서 중요한 설정 파일의 접근권한을 엄격하게 설정해야 한다.

진단 기준

양호

Compute 설정 파일의 접근권한이 640이거나 그보다 엄격한 경우

취약

Compute 설정 파일의 접근권한이 최소 640으로 되어있지 않은 경우

진단 방법

■ Compute 설정파일의 소유자 소유그룹이 root/nova으로 출력되는지 확인

```
# ll /etc/nova/nova.conf
# ll /etc/nova/api-paste.ini
# ll /etc/nova/policy.json
# ll /etc/nova/rootwrap.conf
```

ex)

```
# ll /etc/nova/nova.conf
```

```
[root@localhost ~]# ll /etc/nova/nova.conf
-rw-r-----. 1 root nova 391964 Oct  5 01:23 /etc/nova/nova.conf
```

조치 방법

■ Compute 설정파일의 퍼미션을 640으로 설정

```
# chmod 640 /etc/nova/nova.conf
# chmod 640 /etc/openstack-dashboard/local_settings
# chmod 640 /etc/nova/policy.json
# chmod 640 /etc/nova/rootwrap.conf
```

ex)

```
# chmod 640 /etc/nova/nova.conf
```

```
[root@localhost ~]# chmod 640 /etc/nova/nova.conf
[root@localhost ~]# ll /etc/nova/nova.conf
-rw-r-----. 1 root nova 391964 Oct  5 01:23 /etc/nova/nova.conf
```

블록 스토리지 서비스 설정파일 소유권 설정

항목설명

설정 파일들에는 구성 요소의 기능을 수행하는데 중요한 매개변수와 정보가 들어있다. 만약에 권한이 없는 사용자가 의도적으로 또는 실수로 매개변수나 파일 자체를 수정하거나 삭제하면 심각한 가용성 문제가 발생한다. 따라서 중요한 설정 파일들의 소유자/소유그룹은 root/cinder로 설정해야 한다.

진단 기준

양호

블록 스토리지 서비스 설정 파일의 소유자 및 소유그룹이 root/cinder로 되어 있는 경우

취약

블록 스토리지 서비스 설정 파일의 소유자 및 소유그룹이 root/cinder로 되어있지 않은 경우

진단 방법

■ 블록 스토리지 서비스 설정파일의 소유자 소유그룹이 root/cinder로 출력되는지 확인

```
# ll /etc/cinder/cinder.conf
# ll /etc/cinder/api-paste.ini
# ll /etc/cinder/policy.json
# ll /etc/cinder/rootwrap.conf
```

ex)

```
# ll /etc/cinder/cinder.conf
```

```
[root@localhost ~]# ll /etc/cinder/cinder.conf
-rw-r-----. 1 root cinder 186162 Oct  5 08:55 /etc/cinder/cinder.conf
```

조치 방법

■ 블록 스토리지 서비스 설정파일의 소유자 소유그룹을 root/cinder로 변경

```
# chown root:cinder /etc/cinder/cinder.conf
# chown root:cinder /etc/cinder/api-paste.ini
# chown root:cinder /etc/cinder/policy.json
# chown root:cinder /etc/cinder/rootwrap.conf
```

ex)

```
# chown root:cinder /etc/cinder/cinder.conf
```

```
[root@localhost ~]# chown root:cinder /etc/cinder/cinder.conf
[root@localhost ~]# ll /etc/cinder/cinder.conf
-rw-r-----. 1 root cinder 186162 Oct  5 08:55 /etc/cinder/cinder.conf
```

블록 스토리지 서비스 설정파일 접근권한 설정

항목설명

설정 파일들에는 구성 요소의 기능을 수행하는데 중요한 매개변수와 정보가 들어있다. 만약에 권한이 없는 사용자가 의도적으로 또는 실수로 매개변수나 파일을 수정하거나 삭제하면 심각한 가용성 문제가 발생한다. 따라서 중요한 설정 파일은 엄격한 접근권한을 설정해야 한다.

진단 기준

양호

블록 스토리지 서비스 설정파일의 퍼미션이 640이거나 그보다 엄격한 경우

취약

블록 스토리지 서비스 설정파일의 퍼미션이 최소 640으로 되어 있지 않은 경우

진단 방법

■ 블록 스토리지 서비스 설정파일의 퍼미션을 확인

```
# ll /etc/cinder/cinder.conf
# ll /etc/cinder/api-paste.ini
# ll /etc/cinder/policy.json
# ll /etc/cinder/rootwrap.conf
```

ex)

```
# ll /etc/cinder/cinder.conf
```

```
[root@localhost ~]# ll /etc/cinder/cinder.conf
-rw-r-----. 1 root cinder 186162 Oct  5 08:55 /etc/cinder/cinder.conf
```

조치 방법

■ 블록 스토리지 서비스 설정파일의 퍼미션을 640으로 설정

```
# chmod 640 /etc/cinder/cinder.conf
# chmod 640 /etc/cinder/api-paste.ini
# chmod 640 /etc/cinder/policy.json
# chmod 640 /etc/cinder/rootwrap.conf
```

ex)

```
# chmod 640 /etc/cinder/cinder.conf
```

```
[root@localhost ~]# chmod 640 /etc/cinder/cinder.conf
[root@localhost ~]# ll /etc/cinder/cinder.conf
-rw-r-----. 1 root cinder 186162 Oct  5 08:55 /etc/cinder/cinder.conf
```

이미지 스토리지 설정파일 소유권 설정

항목설명

설정 파일들에는 구성 요소의 기능을 수행하는데 중요한 매개변수와 정보가 들어있다. 권한이 없는 사용자가 의도적으로 또는 실수로 매개변수나 파일 자체를 수정하거나 삭제하면 심각한 가용성 문제로 인해 다른 사용자에게 서비스가 거부 될 수 있다. 따라서 중요한 설정 파일들의 소유자 및 소유그룹은 root/glance로 설정해야 한다.

진단 기준

양호

이미지 스토리지 설정 파일의 소유자 및 소유그룹이 root/glance로 되어 있는 경우

취약

이미지 스토리지 설정 파일의 소유자 및 소유그룹이 root/glance로 되어있지 않은 경우

진단 방법

■ 이미지 스토리지 설정파일의 소유자 소유그룹이 root/glance로 출력되는지 확인

```
# ll /etc/glance/glance-api-paste.ini
# ll /etc/glance/glance-api.conf
# ll /etc/glance/glance-cache.conf
# ll /etc/glance/glance-manage.conf
# ll /etc/glance/glance-registry-paste.ini
# ll /etc/glance/glance-registry.conf
# ll /etc/glance/glance-scrubber.conf
# ll /etc/glance/glance-swift-store.conf
# ll /etc/glance/policy.json
# ll /etc/glance/schema-image.json
# ll /etc/glance/schema.json
```

ex)

```
# ll /etc/glance/glance-api.conf
```

```
[root@localhost ~]# ll /etc/glance/glance-api.conf
-rw-r-----. 1 root glance 160579 Oct  5 00:59 /etc/glance/glance-api.c
onf
```

조치 방법

■ 이미지 스토리지 설정파일의 소유자 소유그룹을 root/glance로 변경

```
# chown root:glance /etc/glance/glance-api-paste.ini
# chown root:glance /etc/glance/glance-api.conf
# chown rootglance /etc/glance/glance-cache.conf
# chown root:glacne /etc/glance/glance-manage.conf
# chown root:glacne /etc/glance/glance-registry-paste.ini
# chown root:glacne /etc/glance/glance-registry.conf
# chown root:glacne /etc/glance/glance-scrubber.conf
# chown root:glacne /etc/glance/glance-swift-store.conf
# chown root:glacne /etc/glance/policy.json
# chown root:glacne /etc/glance/schema-image.json
# chown root:glacne /etc/glance/schema.json
```

ex)

```
# chown root:glance /etc/glance/glance-api.conf
```

```
[root@localhost ~]# chown root:glance /etc/glance/glance-api.conf
[root@localhost ~]# ll /etc/glance/glance-api.conf
-rw-r-----. 1 root glance 160579 Oct  5 00:59 /etc/glance/glance-api.c
onf
```

이미지 스토리지 설정파일 접근권한 설정

항목설명

설정 파일들에는 구성 요소의 기능을 수행하는데 중요한 매개변수와 정보가 들어있다. 권한이 없는 사용자가 의도적으로 또는 실수로 매개변수나 파일 자체를 수정하거나 삭제하면 심각한 가용성 문제로 인해 다른 사용자에게 서비스가 거부 될 수 있다. 따라서 중요한 설정 파일의 접근권한은 엄격하게 설정해야 한다.

진단 기준

양호

이미지 스토리지 설정 파일의 퍼미션이 640 또는 그보다 엄격한 경우

취약

이미지 스토리지 설정 파일의 퍼미션이 최소 640으로 되어 있지 않은 경우

진단 방법

■ 이미지 스토리지 설정파일의 퍼미션이 640이하로 되어있는지 확인

```
# ll /etc/glance/glance-api-paste.ini
# ll /etc/glance/glance-api.conf
# ll /etc/glance/glance-cache.conf
# ll /etc/glance/glance-manage.conf
# ll /etc/glance/glance-registry-paste.ini
# ll /etc/glance/glance-registry.conf
# ll /etc/glance/glance-scrubber.conf
# ll /etc/glance/glance-swift-store.conf
# ll /etc/glance/policy.json
# ll /etc/glance/schema-image.json
# ll /etc/glance/schema.json
```

ex)

```
# ll /etc/glance/glance-api.conf
```

```
[root@localhost ~]# ll /etc/glance/glance-api.conf
-rw-r-----. 1 root glance 160579 Oct  5 00:59 /etc/glance/glance-api.c
onf
```

조치 방법

■ 이미지 스토리지 설정파일의 퍼미션을 640으로 설정

```
# chmod 640 /etc/glance/glance-api-paste.ini
# chmod 640 /etc/glance/glance-api.conf
# chmod 640 /etc/glance/glance-cache.conf
# chmod 640 /etc/glance/glance-manage.conf
# chmod 640 /etc/glance/glance-registry-paste.ini
# chmod 640 /etc/glance/glance-registry.conf
# chmod 640 /etc/glance/glance-scrubber.conf
# chmod 640 /etc/glance/glance-swift-store.conf
# chmod 640 /etc/glance/policy.json
# chmod 640 /etc/glance/schema-image.json
# chmod 640 /etc/glance/schema.json
```

ex)

```
# chmod 640 /etc/glance/glance-api.conf
```

```
[root@localhost ~]# chmod 640 /etc/glance/glance-api.conf
[root@localhost ~]# ll /etc/glance/glance-api.conf
-rw-r-----. 1 root glance 160579 Oct  5 00:59 /etc/glance/glance-api.c
onf
```

공유파일 시스템 설정파일 소유권 설정

항목설명

설정 파일들에는 구성 요소의 기능을 수행하는데 중요한 매개변수와 정보가 들어있다. 권한이 없는 사용자가 의도적으로 또는 실수로 매개변수나 파일 자체를 수정하거나 삭제하면 심각한 가용성 문제로 인해 다른 사용자에게 서비스가 거부 될 수 있다. 따라서 중요한 설정 파일들의 소유자 및 소유그룹은 root/manila로 설정해야 한다.

진단 기준

양호

공유파일 시스템 설정 파일의 소유자 및 소유그룹이 root/manila로 되어있는 경우

취약

공유파일 시스템 설정 파일의 소유자 및 소유그룹이 root/manila로 되어있지 않은 경우

진단 방법

■ 공유파일 시스템 설정파일의 소유자 소유그룹이 root/manila로 출력되는지 확인

```
# ll /etc/manila/manila.conf
# ll /etc/manila/api-paste.ini
# ll /etc/manila/policy.json
# ll /etc/manila/rootwrap.conf
```

ex)

```
# ll /etc/manila/manila.conf
```

```
[root@localhost ~]# ll /etc/manila/manila.conf
-rw-r-----. 1 root manila 120145 Oct  6 00:16 /etc/manila/manila.conf
```

조치 방법

■ 공유파일 시스템 설정파일의 소유자 소유그룹을 root/manila로 변경

```
# chown root:manila /etc/manila/manila.conf
# chown root:manila /etc/manila/api-paste.ini
# chown root:manila /etc/manila/policy.json
# chown root:manila /etc/manila/rootwrap.conf
```

ex)

```
# chown root:manila /etc/manila/manila.conf
```

```
[root@localhost ~]# chown root:manila /etc/manila/manila.conf
[root@localhost ~]# ll /etc/manila/manila.conf
-rw-r-----. 1 root manila 120145 Oct  6 00:16 /etc/manila/manila.conf
```

공유파일 시스템 설정파일 접근권한 설정

항목설명

설정 파일들에는 구성 요소의 기능을 수행하는데 중요한 매개변수와 정보가 들어있다. 권한이 없는 사용자가 의도적으로 또는 실수로 매개변수나 파일 자체를 수정하거나 삭제하면 심각한 가용성 문제로 인해 다른 사용자에게 서비스가 거부 될 수 있다. 따라서 중요한 설정 파일들의 접근권한을 엄격하게 설정해야 한다.

진단 기준

양호

공유파일 시스템 설정 파일의 퍼미션이 640 또는 그보다 엄격한 경우

취약

공유파일 시스템 설정 파일의 640으로 되어 있지 않은 경우

진단 방법

■ 공유파일 시스템 설정파일의 퍼미션이 640이하로 되어있는지 확인

```
# ll /etc/manila/manila.conf
# ll /etc/manila/api-paste.ini
# ll /etc/manila/policy.json
# ll /etc/manila/rootwrap.conf
```

ex)

```
# ll /etc/manila/manila.conf
```

```
[root@localhost ~]# ll /etc/manila/manila.conf
-rw-r-----. 1 root manila 120145 Oct  6 00:16 /etc/manila/manila.conf
```

조치 방법

■ 공유파일 시스템 설정파일의 퍼미션을 640으로 설정

```
# chmod 640 /etc/manila/manila.conf
# chmod 640 /etc/manila/api-paste.ini
# chmod 640 /etc/manila/policy.json
# chmod 640 /etc/manila/rootwrap.conf
```

ex)

```
# chmod 640 /etc/manila/manila.conf
```

```
[root@localhost ~]# chmod 640 /etc/manila/manila.conf
[root@localhost ~]# ll /etc/manila/manila.conf
-rw-r-----. 1 root manila 120145 Oct  6 00:16 /etc/manila/manila.conf
```

네트워킹 서비스 설정파일 소유권 설정

항목설명

설정 파일들에는 구성 요소의 기능을 수행하는데 중요한 매개변수와 정보가 들어있다. 권한이 없는 사용자가 의도적으로 또는 실수로 매개변수나 파일 자체를 수정하거나 삭제하면 심각한 가용성 문제로 인해 다른 사용자에게 서비스가 거부 될 수 있다. 따라서 중요한 설정 파일들의 소유자/소유그룹은 root/neutron으로 설정하고 엄격한 접근권한을 설정하여야 한다.

진단 기준

양호

네트워킹 서비스 설정 파일의 소유자 및 소유그룹이 root/neutron으로 되어있는 경우

취약

네트워킹 서비스 설정 파일의 소유자 및 소유그룹이 root/neutron으로 되어있지 않은 경우

진단 방법

■ 네트워킹 서비스 설정파일의 소유자/소유그룹이 root/neutron로 출력되는지 확인

```
# ll /etc/neutron/neutron.conf
# ll /etc/neutron/api-paste.ini
# ll /etc/neutron/policy.json
# ll /etc/neutron/rootwrap.conf
```

ex)

```
# ll /etc/neutron/neutron.conf
```

```
[root@localhost ~]# ll /etc/neutron/neutron.conf
-rw-r-----. 1 root neutron 72034 Oct  5 08:15 /etc/neutron/neutron.con
f
```

조치 방법

■ 네트워킹 서비스 설정파일의 소유자/소유그룹을 root/neutron로 변경

```
# chown root:neutron /etc/neutron/neutron.conf
# chown root:neutron /etc/neutron/api-paste.ini
# chown root:neutron /etc/neutron/policy.json
# chown root:neutron /etc/neutron/rootwrap.conf
```

ex)

```
# chown root:neutron /etc/neutron/neutron.conf
```

```
[root@localhost ~]# chown root:neutron /etc/neutron/neutron.conf
[root@localhost ~]# ll /etc/neutron/neutron.conf
-rw-r-----. 1 root neutron 72034 Oct  5 08:15 /etc/neutron/neutron.con
f
```

네트워킹 서비스 설정파일 접근권한 설정

항목설명

설정 파일들에는 구성 요소의 기능을 수행하는데 중요한 매개변수와 정보가 들어있다. 권한이 없는 사용자가 의도적으로 또는 실수로 매개변수나 파일 자체를 수정하거나 삭제하면 심각한 가용성 문제로 인해 다른 사용자에게 서비스가 거부 될 수 있다. 따라서 중요한 설정 파일들에 엄격한 접근권한을 설정해야 한다.

진단 기준

양호

네트워킹 서비스 설정 파일의 퍼미션이 또는 그보다 엄격한 경우

취약

네트워킹 서비스 설정 파일의 퍼미션이 640 최소 640으로 되어 있지 않은 경우

진단 방법

■ 네트워킹 서비스 설정파일의 퍼미션이 640 이하로 되어있는지 확인

```
# ll /etc/neutron/neutron.conf
# ll /etc/neutron/api-paste.ini
# ll /etc/neutron/policy.json
# ll /etc/neutron/rootwrap.conf
```

ex)

```
# ll /etc/neutron/neutron.conf
```

```
[root@localhost ~]# ll /etc/neutron/neutron.conf
-rw-r-----. 1 root neutron 72034 Oct  5 08:15 /etc/neutron/neutron.con
f
```

조치 방법

■ 네트워킹 서비스 설정파일의 퍼미션을 640으로 설정

```
# chmod 640 /etc/neutron/neutron.conf
# chmod 640 /etc/neutron/api-paste.ini
# chmod 640 /etc/neutron/policy.json
# chmod 640 /etc/neutron/rootwrap.conf
```

ex)

```
# chmod 640 /etc/neutron/neutron.conf
```

```
[root@localhost ~]# chmod 640 /etc/neutron/neutron.conf
[root@localhost ~]# ll /etc/neutron/neutron.conf
-rw-r-----. 1 root neutron 72034 Oct  5 08:15 /etc/neutron/neutron.con
f
```

Identity TLS 활성화

항목설명

오픈스택 구성요소는 다양한 프로토콜을 사용하여 서로 통신하며 통신에는 민감한 기밀데이터가 포함되어 있을 수 있다. 공격자는 중요한 정보에 접근하기 위해 채널을 도청하려고 시도할 수 있다. 따라서 모든 구성요소는 HTTPS와 같은 보안 통신 프로토콜을 사용하여 통신해야 한다.

진단 기준

양호

HTTP서버에 TLS가 활성화되어 있는 경우

취약

HTTP서버에 TLS가 활성화되어 있지 않은 경우

진단 방법

■ TLS 서비스 포트가 오픈되어 있는지 확인

netstat –tnlp | grep –i httpd | grep 443

```
[root@localhost ~]# netstat -tnlp | grep -i httpd | grep 443
[root@localhost ~]#
```

조치 방법

■ TLS 서비스 활성화

SSL 설정을 활성화한 뒤, TLS 프로토콜을 활성화

PKI토큰의 강력한 해시 알고리즘 사용

항목설명

MD5는 취약하고 가치가 떨어지는 해시 알고리즘으로 무차별 대입 공격으로 크랙될 수 있다. 아이덴티티 토큰은 민감하므로 비인가 노출 및 접근을 방지하기 위해 강력한 해시 알고리즘으로 보호해야 한다.

진단 기준

양호

/etc/keystone/keystone.conf 파일에서 [token] 섹션의 hash_algorithm 매개변수가 SHA256으로 설정되어 있는 경우

취약

/etc/keystone/keystone.conf 파일에서 [token] 섹션의 hash_algorithm 매개변수가 SHA256 보다 약한 알고리즘으로 설정되어 있는 경우

진단 방법

■ /etc/keystone/keystone.conf 파일에서 hash_algorithm 설정 값 확인

cat /etc/keystone/keystone.conf | grep –i “hash_algorithm = sha256”

```
[root@localhost ~]# cat /etc/keystone/keystone.conf | grep -i "hash_al
gorithm = sha 256"
hash_algorithm = sha 256
```

조치 방법

■ /etc/keystone/keystone.conf 파일에서 hash_algorithm 값을 sha256으로 설정

vi /etc/keystone/keystone.conf
[token]
…
hash_algorithm = sha256

```
[token]

hash_algorithm = sha 256
#
# From keystone
```

※ [default]로는 hash_algorithm = md5로 되어있음

Dashboard의 SECURE_PROXY_SSL_HEADER 설정

항목설명

오픈스택 대시보드가 프록시 뒤에 위치하고 프록시가 들어오는 모든 요청에 대해 X-Forwarded-Proto 헤더를 제거하거나 X-Forwarded-Proto를 설정하고 대시보드에 보내지만 HTTPS를 이용하는 경우에는 SECURE_PROXY_SSL_HEADER를 설정하여야 한다.

진단 기준

양호

/etc/openstack-dashboard/local_settings.py 또는 /etc/openstack-dashboard/local_settings 파일에서 SECURE_PROXY_SSL_HEADER 매개변수가 ('HTTP_X_FORWARDED_PROTO', 'https')로 설정되어 있는 경우

취약

/etc/openstack-dashboard/local_settings.py 또는 /etc/openstack-dashboard/local_settings 파일에서 SECURE_PROXY_SSL_HEADER 매개변수가 ('HTTP_X_FORWARDED_PROTO', 'https')로 설정되어 있지 않거나 주석처리 되어 있는 경우

진단 방법

■ /etc/openstack-dashboard/local_settings.py 또는 /etc/openstack-dashboard/local_settings 파일에서 SECURE_PROXY_SSL_HEADER 설정값 확인

cat /etc/openstack-dashboard/local_settings | grep -i "SECURE_PROXY_SSL_HEADER = ('HTTP_X_FORWARDED_PROTO', 'https')"

```
[root@localhost ~]# cat /etc/openstack-dashboard/local_settings | grep
 -i "SECURE_PROXY_SSL_HEADER = ('HTTP_X_FORWARDED_PROTO', 'https')"
#SECURE_PROXY_SSL_HEADER = ('HTTP_X_FORWARDED_PROTO', 'https')
```

조치 방법

■ /etc/openstack-dashboard/local_settings.py 또는 /etc/openstack-dashboard/local_settings 파일에서 SECURE_PROXY_SSL_HEADER 값을 ('HTTP_X_FORWARDED_PROTO', 'https')로 설정

# vi /etc/openstack-dashboard/local_settings.py
SECURE_PROXY_SSL_HEADER = ('HTTP_X_FORWARDED_PROTO', 'https')

또는

# vi /etc/openstack-dashboard/local_settings
SECURE_PROXY_SSL_HEADER = ('HTTP_X_FORWARDED_PROTO', 'https')

```
# https://docs.djangoproject.com/en/dev/ref/settings/#secure-proxy-ssl
-header
SECURE_PROXY_SSL_HEADER = ('HTTP_X_FORWARDED_PROTO', 'https')
```

※ [default]로는 SECURE_PROXY_SSL_HEADER = 〈none〉으로 되어있음

Compute 인증을 위한 보안프로토콜 사용

항목설명

오픈스택 구성요소는 다양한 프로토콜을 사용하여 서로 통신하며 이러한 통신에는 민감하거나 기밀데이터가 포함되어 있을 수 있다. 공격자는 중요한 정보를 얻기 위해 채널을 도청하려고 시도할 수 있다. 모든 구성요소는 보안 통신 프로토콜을 사용하여 통신하여야 한다.

진단 기준

양호

/etc/nova/nova.conf 파일에서 [keystone_authtoken] 섹션의 auth_uri 매개변수가 https://로 시작하고, insecure 매개변수가 False로 되어 있는 경우

취약

/etc/nova/nova.conf 파일에서 [keystone_authtoken] 섹션의 auth_uri 매개변수가 https://로 시작하지 않고, insecure 매개변수가 True로 되어 있는 경우

진단 방법

■ /etc/nova/nova.conf 파일에서 [keystone_authtoken] 섹션의 auth_uri 설정 값 확인

cat /etc/nova/nova.conf | grep –i “auth_uri”

```
[root@localhost ~]# cat /etc/nova/nova.conf | grep -i "auth_uri"
# Deprecated group;name - [keystone_authtoken]/auth_uri
# Reason: The auth_uri option is deprecated in favor of www_authentica
te_uri and
#auth_uri=<None>
```

■ /etc/nova/nova.conf 파일에서 [keystone_authtoken] 섹션의 insecure 설정 값 확인

cat /etc/nova/nova.conf | grep –i “insecure”

```
[root@localhost ~]# cat /etc/nova/nova.conf | grep -i "insecure"
# Specifies if insecure TLS (https) requests. If False, the server's c
ertificate
#insecure=false
#insecure=false
#insecure=false
#insecure=false
#insecure=false
#insecure=false
#allow_insecure_clients=false
#insecure=false
#insecure=false
#insecure=false
#insecure=false
```

조치 방법

■ /etc/nova/nova.conf 파일에서 [keystone_authtoken] 섹션의 auth_uri 값을 https://로 시작하도록 설정

vi /etc/nova/nova.conf
[keystone_authtoken]
...
auth_uri = https://x.x.x.x [주소]

```
[keystone_authtoken]

auth_uri = https://controller:5000
```

■ /etc/nova/nova.conf 파일에서 [keystone_authtoken] 섹션의 insecure 값을 false로 설정

vi /etc/nova/nova.conf
[keystone_authtoken]
...
insecure = false

```
# Verify HTTPS connections. (boolean value)
insecure=false
```

※ [default]로는 auth_uri = None으로 되어있음

Nova와 Glance의 안전한 통신

항목설명

오픈스택 구성요소는 다양한 프로토콜을 사용하여 서로 통신하며 이러한 통신에는 민감하거나 기밀데이터가 포함되어 있을 수 있다. 공격자는 중요한 정보를 얻기 위해 채널을 도청하려고 시도할 수 있다. 모든 구성요소는 보안 통신 프로토콜을 사용하여 통신하여야 한다.

진단 기준

양호

/etc/nova/nova.conf 파일에서 [glance] 섹션의 api_servers 매개변수가 https://로 시작하고, api_insecure 매개변수가 False로 되어있는 경우

취약

/etc/nova/nova.conf 파일에서 [glance] 섹션의 api_servers 매개변수가 https://로 시작하지 않고, api_insecure 매개변수가 True로 되어있는 경우

진단 방법

■ /etc/nova/nova.conf 파일에서 [glance] 섹션의 api_servers 설정 값 확인

cat /etc/nova/nova.conf | grep –i “api_servers”

```
[root@localhost ~]# cat /etc/nova/nova.conf | grep -i "api_servers"
# loading options. Only use api_servers if you need multiple endpoints
 and are
api_servers=http://controller:9292
```

■ /etc/nova/nova.conf 파일에서 [glance] 섹션의 api_insecure 설정 값 확인

cat /etc/nova/nova.conf | grep –i “api_insecure”

```
[root@localhost ~]# cat /etc/nova/nova.conf | grep -i "api_insecure"
api_insecure = False
```

조치 방법

■ /etc/nova/nova.conf 파일에서 [glance] 섹션의 api_servers 값을 https://로 시작하도록 설정

vi /etc/nova/nova.conf
[glance]
…
api_servers = https://x.x.x.x

```
#  (list value)
api_servers=https://controller:9292
api_insecure = False
#
```

■ /etc/nova/nova.conf 파일에서 [glance] 섹션의 api_insecure 값을 false로 설정

vi /etc/nova/nova.conf
[glance]
…
api_insecure = False

```
#  (list value)
api_servers=https://controller:9292
api_insecure = False
#
```

※ [default]로는 api_servers = None, api_insecure = False로 되어있음

블록 스토리지 서비스 인증을 위한 TLS 활성화

항목설명

오픈스택 구성요소는 다양한 프로토콜을 사용하여 서로 통신하며 이러한 통신에는 민감하거나 기밀데이터가 포함되어 있을 수 있다. 공격자는 중요한 정보를 얻기 위해 채널을 도청하려고 시도할 수 있다. 모든 구성요소는 보안 통신 프로토콜을 사용하여 통신하여야 한다.

진단 기준

양호

/etc/cinder/cinder.conf 파일에서 [keystone_authtoken] 섹션의 auth_uri 매개변수가 https://로 시작하고, insecure 매개변수가 False로 되어있는 경우

취약

/etc/cinder/cinder.conf 파일에서 [keystone_authtoken] 섹션의 auth_uri 매개변수가 https://로 시작하지 않고, insecure 매개변수가 True로 되어 있는 경우

진단 방법

■ /etc/cinder/cinder.conf 파일에서 [keystone_authtoken] 섹션의 auth_uri 설정 값 확인

cat /etc/cinder/cinder.conf | grep –i “auth_uri”

```
[root@localhost ~]# cat /etc/cinder/cinder.conf | grep -i "auth_uri"
# Deprecated group/name - [keystone_authtoken]/auth_uri
# Reason: The auth_uri option is deprecated in favor of www_authentica
te_uri
#auth_uri = <None>
```

■ /etc/cinder/cinder.conf 파일에서 [keystone_authtoken] 섹션의 insecure 설정 값 확인

cat /etc/cinder/cinder.conf | grep –i “insecure”

```
[root@localhost ~]# cat /etc/cinder/cinder.conf | grep -i "insecure"
#backup_swift_auth_insecure = false
# Allow to perform insecure SSL (https) requests to glance (https will
 be used
#glance_api_insecure = false
# root user and insecure. If set to True, access is not as root. If se
t to
#vmware_insecure = false
# Specifies if insecure TLS (https) requests. If False, the server's
#insecure = false
#insecure = false
#allow_insecure_clients = false
#insecure = false
```

조치 방법

■ /etc/cinder/cinder.conf 파일에서 [keystone_authtoken] 섹션의 auth_uri 값을 https://로 시작하도록 설정

vi /etc/cinder/cinder.conf
[keystone_authtoken]
...
auth_uri = https://x.x.x.x

```
[keystone_authtoken]

auth_uri = https://controller:5000
```

■ /etc/cinder/cinder.conf파일에서 [keystone_authtoken] 섹션의 insecure 값을 false로 설정

vi /etc/cinder/cinder.conf
[keystone_authtoken]
...
insecure = false

```
# Verify HTTPS connections. (boolean value)
insecure = false
```

※ [default]로는 auth_uri = None으로 되어있음

cinder와 nova의 TLS 통신

항목설명

오픈스택 구성요소는 다양한 프로토콜을 사용하여 서로 통신하며 이러한 통신에는 민감하거나 기밀데이터가 포함되어 있을 수 있다. 공격자는 중요한 정보를 얻기 위해 채널을 도청하려고 시도할 수 있다. 모든 구성요소는 보안 통신 프로토콜을 사용하여 통신하여야 한다.

진단 기준

양호

/etc/cinder/cinder.conf 파일에서 [DEFAULT] 섹션의 nova_api.insecure 매개변수가 False로 되어있는 경우

취약

/etc/cinder/cinder.conf 파일에서 [DEFAULT] 섹션의 nova_api.insecure 매개변수가 True로 되어있는 경우

진단 방법

■ /etc/cinder/cinder.conf 파일에서 [DEFAULT] 섹션의 nova_api.insecure 설정 값 확인

cat /etc/cinder/cinder.conf | grep –i “nova_api.insecure”

```
[root@localhost ~]# cat /etc/cinder/cinder.conf |grep -i "nova_api.ins
ecure"
nova_api.insecure = False
```

조치 방법

■ /etc/cinder/cinder.conf 파일에서 [DEFAULT] 섹션의 nova_api.insecure 설정 값을 False로 설정

# vi /etc/cinder/cinder.conf
nova_api.insecure = False

```
[nova]

#
# From cinder
#

nova_api.insecure = False
```

cinder와 glance의 TLS 통신

항목설명

오픈스택 구성요소는 다양한 프로토콜을 사용하여 서로 통신하며 이러한 통신에는 민감하거나 기밀데이터가 포함되어 있을 수 있다. 공격자는 중요한 정보를 얻기 위해 채널을 도청하려고 시도할 수 있다. 모든 구성요소는 보안 통신 프로토콜을 사용하여 통신하여야 한다.

진단 기준

양호

/etc/cinder/cinder.conf 파일에서 [DEFAULT] 섹션의 glance_api.insecure 매개변수가 False로 되어있고, glance_api.servers 매개변수가 https://로 되어있는 경우

취약

/etc/cinder/cinder.conf 파일에서 [DEFAULT] 섹션의 glance_api.insecure 매개변수가 True로 되어있고, glance_api.servers 매개변수가 https://로 되어있지 않은 경우

진단 방법

■ /etc/cinder/cinder.conf 파일에서 [DEFAULT] 섹션의 glance_api.insecure 설정 값 확인

cat /etc/cinder/cinder.conf | grep –i “glance_api.insecure”

```
[root@localhost ~]# cat /etc/cinder/cinder.conf | grep -i "glance_api.
insecure"
glance_api_insecure = false
```

■ /etc/cinder/cinder.conf 파일에서 [DEFAULT] 섹션의 glance_api_servers 설정값 확인

cat /etc/cinder/cinder.conf | grep –i “glance_api_servers”

```
[root@localhost ~]# cat /etc/cinder/cinder.conf | grep -i "glance_api_
servers"
glance_api_servers = https://controller:5000
```

조치 방법

■ /etc/cinder/cinder.conf 파일에서 [DEFAULT] 섹션의 glance_api.insecure 값을 False로 설정

vi /etc/cinder/cinder.conf
[DEFAULT]
glance_api.insecure = False

```
# but cert validation will not be performed). (boolean value)
glance_api_insecure = false
```

■ /etc/cinder/cinder.conf 파일에서 [DEFAULT] 섹션의 glance_api_servers 값을 https://로 설정

vi /etc/cinder/cinder.conf
[DEFAULT]
glance_api_servers = https://x.x.x.x

```
# http. (list value)
glance_api_servers = https://controller:5000
```

이미지 스토리지 서비스 인증을 위한 TLS 활성화

항목설명

오픈스택 구성요소는 다양한 프로토콜을 사용하여 서로 통신하며 이러한 통신에는 민감하거나 기밀데이터가 포함되어 있을 수 있다. 공격자는 중요한 정보를 얻기 위해 채널을 도청하려고 시도할 수 있다. 모든 구성요소는 보안 통신 프로토콜을 사용하여 통신하여야 한다.

진단 기준

양호

/etc/glance/glance-api.conf 파일에서 [keystone_authtoken] 섹션의 auth_uri 매개변수가 https://로 되어 있고, /etc/glance/glance-registry.conf 파일에서 [keystone_authtoken] 섹션의 insecure 매개변수가 False로 되어있는 경우

취약

/etc/glance/glance-api.conf 파일에서 [keystone_authtoken] 섹션의 auth_uri 매개변수가 https://로 되어 있지 않고, /etc/glance/glance-registry.conf 파일에서 [keystone_authtoken] 섹션의 insecure 매개변수가 True로 되어있는 경우

진단 방법

■ /etc/glance/glance-api.conf 파일에서 [keystone_authtoken] 섹션의 auth_uri 설정 값 확인

cat /etc/glance/glance-api.conf | grep -i "auth_uri"

```
[root@localhost ~]# cat /etc/glance/glance-api.conf | grep -i "auth_ur
i"
# Deprecated group/name - [keystone_authtoken]/auth_uri
# Reason: The auth_uri option is deprecated in favor of www_authentica
te_uri and
#auth_uri = <None>
```

■ /etc/glance/glance-registry.conf 파일에서 [keystone_authtoken] 섹션의 insecure 설정 값 확인

cat /etc/glance/glance-registry.conf | grep -i "insecure"

```
[root@localhost ~]# cat /etc/glance/glance-api.conf | grep -i "insecur
e"
# This option is ignored if the ``registry_client_insecure`` option
#     * registry_client_insecure
# registry's equivalent of specifying --insecure on the command line
#registry_client_insecure = false
# ``cinder_api_insecure`` must be set to ``True`` to enable the verifi
cation.
#     * cinder_api_insecure
# Allow to perform insecure SSL requests to cinder.
#cinder_api_insecure = false
# this option is set, the ``https_insecure`` option will be ignored an
d
#     * https_insecure
#https_insecure = true
#swift_store_auth_insecure = false
#     * swift_store_auth_insecure
# Deprecated group/name - [glance_store]/vmware_api_insecure
#vmware_insecure = false
# If this option is set, the "vmware_insecure" option will be ignored
#     * vmware_insecure
#insecure = false
#allow_insecure_clients = false
```

조치 방법

■ /etc/glance/glance-api.conf 파일에서 [keystone_authtoken] 섹션의 auth_uri 값을 https://로 설정

vi /etc/glance/glance-api.conf
[keystone_authtoken]
auth_uri = https://x.x.x.x

```
# will be removed in the S  release.
auth_uri = https://controller:5000
```

■ /etc/glance/glance-registry.conf 파일에서 [keystone_authtoken] 섹션의 insecure 값을 False로 설정

vi /etc/glance/glance-registry.conf
[keystone_authtoken]
insecure = False

```
# Verify HTTPS connections. (boolean value)
insecure = false
```

공유 파일 시스템 인증을 위한 TLS 활성화

항목설명

오픈스택 구성요소는 다양한 프로토콜을 사용하여 서로 통신하며 이러한 통신에는 민감하거나 기밀데이터가 포함되어 있을 수 있다. 공격자는 중요한 정보를 얻기 위해 채널을 도청하려고 시도할 수 있다. 모든 구성요소는 보안 통신 프로토콜을 사용하여 통신하여야 한다.

진단 기준

양호

1. /etc/manila/manila.conf 파일에서 [keystone_authtoken] 섹션의 auth_protocol 매개변수가 https로 되어 있는 경우
2. /etc/manila/manila.conf 파일에서 [keystone_authtoken] 섹션의 identity_uri 매개변수가 https://로 되어 있고, insecure 매개변수가 False로 되어 있는 경우

취약

1. /etc/manila/manila.conf 파일에서 [keystone_authtoken] 섹션의 auth_protocol 매개변수가 https로 되어 있지 않은 경우
2. /etc/manila/manila.conf 파일에서 [keystone_authtoken] 섹션의 identity_uri 매개변수가 https://로 되어 있지 않고, insecure 매개변수가 True로 되어 있는 경우

진단 방법

■ /etc/manila/manila.conf 파일에서 [keystone_authtoken] 섹션의 auth_protocol 설정값 확인

cat /etc/manila/manila.conf | grep –i “auth_protocol”

```
[root@localhost ~]# cat /etc/manila/manila.conf | grep -i "auth_protoc
ol"
```

또는
/etc/manila/manila.conf 파일에서 [keystone_authtoken] 섹션의 identity_uri 설정값 확인

cat /etc/manila/manila.conf | grep –i “identity_uri”

```
[root@localhost ~]# cat /etc/manila/manila.conf | grep -i "identity_ur
i"
```

■ /etc/manila/manila.conf 파일에서 [keystone_authtoken] 섹션의 insecure 설정값 확인

cat /etc/manila/manila.conf | grep –i “insecure”

```
[root@localhost ~]# cat /etc/manila/manila.conf | grep -i "insecure"
#knfs_export_options = rw,sync,no_root_squash,insecure,no_wdelay,no_su
btree_check
#insecure = false
#insecure = false
#insecure = false
#insecure = false
#allow_insecure_clients = false
```

조치 방법

■ /etc/manila/manila.conf 파일에서 [keystone_authtoken] 섹션의 auth_protocol 값을 https로 설정

vi /etc/manila/manila.conf
[keystone_authtoken]
...
auth_protocol = https

```
[keystone_authtoken]

auth_protocol = https
```

또는
/etc/manila/manila.conf 파일에서 [keystone_authtoken] 섹션의 identity_uri 값을 https://로 설정

vi /etc/manila/manila.conf
[keystone_authtoken]
...
identity_uri = https://x.x.x.x

```
[keystone_authtoken]

identity_uri = https://controller:5000
```

■ /etc/manila/manila.conf 파일에서 [keystone_authtoken] 섹션의 insecure 값을 False로 설정

vi /etc/manila/manila.conf
[keystone_authtoken]
...
insecure = False

```
[keystone_authtoken]

insecure = False
```

TLS를 이용한 공유 파일 시스템과 Compute의 통신

항목설명

오픈스택 구성요소는 다양한 프로토콜을 사용하여 서로 통신하며 이러한 통신에는 민감하거나 기밀데이터가 포함되어 있을 수 있다. 공격자는 중요한 정보를 얻기 위해 채널을 도청하려고 시도할 수 있다. 모든 구성요소는 보안 통신 프로토콜을 사용하여 통신하여야 한다.

진단 기준

양호

/etc/manila/manila.conf 파일에서 [DEFAULT] 섹션의 nova_api_insecure 매개변수가 False로 되어 있는 경우

취약

/etc/manila/manila.conf 파일에서 [DEFAULT] 섹션의 nova_api_insecure 매개변수가 True로 되어 있는 경우

진단 방법

■ /etc/manila/manila.conf 파일에서 [DEFAULT] 섹션의 nova_api_insecure 설정값 확인

cat /etc/manila/manila.conf | grep –i “nova_api_insecure”

```
[root@localhost ~]# cat /etc/manila/manila.conf | grep -i "nova_api_in
secure"
nova_api_insecure = False
```

조치 방법

■ /etc/manila/manila.conf 파일에서 [DEFAULT] 섹션의 nova_api_insecure 값을 False로 설정

vi /etc/manila/manila.conf
[DEFAULT]
…
nova_api_insecure = False

```
[DEFAULT]

#
# From manila
#

nova_api_insecure = False
```

TLS를 이용한 공유 파일 시스템과 네트워킹과의 연결

항목설명

오픈스택 구성요소는 다양한 프로토콜을 사용하여 서로 통신하며 이러한 통신에는 민감하거나 기밀데이터가 포함되어 있을 수 있다. 공격자는 중요한 정보를 얻기 위해 채널을 도청하려고 시도할 수 있다. 모든 구성요소는 보안 통신 프로토콜을 사용하여 통신하여야 한다.

진단 기준

양호

/etc/manila/manila.conf 파일에서 [DEFAULT] 섹션의 neutron_api_insecure 매개변수가 False로 되어 있는 경우

취약

/etc/manila/manila.conf 파일에서 [DEFAULT] 섹션의 neutron_api_insecure 매개변수가 True로 되어 있는 경우

진단 방법

■ /etc/manila/manila.conf 파일에서 [DEFAULT] 섹션의 neutron_api_insecure 설정값 확인

cat /etc/manila/manila.conf | grep –i “neutron_api_insecure”

```
[root@localhost ~]# cat /etc/manila/manila.conf | grep -i "neutron_api
_insecure"
neutron_api_insecure = False
```

조치 방법

■ /etc/manila/manila.conf 파일에서 [DEFAULT] 섹션의 nova_api_insecure 값을 False로 설정

vi /etc/manila/manila.conf
[DEFAULT]
…
nova_api_insecure = False

```
[DEFAULT]

#
# From manila
#

nova_api_insecure = False
```

TLS를 이용한 공유 파일 시스템과 블록 스토리지 서비스와의 연결

항목설명

오픈스택 구성요소는 다양한 프로토콜을 사용하여 서로 통신하며 이러한 통신에는 민감하거나 기밀데이터가 포함되어 있을 수 있다. 공격자는 중요한 정보를 얻기 위해 채널을 도청하려고 시도할 수 있다. 모든 구성요소는 보안 통신 프로토콜을 사용하여 통신하여야 한다.

진단 기준

양호

/etc/manila/manila.conf 파일에서 [DEFAULT] 섹션의 cinder_api_insecure 매개변수가 False로 되어 있는 경우

취약

/etc/manila/manila.conf 파일에서 [DEFAULT] 섹션의 cinder_api_insecure 매개변수가 True로 되어 있는 경우

진단 방법

■ /etc/manila/manila.conf 파일에서 [DEFAULT] 섹션의 cinder_api_insecure 설정 값 확인

cat /etc/manila/manila.conf | grep –i “cinder_api_insecure”

```
[root@localhost ~]# cat /etc/manila/manila.conf | grep -i "cinder_api_
insecure"
cinder_api_insecure = False
```

조치 방법

■ /etc/manila/manila.conf 파일에서 [DEFAULT] 섹션의 cinder_api_insecure 값을 False로 설정

vi /etc/manila/manila.conf
[DEFAULT]
...
cinder_api_insecure = False

```
[DEFAULT]

#
# From manila
#

cinder_api_insecure = False
```

네트워킹 서비스의 인증을 위한 안전한 프로토콜 사용

항목설명

오픈스택 구성요소는 다양한 프로토콜을 사용하여 서로 통신하며 이러한 통신에는 민감하거나 기밀데이터가 포함되어 있을 수 있다. 공격자는 중요한 정보를 얻기 위해 채널을 도청하려고 시도할 수 있다. 모든 구성요소는 보안 통신 프로토콜을 사용하여 통신하여야 한다.

진단 기준

양호

/etc/neutron/neutron.conf 파일에서 [keystone_authtoken] 섹션의 auth_uri 매개변수가 https://로 되어 있고, insecure 매개변수가 False로 되어 있는 경우

취약

/etc/neutron/neutron.conf 파일에서 [keystone_authtoken] 섹션의 auth_uri 매개변수가 https://로 되어 있지 않고, insecure 매개변수가 True로 되어 있는 경우

진단 방법

■ /etc/neutron/neutron.conf 파일에서 [keystone_authtoken] 섹션의 auth_uri 설정값 확인

cat /etc/neutron/neutron.conf | grep –i “auth_uri”

```
[root@localhost ~]# cat /etc/neutron/neutron.conf | grep -i "auth_uri"
# Deprecated group/name - [keystone_authtoken]/auth_uri
# Reason: The auth_uri option is deprecated in favor of www_authentica
te_uri
#auth_uri = <None>
```

■ /etc/neutron/neutron.conf 파일에서 [keystone_authtoken] 섹션의 insecure 설정 값 확인

cat /etc/neutron/neutron.conf | grep –i “insecure”

```
[root@localhost ~]# cat /etc/neutron/neutron.conf | grep -i "insecure"

#insecure = false
#insecure = false
#allow_insecure_clients = false
```

조치 방법

■ /etc/neutron/neutron.conf 파일에서 [keystone_authtoken] 섹션의 auth_uri 값을 https://로 설정

vi /etc/neutron/neutron.conf
[keystone_authtoken]
...
auth_uri = https://x.x.x.x

```
# and will be removed in the S  release.
auth_uri = https://controller:5000
```

■ /etc/neutron/neutron.conf 파일에서 [keystone_authtoken] 섹션의 insecure 값을 False로 설정

vi /etc/neutron/neutron.conf
[keystone_authtoken]
...
insecure = False

```
# Verify HTTPS connections. (boolean value)
insecure = false
```

Neutron API 서버의 TLS 활성화

항목설명

오픈스택 구성요소는 다양한 프로토콜을 사용하여 서로 통신하며 이러한 통신에는 민감하거나 기밀데이터가 포함되어 있을 수 있다. 공격자는 중요한 정보를 얻기 위해 채널을 도청하려고 시도할 수 있다. 모든 구성요소는 보안 통신 프로토콜을 사용하여 통신하여야 한다.

진단 기준

양호

/etc/neutron/neutron.conf 파일에서 [DEFAULT] 섹션의 use_ssl 매개변수가 True로 되어 있는 경우

취약

/etc/neutron/neutron.conf 파일에서 [DEFAULT] 섹션의 use_ssl 매개변수가 False로 되어 있는 경우

진단 방법

■ /etc/neutron/neutron.conf 파일에서 [DEFAULT] 섹션의 use_ssl 설정 값 확인

cat /etc/neutron/neutron.conf | grep –i “use_ssl”

```
[root@localhost ~]# cat /etc/neutron/neutron.conf | grep -i "use_ssl"
#use_ssl = false
```

조치 방법

■ /etc/neutron/neutron.conf 파일에서 [DEFAULT] 섹션의 use_ssl 값을 True로 설정

vi /etc/neutron/neutron.conf
[DEFAULT]
…
use_ssl = True

```
# Enable SSL on the API server (boolean value)
use_ssl = true
```

Identity 서비스 max_request_body_size 설정

항목설명

max_request_body_size 매개변수는 요청 당 최대 본문 크기를 바이트 단위로 정의한다. 최대 크기가 정의되지 않은 경우 공격자는 대량의 대용량 요청을 생성하여 서비스를 중단시키고 결국 DoS(서비스거부) 공격을 유발할 수 있다. 최댓값을 지정하면 악의적인 대용량 요청이 차단되어 구성요소의 지속적인 가용성을 보장할 수 있다.

진단 기준

양호

/etc/keystone/keystone.conf 파일에서 max_request_body_size가 기본값(114688) 또는 적절한 값으로 설정되어 있는 경우

취약

/etc/keystone/keystone.conf 파일에서 max_request_body_size가 설정되어 있지 않은 경우

진단 방법

■ /etc/keystone/keystone.conf 파일에서 max_request_body_size 설정값 확인

cat /etc/keystone/keystone.conf | grep –i “max_request_body_size”

```
[root@localhost ~]# cat /etc/keystone/keystone.conf | grep -i "max_req
uest_body_size"
# Deprecated group/name - [DEFAULT]/osapi_max_request_body_size
# Deprecated group/name - [DEFAULT]/max_request_body_size
#max_request_body_size = 114688
```

조치 방법

■ /etc/keystone/keystone.conf 파일에서 max_request_body_size 값을 114688 또는 환경에 맞는 적절한 값으로 설정

# vi /etc/keystone/keystone.conf
max_request_body_size = 114688

```
# Deprecated group/name - [DEFAULT]/osapi_max_request_body_size
# Deprecated group/name - [DEFAULT]/max_request_body_size
max_request_body_size = 114688
```

※ [default]로는 max_request_body_size = 114688로 되어있음

admin 토큰 비활성화

항목설명

관리자 토큰은 일반적으로 ID를 부트스트랩하는데 사용된다. 이 토큰은 클라우드 관리자 권한을 얻는데 사용할 수 있는 가장 유용한 아이덴티티 자산이다.

진단 기준

양호

/etc/keystone/keystone.conf 파일에서 [DEFAULT] 섹션의 admin_token이 비활성화 되어 있고, /etc/keystone/keystone-paste.ini 파일에서 [filter:admin_token_auth] 섹션의 AdminTokenAuthMiddleware가 제거되어 있는 경우

취약

/etc/keystone/keystone.conf 파일에서 [DEFAULT] 섹션의 admin_token이 활성화 되어 있고, /etc/keystone/keystone-paste.ini 파일에서 [filter:admin_token_auth] 섹션의 AdminTokenAuthMiddleware가 존재하는 경우

진단 방법

■ /etc/keystone/keystone.conf 파일에서 [DEFAULT] 섹션의 admin_token 활성화 여부 확인

cat /etc/keystone/keystone.conf | grep –i “admin_token”

```
[root@localhost ~]# cat /etc/keystone/keystone.conf | grep -i "admin_t
oken"
# value is ignored and the `admin_token` middleware is effectively dis
abled.
#admin_token = <None>
```

■ /etc/keystone/keystone-paste.ini 파일에서 [filter:admin_token_auth] 섹션의 AdminTokenAuthMiddleware 존재 여부 확인

cat /etc/keystone/keystone-paste.ini | grep –i “AdminTokenAuthMiddleware”

```
[root@localhost ~]# cat /etc/keystone/keystone-paste.ini | grep -i "Ad
minTokenAuthMiddleware"
```

조치 방법

■ /etc/keystone/keystone.conf 파일에서 [DEFAULT] 섹션의 admin_token 비활성화

vi /etc/keystone/keystone.conf
[DEFAULT]
admin_token = 7e3a823....

```
# (string value)
#admin_token = <None>
```

■ /etc/keystone/keystone-paste.ini 파일에서 [filter:admin_token_auth] 섹션의 AdminTokenAuthMiddleware 비활성화

vi /etc/keystone/keystone-paste.ini
[filter:admin_token_auth]
paste.filter_factory = keystone.middleware:AdminTokenAuthMiddleware.factory.

```
[filter:admin_token_auth]
# paste.filter_factory = keystone.middleware:AdminTokenAuthMiddleware.
factory.
```

※ [default]로는 admin_token = ADMIN으로 되어있음

Dashboard의 DISALLOW_IFRAME_EMBED 설정

항목설명

DISALLOW_IFRAME_EMBED는 오픈스택 대시보드가 iframe 내에 포함되지 않도록 예방하는데 사용할 수 있다. 기존 브라우저는 여전히 XFS (Cross-Frame Scripting) 취약점에 취약하므로 이 옵션을 사용하면 배포 시 iframe을 사용하지 않는 경우 보안을 강화할 수 있다.

진단 기준

양호

/etc/openstack-dashboard/ local_settings.py 또는 /etc/openstack-dashboard/ local_settings 파일에서 DISALLOW_IFRAME_EMBED 매개변수가 True로 되어 있는 경우

취약

/etc/openstack-dashboard/ local_settings.py 또는 /etc/openstack-dashboard/ local_settings 파일에서 DISALLOW_IFRAME_EMBED 매개변수가 False로 되어 있는 경우

진단 방법

■ /etc/openstack-dashboard/local_settings.py 또는 /etc/openstack-dashboard/local_settings 파일에서 DISALLOW_IFRAME_EMBED 설정 값 확인

cat /etc/openstack-dashboard/local_settings.py | grep –i "DISALLOW_IFRAME_EMBED"

또는
cat /etc/openstack-dashboard/local_settings | grep –i "DISALLOW_IFRAME_EMBED"

```
[root@localhost ~]# cat /etc/openstack-dashboard/local_settings | grep
 -i "DISALLOW_IFRAME_EMBED"
# DISALLOW_IFRAME_EMBED can be used to prevent Horizon from being embe
dded
#DISALLOW_IFRAME_EMBED = True
```

조치 방법

■ /etc/openstack-dashboard/local_settings.py 또는 /etc/openstack-dashboard/local_settings 파일에서 DISALLOW_IFRAME_EMBED 값을 True로 설정

# vi /etc/openstack-dashboard/local_settings.py
DISALLOW_IFRAME_EMBED = True

또는
# vi /etc/openstack-dashboard/local_settings
DISALLOW_IFRAME_EMBED = True

```
# http://tinyurl.com/anticlickjack
DISALLOW_IFRAME_EMBED = True
```

※ [default]로는 DISALLOW_IFRAME_EMBED = True로 되어있음

Dashboard의 CSRF_COOKIE_SECURE 설정

항목설명

CSRF(사이트 간 요청 변조)는 사용자가 현재 인증된 웹 응용프로그램에서 권한이 없는 명령을 실행하도록 하는 공격이다. CSRF 공격이 성공하면 사용자 데이터 및 운영을 손상시킬 수 있다. 사용자에게 관리자 권한이 있으면 전체 웹 응용프로그램이 손상될 수 있다.

진단 기준

양호

/etc/openstack-dashboard/ local_settings.py 또는 /etc/openstack-dashboard/ local_settings 파일에서 CSRF_COOKIE_SECURE 매개변수가 True로 되어 있는 경우

취약

/etc/openstack-dashboard/ local_settings.py 또는 /etc/openstack-dashboard/ local_settings 파일에서 CSRF_COOKIE_SECURE 매개변수가 False로 되어 있는 경우

진단 방법

■ /etc/openstack-dashboard/local_settings.py 또는 /etc/openstack-dashboard/local_settings 파일에서 CSRF_COOKIE_SECURE 설정 값 확인

cat /etc/openstack-dashboard/local_settings.py | grep –i "CSRF_COOKIE_SECURE"

또는
cat /etc/openstack-dashboard/local_settings | grep –i "CSRF_COOKIE_SECURE"

```
[root@localhost ~]# cat /etc/openstack-dashboard/local_settings | grep
 -i "CSRF_COOKIE_SECURE"
#CSRF_COOKIE_SECURE = True
```

조치 방법

■ /etc/openstack-dashboard/local_settings.py 또는 /etc/openstack-dashboard/local_settings 파일에서 CSRF_COOKIE_SECURE 값을 True로 설정

# vi /etc/openstack-dashboard/local_settings.py
CSRF_COOKIE_SECURE = True

또는
# vi /etc/openstack-dashboard/local_settings
CSRF_COOKIE_SECURE = True

```
# settings to better secure the cookies from security exploits
CSRF_COOKIE_SECURE = True
#SESSION_COOKIE_SECURE = True
```

Dashboard의 SESSION_COOKIE_SECURE 설정

항목설명

"SECURE" 쿠키 속성은 웹 브라우저가 암호화된 HTTPS(SSL / TLS) 연결을 통해서만 쿠키를 보내도록 한다. 이 세션 보호 메커니즘은 MitM (Main-in-the-Middle) 공격을 통한 세션 ID의 공개를 막기 위해 반드시 필요하다. 침입자는 단순히 웹 브라우저 트래픽에서 세션 ID를 캡쳐할 수 없다.

진단 기준

양호

/etc/openstack-dashboard/ local_settings.py 또는 /etc/openstack-dashboard/ local_settings 파일에서 SESSION_COOKIE_SECURE 매개변수가 True로 되어 있는 경우

취약

/etc/openstack-dashboard/ local_settings.py 또는 /etc/openstack-dashboard/ local_settings 파일에서 SESSION_COOKIE_SECURE 매개변수가 False로 되어 있는 경우

진단 방법

■ /etc/openstack-dashboard/local_settings.py 또는 /etc/openstack-dashboard/local_settings 파일에서 SESSION_COOKIE_SECURE 설정 값 확인

cat /etc/openstack-dashboard/local_settings.py | grep –i "SESSION_COOKIE_SECURE"

또는

cat /etc/openstack-dashboard/local_settings | grep –i "SESSION_COOKIE_SECURE"

```
[root@localhost ~]# cat /etc/openstack-dashboard/local_settings | grep
 -i "SESSION_COOKIE_SECURE"
#SESSION_COOKIE_SECURE = True
```

조치 방법

■ /etc/openstack-dashboard/local_settings.py 또는 /etc/openstack-dashboard/local_settings 파일에서 SESSION_COOKIE_SECURE 값을 True로 설정

# vi /etc/openstack-dashboard/local_settings.py
SESSION_COOKIE_SECURE = True

또는

# vi /etc/openstack-dashboard/local_settings
SESSION_COOKIE_SECURE = True

```
# settings to better secure the cookies from security exploits
CSRF_COOKIE_SECURE = True
SESSION_COOKIE_SECURE = True
```

Dashboard의 SESSION_COOKIE_HTTPONLY 설정

항목설명

"HTTPONLY" 쿠키 속성은 웹 브라우저가 스크립트(예 : JavaScript 또는 VBscript)가 DOM document.cookie 객체를 통해 쿠키에 액세스하는 것을 허용하지 않도록 한다. 이 세션 ID 보호는 XSS공격을 통한 세션 ID 도용을 방지하기 위해 필수적이다.

진단 기준

양호

/etc/openstack-dashboard/ local_settings.py 또는 /etc/openstack-dashboard/ local_settings 파일에서 SESSION_COOKIE_HTTPONLY 매개변수가 True로 되어 있는 경우

취약

/etc/openstack-dashboard/ local_settings.py 또는 /etc/openstack-dashboard/ local_settings 파일에서 SESSION_COOKIE_HTTPONLY 매개변수가 False로 되어 있는 경우

진단 방법

■ /etc/openstack-dashboard/local_settings.py 또는 /etc/openstack-dashboard/local_settings 파일에서 SESSION_COOKIE_HTTPONLY 설정 값 확인

cat /etc/openstack-dashboard/local_settings.py | grep –i "SESSION_COOKIE_HTTPONLY"

또는
cat /etc/openstack-dashboard/local_settings | grep –i "SESSION_COOKIE_HTTPONLY"

```
[root@localhost ~]# cat /etc/openstack-dashboard/local_settings | grep
 -i "SESSION_COOKIE_HTTPONLY"
SESSION_COOKIE_HTTPONLY = True
```

조치 방법

■ /etc/openstack-dashboard/local_settings.py 또는 /etc/openstack-dashboard/local_settings 파일에서 SESSION_COOKIE_HTTPONLY 값을 True로 설정

# vi /etc/openstack-dashboard/local_settings.py
SESSION_COOKIE_HTTPONLY = True

또는
# vi /etc/openstack-dashboard/local_settings
SESSION_COOKIE_HTTPONLY = True

```
# settings to better secure the cookies from security exploits
CSRF_COOKIE_SECURE = True
SESSION_COOKIE_SECURE = True
SESSION_COOKIE_HTTPONLY = True
```

※ [default]로는 SESSION_COOKIE_HTTPONLY = True로 되어있음

Dashboard의 PASSWORD_AUTOCOMPLETE 설정

항목설명

응용 프로그램이 사용자에게 편의를 제공하기 위해 사용하는 공통 기능은 암호를 클라이언트 컴퓨터의 브라우저에 로컬로 캐시하고 모든 후속 요청에서 암호를 미리 입력하는 것이다. 이러한 기능은 일반적인 사용자에게 매우 친숙한 것으로 인식될 수 있지만 동시에 클라이언트 시스템에서 동일한 계정을 이용하는 사용자가 계정에 쉽게 접근할 수 있어 계정이 손상될 수 있는 취약점을 유발할 수 있다.

진단 기준

양호

/etc/openstack-dashboard/
local_settings.py 또는
/etc/openstack-dashboard/
local_settings 파일에서
PASSWORD_AUTOCOMPLETE
매개변수가 False로 되어 있는 경우

취약

/etc/openstack-dashboard/
local_settings.py 또는
/etc/openstack-dashboard/
local_settings 파일에서
PASSWORD_AUTOCOMPLETE
매개변수가 True로 되어 있는 경우

진단 방법

■ /etc/openstack-dashboard/local_settings.py 또는
/etc/openstack-dashboard/local_settings 파일에서
PASSWORD_AUTOCOMPLETE 설정 값 확인

cat /etc/openstack-dashboard/local_settings.py | grep –i
“PASSWORD_AUTOCOMPLETE”

또는
cat /etc/openstack-dashboard/local_settings | grep –i
“PASSWORD_AUTOCOMPLETE”

```
[root@localhost ~]# cat /etc/openstack-dashboard/local_settings | grep
 -i "PASSWORD_AUTOCOMPLETE"
#HORIZON_CONFIG["password_autocomplete"] = "off"
```

조치 방법

■ /etc/openstack-dashboard/local_settings.py 또는
/etc/openstack-dashboard/local_settings 파일에서
PASSWORD_AUTOCOMPLETE 값을 False로 설정

# vi /etc/openstack-dashboard/local_settings.py
PASSWORD_AUTOCOMPLETE = false

또는
# vi /etc/openstack-dashboard/local_settings
PASSWORD_AUTOCOMPLETE = false

```
# the database creation workflow if so desired.
PASSWORD_AUTOCOMPLETE = false
```

※ [default]로는 PASSWORD_AUTOCOMPLETE = off로 되어있음

Dashboard의 DISABLE_PASSWORD_REVEAL 설정

항목설명

클라이언트 시스템에서 동일한 계정을 이용하는 사용자가 계정에 쉽게 접근할 수 있어 계정이 손상될 수 있는 취약점을 유발할 수 있으므로 패스워드 필드를 노출하지 않아야 한다.

진단 기준

양호

/etc/openstack-dashboard/ local_settings.py 또는 /etc/openstack-dashboard/ local_settings 파일에서 DISABLE_PASSWORD_REVEAL 매개변수가 True로 되어 있는 경우

취약

/etc/openstack-dashboard/ local_settings.py 또는 /etc/openstack-dashboard/l ocal_settings 파일에서 DISABLE_PASSWORD_REVEAL 매개변수가 False로 되어 있는 경우

진단 방법

■ /etc/openstack-dashboard/local_settings.py 또는 /etc/openstack-dashboard/local_settings 파일에서 DISABLE_PASSWORD_REVEAL 설정 값 확인

cat /etc/openstack-dashboard/local_settings.py | grep –i “DISABLE_PASSWORD_REVEAL”

또는

cat /etc/openstack-dashboard/local_settings | grep –i “DISABLE_PASSWORD_REVEAL”

```
[root@localhost ~]# cat /etc/openstack-dashboard/local_settings | grep
 -i "DISABLE_PASSWORD_REVEAL"
#HORIZON_CONFIG["disable_password_reveal"] = False
```

조치 방법

■ /etc/openstack-dashboard/local_settings.py 또는 /etc/openstack-dashboard/local_settings 파일에서 DISABLE_PASSWORD_REVEAL 값을 True로 설정

# vi /etc/openstack-dashboard/local_settings.py
DISABLE_PASSWORD_REVEAL = true

또는

# vi /etc/openstack-dashboard/local_settings
DISABLE_PASSWORD_REVEAL = true

```
# including on the login form.
DISABLE_PASSWORD_REVEAL = true
```

※ [default]로는 DISABLE_PASSWORD_REVEAL = false로 되어있음

Dashboard의 ENFORCE_PASSWORD_CHECK 설정

항목설명

ENFORCE_PASSWORD_CHECK를 True로 설정하면 실제로 암호를 변경하려는 관리자로 로그인했는지 검증하기 위해 패스워드 변경 폼에 'Admin Password' 필드가 화면에 표시된다.

진단 기준

양호

/etc/openstack-dashboard/ local_settings.py 또는 /etc/openstack-dashboard/ local_settings 파일에서 ENFORCE_PASSWORD_CHECK 매개변수가 True로 되어 있는 경우

취약

/etc/openstack-dashboard/ local_settings.py 또는 /etc/openstack-dashboard/ local_settings 파일에서 ENFORCE_PASSWORD_CHECK 매개변수가 False로 되어 있는 경우

진단 방법

■ /etc/openstack-dashboard/local_settings.py 또는 /etc/openstack-dashboard/local_settings 파일에서 ENFORCE_PASSWORD_CHECK 설정 값 확인

cat /etc/openstack-dashboard/local_settings.py | grep –i "ENFORCE_PASSWORD_CHECK"

또는

cat /etc/openstack-dashboard/local_settings | grep –i "ENFORCE_PASSWORD_CHECK"

```
[root@localhost ~]# cat /etc/openstack-dashboard/local_settings | grep
 -i "ENFORCE_PASSWORD_CHECK"
ENFORCE_PASSWORD_CHECK = true
```

조치 방법

■ /etc/openstack-dashboard/local_settings.py 또는 /etc/openstack-dashboard/local_settings 파일에서 ENFORCE_PASSWORD_CHECK 값을 True로 설정

# vi /etc/openstack-dashboard/local_settings.py
ENFORCE_PASSWORD_CHECK = true

또는

# vi /etc/openstack-dashboard/local_settings
ENFORCE_PASSWORD_CHECK = true

```
# the password.
ENFORCE_PASSWORD_CHECK = true
```

※ [default]로는 ENFORCE_PASSWORD_CHECK = false로 되어있음

Dashboard의 PASSWORD_VALIDATOR 설정

항목설명

사용자 패스워드 복잡성을 검증하기 위해 정규 표현식을 허용해야 한다.

진단 기준

양호

/etc/openstack-dashboard/local_settings.py 또는 /etc/openstack-dashboard/local_settings 파일에서 PASSWORD_VALIDATOR가 설정되어 있는 경우

취약

/etc/openstack-dashboard/local_settings.py 또는 /etc/openstack-dashboard/local_settings 파일에서 PASSWORD_VALIDATOR가 설정되어 있지 않은 경우

진단 방법

■ /etc/openstack-dashboard/local_settings.py 또는 /etc/openstack-dashboard/local_settings 파일에서 PASSWORD_VALIDATOR 설정 확인

cat /etc/openstack-dashboard/local_settings.py | grep –i "PASSWORD_VALIDATOR" -A5

또는
cat /etc/openstack-dashboard/local_settings | grep –i "PASSWORD_VALIDATOR" -A5

```
[root@localhost ~]# cat /etc/openstack-dashboard/local_settings | grep
 -i "PASSWORD_VALIDATOR" -A5
#HORIZON_CONFIG["password_validator"] = {
#     "regex": '.*',
#     "help_text": _("Your password does not meet the requirements."),
#}

# Turn off browser autocompletion for forms including the login form a
nd
```

조치 방법

■ /etc/openstack-dashboard/local_settings.py 또는 /etc/openstack-dashboard/local_settings 파일에서 PASSWORD_VALIDATOR 설정

# vi /etc/openstack-dashboard/local_settings.py
HORIZON_CONFIG[“password_validator”] = {
“regex”: ‘.*’,
“help_text”: _(“Your password does not meet the requirements.”),

또는
# vi /etc/openstack-dashboard/local_settings
HORIZON_CONFIG[“password_validator”] = {
“regex”: ‘.*’,
“help_text”: _(“Your password does not meet the requirements.”),

```
# Specify a regular expression to validate user passwords.
HORIZON_CONFIG["password_validator"] = {
    "regex": '.*',
    "help_text": _("Your password does not meet the requirements."),
}
```

※ [default]로는 password_validator = {‘regex’: ‘.*’, ‘help_text’: _(“Password is not accepted”)}로 되어있음

Compute의 인증을 위한 keystone 사용

항목설명

오픈스택은 noauth, keystone와 같은 다양한 인증을 지원한다. noauth을 사용하면 사용자는 인증없이 OpenStack 서비스와 상호 작용할 수 있다. 이것은 공격자가 오픈스택 구성요소에 비인가 접근을 할 수 있기 때문에 잠재적인 위험이 될 수 있다. 모든 서비스는 서비스 계정을 사용하여 keystone으로 인증해야 한다.

진단 기준

양호

/etc/nova/nova.conf 파일에서 [DEFAULT] 섹션의 auth_strategy 매개변수가 keystone으로 되어있는 경우

취약

/etc/nova/nova.conf 파일에서 [DEFAULT] 섹션의 auth_strategy 매개변수가 noauth 또는 noauth2로 되어있는 경우

진단 방법

■ /etc/nova/nova.conf 파일에서 [DEFAULT] 섹션의 auth_strategy 설정 값 확인

cat /etc/nova/nova.conf | grep –i “auth_strategy”

```
[root@localhost ~]# cat /etc/nova/nova.conf | grep -i "auth_strategy"
auth_strategy=keystone
```

조치 방법

■ /etc/nova/nova.conf 파일에서 [DEFAULT] 섹션의 auth_strategy 값을 keystone으로 설정

vi /etc/nova/nova.conf
[DEFAULT]
auth_strategy = keystone

※ [default]로는 auth_strategy = keystone으로 되어있음

블록 스토리지 서비스의 인증을 위한 keystone 사용

항목설명

오픈스택은 noauth, keystone와 같은 다양한 인증을 지원한다. noauth을 사용하면 사용자는 인증 없이 OpenStack 서비스와 상호 작용할 수 있다. 이것은 공격자가 오픈스택 구성요소에 비인가 접근을 할 수 있기 때문에 잠재적인 위험이 될 수 있다. 모든 서비스는 서비스 계정을 사용하여 keystone으로 인증해야 한다.

진단 기준

양호

/etc/cinder/cinder.conf 파일에서 [DEFAULT] 섹션의 auth_strategy 매개변수가 keystone으로 되어있는 경우

취약

/etc/cinder/cinder.conf 파일에서 [DEFAULT] 섹션의 auth_strategy 매개변수가 noauth로 되어있는 경우

진단 방법

■ /etc/cinder/cinder.conf 파일에서 [DEFAULT] 섹션의 auth_strategy 설정 값 확인

cat /etc/cinder/cinder.conf | grep –i “auth_strategy”

```
[root@localhost ~]# cat /etc/cinder/cinder.conf | grep -i "auth_strate
gy"
auth_strategy = keystone
```

조치 방법

■ /etc/cinder/cinder.conf 파일에서 [DEFAULT] 섹션의 auth_strategy 값을 keystone으로 설정

vi /etc/cinder/cinder.conf
[DEFAULT]
auth_strategy = keystone

※ [default]로는 auth_strategy = noauth으로 되어있음

안전한 환경에서의 NAS 운영

항목설명

Cinder는 기존 블록 저장소 드라이버와 다르게 작동하는 NFS 드라이버를 지원한다. NFS 드라이버는 실제로 인스턴스가 블록 수준에서 저장 장치에 액세스하는 것을 허용하지 않는다. 대신 NFS 공유에 파일이 만들어지고 블록 장치를 에뮬레이트하는 인스턴스에 매핑된다. Cinder는 Cinder 볼륨이 생성될 때 파일 사용권한을 제어하여 이러한 파일에 대한 보안 구성을 지원한다. 또한 Cinder 설정은 파일 작업이 루트 사용자로 실행되는지 또는 현재 오픈스택 프로세스 사용자로 실행되는지 여부를 제어할 수 있다.

진단 기준

양호

/etc/cinder/cinder.conf 파일에서 [DEFAULT] 섹션의 nas_secure_file_permission 매개변수가 auto로 되어 있고, nas_secure_file_operations 매개변수가 auto로 되어있는 경우

취약

/etc/cinder/cinder.conf 파일에서 [DEFAULT] 섹션의 nas_secure_file_permission 매개변수가 false로 되어 있고, nas_secure_file_operations 매개변수가 false로 되어있는 경우

진단 방법

■ /etc/cinder/cinder.conf 파일에서 [DEFAULT] 섹션의 nas_secure_file_permission 설정 값 확인

cat /etc/cinder/cinder.conf | grep –i “nas_secure_file_permission”

```
[root@localhost ~]# cat /etc/cinder/cinder.conf | grep -i "nas_secure_
file_permission"
#nas_secure_file_permissions = auto
```

■ /etc/cinder/cinder.conf 파일에서 [DEFAULT] 섹션의 nas_secure_file_operations 설정 값 확인

cat /etc/cinder/cinder.conf | grep –i “nas_secure_file_operations”

```
[root@localhost ~]# cat /etc/cinder/cinder.conf | grep -i "nas_secure_
file_operations"
#nas_secure_file_operations = auto
```

조치 방법

■ /etc/cinder/cinder.conf 파일에서 [DEFAULT] 섹션의 nas_secure_file_permission 값을 auto로 설정

vi /etc/cinder/cinder.conf
[DEFAULT]
nas_secure_file_permission = auto

```
# is auto. (string value)
nas_secure_file_permissions = auto
```

■ /etc/cinder/cinder.conf 파일에서 [DEFAULT] 섹션의 nas_secure_file_operations 값을 auto로 설정

vi /etc/cinder/cinder.conf
[DEFAULT]
nas_secure_file_operations = auto

```
# used if so, otherwise False. Default is auto. (string value)
nas_secure_file_operations = auto
```

※ [default]로는 nas_secure_file_operations = auto로 되어있음

블록 스토리지 서비스에서 요청 본문 최대 크기 설정

항목설명

요청 당 최대 본문 크기가 정의되지 않은 경우 공격자는 큰 사이즈의 임의 OSAPI요청을 작성하여 서비스가 중단되는 Dos(Denial of Service) 공격이 발생할 수 있다. 최대값을 지정하면 악의적인 대량 요청이 차단되어 서비스의 지속적인 가용성을 보장할 수 있다.

진단 기준

양호

/etc/cinder/cinder.conf 파일에서 [DEFAULT] 섹션의 osapi_max_request_body_size가 기본 값(114688) 또는 적절한 값으로 설정되어 있거나, [oslo_middleware] 섹션의 max_request_body_size 매개변수가 기본 값(114688) 또는 적절한 값으로 설정되어 있는 경우

취약

/etc/cinder/cinder.conf 파일에서 [DEFAULT] 섹션의 osapi_max_request_body_size가 기본 값(114688) 또는 적절한 값으로 설정되어 있지 않거나, [oslo_middleware] 섹션의 max_request_body_size 매개변수가 기본 값(114688) 또는 적절한 값으로 설정되어 있지 않은 경우

진단 방법

■ /etc/cinder/cinder.conf 파일에서 [DEFAULT] 섹션의 osapi_max_request_body_size 설정 값 확인

cat /etc/cinder/cinder.conf | grep –i “osapi_max_request_body_size”

```
[root@localhost ~]# cat /etc/cinder/cinder.conf | grep -i "osapi_max_r
equest_body_size"
# Deprecated group/name - [DEFAULT]/osapi_max_request_body_size
osapi_max_request_body_size = 114688
```

■ /etc/cinder/cinder.conf 파일에서 [oslo_middleware] 섹션의 max_request_body_size 설정 값 확인

cat /etc/cinder/cinder.conf | grep –i “max_request_body_size”

```
[root@localhost ~]# cat /etc/cinder/cinder.conf | grep -i "max_request
_body_size"
# Deprecated group/name - [DEFAULT]/osapi_max_request_body_size
# Deprecated group/name - [DEFAULT]/max_request_body_size
osapi_max_request_body_size = 114688
max_request_body_size = 114688
```

조치 방법

■ /etc/cinder/cinder.conf 파일에서 [DEFAULT] 섹션의
osapi_max_request_body_size 값을 114866 또는 환경에 맞는 적절한 값으로 설정

vi /etc/cinder/cinder.conf
[DEFAULT]
...
osapi_max_request_body_size = 114688

```
# The maximum body size for each  request, in bytes. (integer value)
# Deprecated group/name - [DEFAULT]/osapi_max_request_body_size
# Deprecated group/name - [DEFAULT]/max_request_body_size
osapi_max_request_body_size = 114688
```

■ /etc/cinder/cinder.conf 파일에서 [oslo_middleware] 섹션의
max_request_body_size 값을 114866 또는 환경에 맞는 적절한 값으로 설정

vi /etc/cinder/cinder.conf
[oslo_middleware]
...
max_request_body_size = 114688

```
# The maximum body size for each  request, in bytes. (integer value)
# Deprecated group/name - [DEFAULT]/osapi_max_request_body_size
# Deprecated group/name - [DEFAULT]/max_request_body_size
osapi_max_request_body_size = 114688
max_request_body_size = 114688
```

※ [default]로는 osapi_max_request_body_size = 114688, max_request_body_size = 114688 으로 되어있음

블록 스토리지 볼륨 암호화

항목설명

암호화되지 않은 볼륨 데이터는 공격자가 여러 VM에 대한 데이터를 읽을 수 있으며 특히 볼륨 호스팅 플랫폼이 공격자에게 주요대상이 될 위험이 존재한다. 또한 물리적 저장 매체를 다른 컴퓨터에서 도난당하거나 재설치하거나 액세스할 수 있다. 볼륨 데이터를 암호화하면 이러한 위험이 완화되고 볼륨 호스팅 플랫폼에 심층적인 방어가 가능하다. 블록저장소(cinder)는 볼륨 데이터를 디스크에 쓰기 전에 암호화할 수 있으며 볼륨 암호화 기능을 사용하여야 한다.

진단 기준

양호

1. /etc/cinder/cinder.conf 파일에서 [KEY_MANAGER] 섹션의 api_class 매개변수가 설정되어 있는 경우
2. /etc/nova/nova.conf 파일에서 [KEY_MANAGER] 섹션의 api_class 매개변수가 설정되어 있는 경우

취약

1. /etc/cinder/cinder.conf 파일에서 [KEY_MANAGER] 섹션의 api_class 매개변수가 설정되어 있지 않은 경우
2. /etc/nova/nova.conf 파일에서 [KEY_MANAGER] 섹션의 api_class 매개변수가 설정되어 있지 않은 경우

진단 방법

■ /etc/cinder/cinder.conf 파일에서 [KEY_MANAGER] 섹션의 api_class 설정 값 확인

cat /etc/cinder/cinder.conf | grep –i “api_class”

```
[root@localhost ~]# cat /etc/cinder/cinder.conf | grep -i "api_class"
#volume_api_class = cinder.volume.api.API
#backup_api_class = cinder.backup.api.API
#transfer_api_class = cinder.transfer.api.API
#consistencygroup_api_class = cinder.consistencygroup.api.API
#group_api_class = cinder.group.api.API
#compute_api_class = cinder.compute.nova.API
# [key_manager]/api_class for some time. (string value)
# Deprecated group/name - [key_manager]/api_class
```

■ /etc/nova/nova.conf 파일에서 [KEY_MANAGER] 섹션의 api_class 설정 값 확인

cat /etc/nova/nova.conf | grep –i “api_class”

```
[root@localhost ~]# cat /etc/nova/nova.conf | grep -i "api_class"
# [key_manager]/api_class for some time. (string value)
# Deprecated group;name - [key_manager]/api_class
```

조치 방법

■ /etc/cinder/cinder.conf 파일에서 [KEY_MANAGER] 섹션의 api_class 설정

vi /etc/cinder/cinder.conf
[KEY_MANAGER]
...
api_class = castellan.key_manager.barbican_key_manager.BarbicanKeyManager

```
[key_manager]

#
# From castellan.config
#

api_class = castellan.key_manager.barbican_key_manager.BarbicanKeyMana
ger
```

■ /etc/nova/nova.conf 파일에서 [KEY_MANAGER] 섹션의 api_class 설정

vi /etc/nova/nova.conf
[KEY_MANAGER]
...
api_class = castellan.key_manager.barbican_key_manager.BarbicanKeyManager

```
[key_manager]

#
# From nova.conf
#

api_class = castellan.key_manager.barbican_key_manager.BarbicanKeyMana
ger
```

※ [default]로는 api_class = cinder.keymgr.conf_key_mgr.ConfKeyManager로 되어있음

이미지 스토리지 서비스 인증을 위한 keystone 설정

항목설명

오픈스택은 noauth, keystone과 같은 다양한 인증 전략을 지원한다. noauth 전략을 사용하면 사용자는 인증 없이 OpenStack 서비스와 상호 작용할 수 있다. 이것은 공격자가 오픈스택 구성요소에 비인가 접근을 할 수 있기 때문에 잠재적인 위험이 될 수 있다. 모든 서비스는 서비스 계정을 사용하여 keystone으로 인증해야 한다.

진단 기준

양호

/etc/glance/glance-api.conf 파일에서 [DEFAULT] 섹션의 auth_strategy 매개변수가 keystone으로 되어 있고, /etc/glance/glance-registry.conf 파일에서 [DEFAULT] 섹션의 auth_strategy 매개변수가 keystone으로 되어 있는 경우

취약

/etc/glance/glance-api.conf 파일에서 [DEFAULT] 섹션의 auth_strategy 매개변수가 noauth로 되어 있거나, /etc/glance/glance-registry.conf 파일에서 [DEFAULT] 섹션의 auth_strategy 매개변수가 noauth로 되어 있는 경우

진단 방법

- /etc/glance/glance-api.conf 파일에서 [DEFAULT] 섹션의 auth_strategy 설정 값 확인

  # cat /etc/glance/glance-api.conf | grep -i "auth_strategy"

```
[root@localhost ~]# cat /etc/glance/glance-api.conf | grep -i "auth_st
rategy"
#auth_strategy = noauth
```

- /etc/glance/glance-registry.conf 파일에서 [DEFAULT] 섹션의 auth_strategy 설정 값 확인

  # cat /etc/glance/glance-registry.conf | grep -i "auth_strategy"

```
[root@localhost ~]# cat /etc/glance/glance-registry.conf | grep -i "au
th_strategy"
```

조치 방법

■ /etc/glance/glance-api.conf 파일에서 [DEFAULT] 섹션의 auth_strategy를 keystone으로 설정

vi /etc/glance/glance-api.conf
[DEFAULT]
auth_strategy = keystone

```
# Keystone trusts support.
auth_strategy = keystone
```

■ /etc/glance/glance-registry.conf 파일에서 [DEFAULT] 섹션의 auth_strategy를 keystone으로 설정

vi /etc/glance/glance-registry.conf
[DEFAULT]
auth_strategy = keystone

```
[DEFAULT]

#
# From glance.registry
#

auth_strategy = keystone
```

※ [default]로는 auth_strategy = keystone

공유파일 시스템 인증을 위한 오픈스택 Identity 사용

항목설명

오픈스택은 noauth, keystone과 같은 다양한 인증을 지원한다. noauth을 사용하면 사용자는 인증 없이 OpenStack 서비스와 상호 작용할 수 있다. 이것은 공격자가 오픈스택 구성요소에 비인가 접근을 할 수 있기 때문에 잠재적인 위험이 될 수 있다. 모든 서비스는 서비스 계정을 사용하여 keystone으로 인증해야 한다.

진단 기준

양호

/etc/manila/manila.conf 파일에서 [DEFAULT] 섹션의 auth_strategy 매개변수가 keystone으로 되어있는 경우

취약

/etc/manila/manila.conf 파일에서 [DEFAULT] 섹션의 auth_strategy 매개변수가 noauth로 되어있는 경우

진단 방법

■ /etc/manila/manila.conf 파일에서 [DEFAULT] 섹션의 auth_strategy 설정 값 확인

cat /etc/manila/manila.conf | grep –i “auth_strategy”

```
[root@localhost ~]# cat /etc/manila/manila.conf | grep -i "auth_strate
gy"
auth_strategy = keystone
```

조치 방법

■ /etc/manila/manila.conf파일에서 [DEFAULT] 섹션의 auth_strategy를 keystone으로 설정

vi /etc/manila/manila.conf
[DEFAULT]
auth_strategy = keystone

```
[DEFAULT]

#
# From manila
#

auth_strategy = keystone
```

※ [default]로는 auth_strategy = keystone

공유파일 시스템에서 요청 본문 최대 사이즈 설정

항목설명

요청 당 최대 본문 크기가 정의되지 않은 경우 공격자는 큰 사이즈의 임의 OSAPI요청을 작성하여 서비스가 중단되는 DoS(Denial of Service) 공격이 발생할 수 있다. 최댓값을 지정하면 악의적인 대량 요청이 차단되어 서비스의 지속적인 가용성을 보장할 수 있다.

진단 기준

양호

/etc/manila/manila.conf 파일에서 [DEFAULT] 섹션의 osapi_max_request_body_size가 기본 값(114688) 또는 적절한 값으로 설정되어 있거나, [oslo_middleware] 섹션의 max_request_body_size 매개변수가 기본 값(114688) 또는 적절한 값으로 설정되어 있는 경우

취약

/etc/manila/manila.conf 파일에서 [DEFAULT] 섹션의 osapi_max_request_body_size가 기본 값(114688) 또는 적절한 값으로 설정되어 있지 않거나, [oslo_middleware] 섹션의 max_request_body_size 매개변수가 기본 값(114688) 또는 적절한 값으로 설정되어 있지 않은 경우

진단 방법

■ /etc/manila/manila.conf 파일에서 [DEFAULT] 섹션의 osapi_max_request_body_size 설정 값 확인

cat /etc/manila/manila.conf | grep –i “osapi_max_request_body_size”

```
[root@localhost ~]# cat /etc/manila/manila.conf | grep -i "osapi_max_r
equest_body_size"
# Deprecated group/name - [DEFAULT]/osapi_max_request_body_size
osapi_max_request_body_size = 114688
```

■ /etc/manila/manila.conf 파일에서 [oslo_middleware] 섹션의 max_request_body_size 설정 값 확인

cat /etc/manila/manila.conf | grep –i “max_request_body_size”

```
[root@localhost ~]# cat /etc/manila/manila.conf | grep -i "max_request
_body_size"
# Deprecated group/name - [DEFAULT]/osapi_max_request_body_size
# Deprecated group/name - [DEFAULT]/max_request_body_size
osapi_max_request_body_size = 114688
max_request_body_size = 114688
```

조치 방법

■ /etc/manila/manila.conf 파일에서 [DEFAULT] 섹션의 osapi_max_request_body_size 값을 114688 또는 환경에 맞는 적절한 값으로 설정

vi /etc/manila/manila.conf
[DEFAULT]
...
osapi_max_request_body_size = 114688

```
# The maximum body size for each  request, in bytes. (integer value)
# Deprecated group/name - [DEFAULT]/osapi_max_request_body_size
# Deprecated group/name - [DEFAULT]/max_request_body_size
osapi_max_request_body_size = 114688
```

■ /etc/manila/manila.conf 파일에서 [oslo_middleware] 섹션의 max_request_body_size 값을 114688 또는 환경에 맞는 적절한 값으로 설정

vi /etc/manila/manila.conf
[oslo_middleware]
...
max_request_body_size = 114688

```
# The maximum body size for each  request, in bytes. (integer value)
# Deprecated group/name - [DEFAULT]/osapi_max_request_body_size
# Deprecated group/name - [DEFAULT]/max_request_body_size
osapi_max_request_body_size = 114688
max_request_body_size = 114688
```

※ [default]로는 osapi_max_request_body_size = 114688, max_request_body_size = 114688 으로 되어있음

2.30.

PHP

2.30. PHP

보안설정(5개 항목), 패치 관리(1개 항목) 총 2개 영역에서 6개 항목으로 구성된다.

[표 30] PHP 진단 체크리스트

구분	진단 항목
가. 보안 설정	오류 메시지 노출
	불필요한 헤더 정보 노출
	외부 URL 파일 인클루드 비활성화
	불필요한 명령어 사용제한
	PHP 실행 경로 제한
나. 패치 관리	최신 보안 패치 적용

오류 메시지 노출

항목설명

소스 코드, 예외 처리, 시스템 콜, API 함수 호출 등 오류가 발생한 경우 실행 환경, 개발 정보, 사용자 관련 데이터에 대한 민감한 정보를 포함하는 오류 메시지가 노출될 수 있다. PHP는 display_errors 설정이 Off로 설정된 경우 오류 메시지가 웹 페이지에 노출되지 않는다.

진단 기준

양호

display_errors 항목이 Off로 설정된 경우

취약

display_errors 항목이 On으로 설정된 경우

진단 방법

■ PHP 설정 파일 조회

1) # cat /[PHP 설치 디렉터리]/php.ini | grep display_errors

```
root@ubuntu:/etc/php/8.1/cli# cat /etc/php/8.1/cli/php.ini | grep display_errors
; display_errors
display_errors = Off
; separately from display_errors. We strongly recommend you set this to 'off'
root@ubuntu:/etc/php/8.1/cli#
```

※ default 설정 : Off

조치 방법

■ PHP 설정 파일에서 수정

1) # vi /[PHP 설치 디렉터리]/php.ini
   display_errors = Off

불필요한 헤더 정보 노출

항목설명

HTTP 프로토콜을 이용할 경우 간혹 HTTP 헤더에 PHP 정보가 노출되어 공격자에게 정보를 제공한다. 공격자는 노출된 헤더 정보(운영체제, 웹 서버, PHP 버전 등)를 이용하여 추가 공격을 진행할 수 있으므로, PHP 옵션 중 expose_php를 Off로 설정하여 HTTP 헤더에 정보가 노출되지 않도록 설정해야 한다.

진단 기준

양호

expose_php가 Off로 설정된 경우

취약

expose_php가 On으로 설정된 경우

진단 방법

■ PHP 설정 파일 조회

1) # cat /[PHP 설치 디렉터리]/php.ini | grep expose_php

```
root@ubuntu:/etc/php/8.1/cli# cat /etc/php/8.1/cli/php.ini | grep expose_php
expose_php = On
root@ubuntu:/etc/php/8.1/cli#
```

조치 방법

■ PHP 설정 파일에서 수정

1) # vi /[PHP 설치 디렉터리]/php.ini
expose_php = Off

```
; threat in any way, but it makes it possible to determine whether you use PHP
; on your server or not.
; https://php.net/expose-php
expose_php = Off
```

외부 URL 파일 인클루드 비활성화

항목설명

웹 서버에 파일을 참조하는 파라미터가 존재할 경우, 외부 URL을 입력한다면 *RFI(Shell 코드 및 악성코드를 실행) 취약점이 발생할 수 있다. 이러한 문제점을 해결하기 위해 PHP 옵션 중 allow_url_fopen 설정이 존재하는데, 해당 설정을 Off로 설정하여 외부 파일을 참조하지 못하도록 설정하는 것을 권고한다.
*** RFI(Remote File Inclusion): 공격자가 입력한 URL을 서버가 참조하여 실행하는 취약점**

진단 기준

양호
allow_url_fopen이 Off로 설정된 경우

취약
allow_url_fopen이 On으로 설정된 경우

진단 방법

■ PHP 설정 파일 조회

1) # cat /[PHP 설치 디렉터리]/php.ini | grep allow_url_fopen

```
root@ubuntu:/etc/php/8.1/cli# cat /etc/php/8.1/cli/php.ini | grep allow_url_fopen
allow_url_fopen = On
root@ubuntu:/etc/php/8.1/cli#
```

조치 방법

■ PHP 설정 파일에서 수정

1) # vi /[PHP 설치 디렉터리]/php.ini
expose_php = Off

```
; Whether to allow the treatment of URLs (like http:// or ftp://) as files.
; https://php.net/allow-url-fopen
allow_url_fopen = Off
```

불필요한 명령어 사용 제한

항목설명

PHP 페이지 중 명령어를 입력할 수 있는 페이지 또는 악성 스크립트 파일이 실행(Web Shell, 악성코드 등)될 경우 시스템 권한을 획득할 수 있다. 이러한 문제점을 해결하기 위해 PHP 옵션 중 disable_functions 항목으로 명령어를 제어하여 시스템의 피해를 최소화할 수 있다.

진단 기준

양호

disable_functions에 설정(불필요한 함수)이 존재할 경우

취약

disable_functions에 설정이 존재하지 않을 경우

진단 방법

■ PHP 설정 파일 조회

1) # cat /[PHP 설치 디렉터리]/php.ini | grep disable_functions

```
root@ubuntu:/etc/php/8.1/cli# cat /etc/php/8.1/cli/php.ini | grep disable_functions
disable_functions =
root@ubuntu:/etc/php/8.1/cli#
```

아무런 설정값이 존재하지 않을 경우 취약

조치 방법

■ PHP 설정 파일에서 수정

1) # vi /[PHP 설치 디렉터리]/php.ini
예시)
disable_functions = exec, passthru, shell_exec, system, proc_open, popen, curl_exec, curl_multi_exec, parse_ini_file, show_source

```
; This directive allows you to disable certain functions.
; It receives a comma-delimited list of function names.
; https://php.net/disable-functions
disable_functions = exec, passthru, shell_exec, system, proc_open, popen, curl_exec,
curl_multi_exec, parse_ini_file, show_source
```

비고

※ 시스템에 영향을 주는 함수 예시
exec – 외부 프로그램을 실행하는 함수로 쉘 명령어 사용 가능
system – 외부 프로그램을 실행하는 함수로 쉘 명령어 사용 가능
shell_exec – PHP 상에서 쉘 명령어에 대한 결과값을 웹상에 출력하게 하는 함수
passthru – 외부 프로그램을 실행하고 실행되는 동안 화면을 실시간으로 출력하는 함수
phpinfo – PHP 정보(OS 및 PHP 정보 등)를 보여주는 함수
show_source – 소스 코드를 출력하는 함수
popen – 파일을 실행하고 그 결과값을 반환하는 함수
parse_ini_file – php 설정 파일을 배열에 저장하는 함수

PHP 실행 경로 제한

항목설명

파일 업로드, 파일 다운로드 및 파일 경로를 참조 페이지가 존재할 경우, 웹 루트 상위 폴더를 벗어나 시스템 파일을 참조할 수 있는 문제점이 발생(예) /etc/shadow, %WINNT%system32/config/SAM)한다. 웹 서버의 피해를 최소화하기 위해 PHP 옵션 open_basedir 경로를 지정하여 지정된 경로의 상위 폴더 접근을 제한할 수 있다.

진단 기준

양호

open_basedir에 경로를 지정한 경우

취약

open_basedir에 경로가 지정되어 있지 않은 경우

진단 방법

■ PHP 설정 파일 조회

1) # cat /[PHP 설치 디렉터리]/php.ini | grep open_basedir

```
root@ubuntu:/etc/php/8.1/cli# cat /etc/php/8.1/cli/php.ini | grep open_basedir
; open_basedir, if set, limits all file operations to the defined directory
;open_basedir =
; Note: if open_basedir is set, the cache is disabled
```

조치 방법

■ PHP 설정 파일에서 수정

1) # vi /[PHP 설치 디렉터리]/php.ini

```
; open_basedir, if set, limits all file operations to the defined directory
; and below.  This directive makes most sense if used in a per-directory
; or per-virtualhost web server configuration file.
; Note: disables the realpath cache
; https://php.net/open-basedir
;open_basedir = /var/www:/tmp
```

비고

※ 경로를 여러 개 지정할 시 :(콜론) 구분자를 이용하여 설정

※ 경로의 마지막에 /이 있으면 해당 디렉터리만 경로를 지정하고, /가 없는 경우에는 하위 디렉터리까지 경로를 지정함

최신 보안 패치 적용

항목설명

소프트웨어의 취약점이 공개되면 소프트웨어 및 버전별 문제점을 공개하는 사이트(CCE, CWE, CVE 등)들이 존재한다. 공격자는 간단한 검색만으로 소프트웨어 또는 버전별 취약점을 확인하여 추가 공격을 진행할 수 있다. 관련하여 소프트웨어의 보안 패치를 항상 주기적으로 업데이트하여 최신화해야 한다.

진단 기준

양호

최신 보안패치를 적용한 경우

취약

최신 보안패치를 적용하지 않은 경우

진단 방법

■ PHP 버전 조회

1) # php –v

```
PHP 8.1.25 (cli) (built: Oct 27 2023 14:00:40) (NTS)
Copyright (c) The PHP Group
Zend Engine v4.1.25, Copyright (c) Zend Technologies
    with Zend OPcache v8.1.25, Copyright (c), by Zend Technologies
root@ubuntu:/etc/php/8.1/cli# nano php.ini
```

조치 방법

■ PHP 사이트를 통해 주기적으로 버전 점검을 하도록 하며, 최신 보안 패치 적용 시 시스템 영향도를 파악하여 충분한 테스트 후 적용 권고

※ 최신 버전을 사용하도록 권고하고 있으나 시스템 운영상 적용이 어려운 경우 최신이 아닌 취약점이 존재하지 않는 버전도 허용하고 있음

2.31.

RabbitMQ

2.31. RabbitMQ

보안설정(4개 항목), 디렉터리 및 파일 권한 관리(2개 항목), 패치 및 로그 관리(2개 항목) 총 3개 영역에서 8개 항목으로 구성된다.

[표 31] RabbitMQ 진단 체크리스트

구분	진단 항목
가. 보안 설정	Guest 계정 제거
	불필요한 계정 권한 제거
	접속 IP 제한
	SSL 활성화
나. 디렉터리 및 파일 권한 관리	Mnesia 데이터베이스 디렉터리 및 파일 권한 설정
	설정 파일 권한 설정
나. 패치 및 로그 관리	로그 활성화
	최신 보안 패치 적용

Guest 계정 제거

항목설명

RabbitMQ 최초 설치 시 관리자 권한을 가진 guest 계정이 존재한다. guest 계정이 존재할 경우 비인가자에 의해 설정이 변경되어 서비스에 영향을 줄 수 있다. 이러한 문제를 해결하기 위해 guest 계정을 제거하여 비인가자에 의한 피해를 최소화 할 수 있다.

진단 기준

양호

guest 계정이 존재하지 않는 경우

취약

guest 계정이 존재하는 경우

진단 방법

■ guest 계정 조회

1) # [RabbitMQ 설치 디렉터리]/sbin/rabbitmqctl list_users

예시)

rabbitmqctl list_users

```
root@ubuntu:~# rabbitmqctl list_users
Listing users ...
user    tags
guest   [administrator]
root@ubuntu:~#
```

조치 방법

■ guest 계정 삭제

1) # [RabbitMQ 설치 디렉터리]/sbin/rabbitmqctl delete_user guest

```
root@ubuntu:/etc/rabbitmq# rabbitmqctl delete_user guest
Deleting user "guest" ...
root@ubuntu:/etc/rabbitmq# rabbitmqctl list_users
Listing users ...

root@ubuntu:/etc/rabbitmq#
```

불필요한 계정 권한 제거

항목설명

데이터베이스 계정 중 인가되지 않은 계정, 테스트 계정 등 실제로 업무에 사용하지 않는 불필요한 계정이 존재하고 그 계정 중 높은 권한이 존재할 경우 비인가자가 데이터베이스에 접속하여 데이터를 열람, 삭제, 및 수정할 수 있으므로 불필요한 계정이나 권한을 제거해야 한다.

진단 기준

양호

불필요한 계정이나 권한이 존재하지 않는 경우

취약

불필요한 계정이나 권한이 존재하는 경우

진단 방법

■ 계정 및 권한 조회

1) # [RabbitMQ 설치 디렉터리]/sbin/rabbitmqctl list_users

```
root@ubuntu:/etc/rabbitmq# rabbitmqctl list_users
Listing users ...
user    tags
monitor [monitoring]
TEST1   []
TEST    [administrator]
root@ubuntu:/etc/rabbitmq#
```

조치 방법

■ 불필요한 계정 또는 권한 제거

1) # [RabbitMQ 설치 디렉터리]/sbin/rabbitmqctl delete_user 〈계정명〉

```
root@ubuntu:/etc/rabbitmq# rabbitmqctl delete_user guest
Deleting user "guest" ...
```

2) # [RabbitMQ 설치 디렉터리]/sbin/rabbitmqctl set_user_tags 〈계정명〉

```
root@ubuntu:/etc/rabbitmq# rabbitmqctl set_user_tags TEST1 ''
Setting tags for user "TEST1" to [] ...
root@ubuntu:/etc/rabbitmq#
```

접속 IP 제한

항목설명

인가된 IP 접근만 가능하도록 설정되어 있지 않은 경우에 비인가 사용자가 RabbitMQ에 접근하여 설정 조회 및 설정 변경 위험이 존재하므로 RabbitMQ에 접근할 수 있는 IP를 제한하여야 한다.

진단 기준

양호

인가된 IP만 접근하도록 설정된 경우

취약

모든 IP 대역에서 접근할 수 있도록 설정된 경우

진단 방법

■ IP 설정 조회

1) # cat [RabbitMQ 설치 디렉터리]/rabbitmq.config

※ RabbitMQ가 설치된 Linux 서버의 접근 통제 설정 확인 필요

예시)

```
[root@localhost ~]# cat /etc/rabbitmq/rabbitmq.config
%% -*- mode: erlang -*-
%%----------------------------------------------------------------------------
%% RabbitMQ Sample Configuration File.
%%
%% See http://www.rabbitmq.com/configure.html for details.
%%----------------------------------------------------------------------------
[
 {rabbit,
  [%%
   %% Network Connectivity
   %% ====================
   %%

   %% By default, RabbitMQ will listen on all interfaces, using
   %% the standard (reserved) AMQP port.
   %%
   %% {tcp_listeners, [5672]},

   %% To listen on a specific interface, provide a tuple of {IpAddress, Port}.
   %% For example, to listen only on localhost for both IPv4 and IPv6:
   %%
   {tcp_listeners, [{"127.0.0.1", 5672},
   %%                  {"::1",       5672}]},
```

조치 방법

■ 불필요한 계정 도는 권한 제거

1) # vi [RabbitMQ 설치 디렉터리]/rabbitmq.config

예시)

```
%% -*- mode: erlang -*-
%%----------------------------------------------------------------------------
%% RabbitMQ Sample Configuration File.
%%
%% See http://www.rabbitmq.com/configure.html for details.
%%----------------------------------------------------------------------------
[
 {rabbit,
  [%%
   %% Network Connectivity
   %% ====================
   %%

   %% By default, RabbitMQ will listen on all interfaces, using
   %% the standard (reserved) AMQP port.
   %%
   %% {tcp_listeners, [5672]},

   %% To listen on a specific interface, provide a tuple of {IpAddress, Port}.
   %% For example, to listen only on localhost for both IPv4 and IPv6:
   %%
   {tcp_listeners, [{"127.0.0.1", 5672},
   %%                  {"::1",       5672}]},
```

SSL 활성화

항목설명

RabbitMQ는 기본적으로 SSL이 비활성화되어 있다. 만약 SSL을 사용하지 않는다면 스니핑을 통해 RabbitMQ와 Producer 간의 메시지를 훔쳐볼 수 있다. 이를 방지하기 위해 SSL을 활성화하여 메시지를 암호화하면 데이터 도청을 방지할 수 있다.

진단 기준

양호

SSL 설정이 활성화되어 있는 경우

취약

SSL 설정이 비활성화되어 있는 경우

진단 방법

■ SSL 활성화 여부 확인

1) # cat [RabbitMQ 설치 디렉터리]/rabbitmq.config

예시)

```
{ssl_options, [{cacertfile,"/etc/rabbitmq/conf/cacert.pem"},
               {certfile,"/etc/rabbitmq/conf/cert.pem"},
               {keyfile,"/etc/rabbitmq/conf/key.pem"},
               {verify,verify_peer},
               {fail_if_no_peer_cert,false}]}
```

조치 방법

■ SSL 활성화

1) # vi [RabbitMQ 설치 디렉터리]/rabbitmq.config

```
{ssl_options, [{cacertfile,"/etc/rabbitmq/conf/cacert.pem"},
               {certfile,"/etc/rabbitmq/conf/cert.pem"},
               {keyfile,"/etc/rabbitmq/conf/key.pem"},
               {verify,verify_peer},
               {fail_if_no_peer_cert,false}]}
```

비고

※ SSL 활성화 시, SSL 포트 2개가 활성화되므로 Producer에서 SSL 포트를 사용해야 함

Mnesia 데이터베이스 디렉터리 및 파일 권한 설정

항목설명

RabbitMQ는 Erlang 언어로 제작되어 있으며 Mnesia 데이터베이스를 사용한다. Mnesia 데이터베이스에는 RabbitMQ 계정, 패스워드, 권한 등을 저장하며 파일 형태로 관리가 이루어진다. 만약 비인가자에 의해 데이터베이스 파일이 변조 또는 삭제될 경우 계정정보가 매칭되지 않으므로 서비스에 악영향을 끼칠 수 있다. 이를 방지하기 위해 Mnesia 데이터베이스 디렉터리 및 파일 권한에 other 권한을 제거해 비인가자에 의한 데이터베이스 파일의 변조 및 삭제를 막을 수 있다.

진단 기준

양호

Mnesia 데이터 디렉터리 및 파일 권한에 Other 쓰기 권한이 존재하지 않을 경우

취약

Mnesia 데이터 디렉터리 및 파일 권한에 Other 쓰기 권한이 존재할 경우

진단 방법

■ Mnesia 데이터 디렉터리 및 파일 권한 조회

1) # ls -l /[Mnesia 데이터 디렉터리] 권한 조회

```
[root@localhost ~]# ls -ld /var/lib/rabbitmq/mnesia/rabbit@localhost
drwxr-xr-x. 4 rabbitmq rabbitmq 4096 10월  22 09:39 /var/lib/rabbitmq/mnesia/rabbit@localhost
```

2) # ls -l /[Mnesia 데이터 디렉터리]/ 데이터 파일 권한 조회

```
[root@localhost ~]# ls -l /var/lib/rabbitmq/mnesia/rabbit@localhost
합계 88
-rw-r--r--. 1 rabbitmq rabbitmq   154 10월  22 09:39 DECISION_TAB.LOG
-rw-r--r--. 1 rabbitmq rabbitmq    93 10월  22 09:39 LATEST.LOG
-rw-r--r--. 1 rabbitmq rabbitmq    41 10월  18 17:52 cluster_nodes.config
drwxr-xr-x. 2 rabbitmq rabbitmq    18 10월  18 17:52 msg_store_persistent
drwxr-xr-x. 2 rabbitmq rabbitmq    18 10월  18 17:52 msg_store_transient
-rw-r--r--. 1 rabbitmq rabbitmq    20 10월  18 17:52 nodes_running_at_shutdown
-rw-r--r--. 1 rabbitmq rabbitmq  1115 10월  18 11:09 rabbit_durable_exchange.DCD
-rw-r--r--. 1 rabbitmq rabbitmq     8 10월  18 11:07 rabbit_durable_queue.DCD
-rw-r--r--. 1 rabbitmq rabbitmq     8 10월  18 11:07 rabbit_durable_route.DCD
-rw-r--r--. 1 rabbitmq rabbitmq   159 10월  18 13:31 rabbit_runtime_parameters.DCD
-rw-r--r--. 1 rabbitmq rabbitmq     4 10월  18 17:52 rabbit_serial
-rw-r--r--. 1 rabbitmq rabbitmq   257 10월  22 09:39 rabbit_user.DCD
-rw-r--r--. 1 rabbitmq rabbitmq   187 10월  18 11:09 rabbit_user_permission.DCD
-rw-r--r--. 1 rabbitmq rabbitmq   425 10월  22 09:27 rabbit_user_permission.DCL
-rw-r--r--. 1 rabbitmq rabbitmq   128 10월  18 11:09 rabbit_vhost.DCD
-rw-r--r--. 1 rabbitmq rabbitmq  5464 10월  18 17:52 recovery.dets
-rw-r--r--. 1 rabbitmq rabbitmq 21173 10월  18 11:09 schema.DAT
-rw-r--r--. 1 rabbitmq rabbitmq   272 10월  18 11:07 schema_version
```

조치 방법

■ 패스워드 관련 파일 권한 변경

1) # chmod o-w /Mnesia 데이터 디렉터리 명령어를 통해 Other 쓰기 권한 제거
2) # cd /Mnesia 데이터 디렉터리 이동 후 해당 디렉터리의 파일에 Other 쓰기 권한 제거

설정 파일 권한 설정

항목설명

RabbitMQ 환경설정 파일의 Other에 쓰기 권한이 존재할 경우 비인가자가 RabbitMQ의 설정을 변경하여 시스템 장애를 유발할 수 있다. 이러한 문제점을 해결하기 위해 RabbitMQ 환경설정 파일의 Other에 쓰기 권한을 제거하여 비인가자에 의한 피해를 최소화할 수 있다.

진단 기준

양호

설정 파일의 Other에 쓰기 권한이 존재하지 않는 경우

취약

설정 파일의 Other에 쓰기 권한이 존재하는 경우

진단 방법

■ 설정 파일 권한 조회

1) # ls –l /[RabbitMQ 설치 디렉터리]

```
root@ubuntu:/etc/rabbitmq# ls -l /etc/rabbitmq
합 계  8
-rw-r--r-- 1 root     root      23 11월  13 14:39 enabled_plugins
-rw-r--r-- 1 rabbitmq rabbitmq 535 11월  13 14:37 rabbitmq-env.conf
```

조치 방법

■ Other의 쓰기 권한 제거

1) # chmod 640 'RabbitMQ 설정파일'

예시)

```
root@ubuntu:/etc/rabbitmq# chmod 640 rabbitmq-env.conf
root@ubuntu:/etc/rabbitmq# ls -l rabbitmq-env.conf
-rw-r----- 1 rabbitmq rabbitmq 535 11월  13 14:37 rabbitmq-env.conf
root@ubuntu:/etc/rabbitmq#
```

로그 활성화

항목설명

로그를 정기적으로 분석하여 침입유무를 파악하고, 침입 시도 의심 사례를 분석하여 사전에 해당 장비에 대한 접근을 차단하는 등 체계적인 로그 관리 작업이 이루어져야 한다.

진단 기준

양호

로그가 활성화되어 있는 경우

취약

로그가 비활성화되어 있는 경우

진단 방법

■ 설정 파일에서 로그 설정 확인

1) # [RabbitMQ설치 디렉터리]/rabbitmqctl report | grep logger

```
root@ubuntu:/etc/rabbitmq# rabbitmqctl report | grep logger
      {logger,
          [{handler,default,logger_std_h,
                    {logger_formatter,
      {logger_level,notice},
      {logger_sasl_compatible,false},
      {logger,
                #{formatter => {logger_formatter,#{template => [msg]}}}}]},
 {syslog,["logger","[]"]},
 {syslog,["syslog_error_logger","false"]}]
root@ubuntu:/etc/rabbitmq#
```

조치 방법

■ 설정 파일에서 로그 설정

1) # vi [RabbitMQ 설치 디렉터리]/rabbitmq-env.conf

예시)

```
#NODENAME=rabbit
NODENAME=TEST
CONFIG_FILE = /TEST/data/rabbitmq/test
MNESIA_BASE = /TEST/data/rabbitmq
LOG_BASE = /TEST/log/rabbitmq

# By default RabbitMQ will bind to all interfaces
```

비고

※ RabbitMQ 설치 시 Default로 로그가 활성화되어 있으며 rabbitmq-env.conf에서 log.file = false로 설정하면 로그가 비활성화됨

최신 보안 패치 적용

항목설명

최신 보안 패치를 적용하지 않으면 해당 버전의 취약점으로 인해 침해사고가 발생할 수 있으므로 주기적으로 공식 릴리즈 사이트를 방문하여 보안 패치를 적용해야 한다.

진단 기준

양호

최신 보안 패치를 적용한 경우

취약

최신 보안 패치를 적용한 하지 않은 경우

진단 방법

■ RabbitMQ 버전 조회

1) [RabbitMQ 설치 디렉터리] # rabbitmqctl status | grep “RabitMQ version”

```
root@ubuntu:/etc/rabbitmq# rabbitmqctl status | grep "RabbitMQ"
RabbitMQ version: 3.9.13
root@ubuntu:/etc/rabbitmq#
```

조치 방법

■ RabbitMQ 사이트를 통해 주기적으로 버전 점검을 하도록 하며 최신 보안 패치 적용 시 충분한 테스트 후 적용 권고

※ 최신 버전을 사용하도록 권고하고 있으나 시스템 운영상 적용이 어려운 경우 최신이 아닌 취약점이 존재하지 않는 버전도 허용하고 있음

2.32.

Node.js

2.32. Node.js

보안설정(4개 항목), 로그 및 패치 관리(3개 항목) 총 2개 영역에서 7개 항목으로 구성된다.

[표 32] Node.js 진단 체크리스트

구분	진단 항목
가. 보안 설정	node 프로세스 권한 제한
	헤더 정보 노출 방지
	오류 메시지 설정
	로그 디렉터리 및 파일 권한 설정
나. 로그 및 패치 관리	로그 포맷 설정
	로그 파일 보관 및 주기적 백업
	최신 보안 패치 적용

node 프로세스 권한 제한

항목설명

Node 애플리케이션이 root 권한으로 구동될 경우 공격자가 애플리케이션의 에러나 버그를 악용하여 전체 시스템을 작동 불능상태에 빠뜨릴 수 있으므로 Node 애플리케이션이 root 권한으로 구동되지 않도록 관리해야 한다.

진단 기준

양호

Node 애플리케이션이 전용 계정으로 구동 중이며, production 모드로 설정된 경우

취약

Node 애플리케이션이 root 권한으로 구동 중이거나, development 모드로 설정된 경우

진단 방법

■ 프로세스 권한 확인

1) # ps –ef | grep node | grep –v grep

```
[root@localhost www]# ps -ef | grep node | grep -v grep
root      49019  49009  0 10:29 pts/1    00:00:00 node ./bin/www dev
[root@localhost www]#
```

■ production 모드 확인

1) # app.js | grep “process.env.NODE_ENV”

※ 참고) Express Framework

모드	설명
production	파일 캐싱, 에러 메시지 감추기 등 배포에 적합한 환경
development	파일 캐싱 방지, 디버그를 위한 상세한 에러 메시지 보이기 등 개발에 적합한 환경

조치 방법

■ root 계정 이외의 계정으로 node 프로세스 실행

1) # set DEBU=www & npm start dev

■ production 모드로 변경

1) # export NODE_ENV=production

헤더 정보 노출 방지

항목설명

HTTP 요청에 대한 응답 헤더에 서버의 이름, 버전 등의 정보를 제공하는 경우, 공격자가 해당 정보를 이용하여 공격에 이용할 수 있다.

진단 기준

양호

헤더 정보 노출 방지 설정이 적용된 경우

취약

헤더 정보 노출 방지 설정이 적용되어 있지 않은 경우

진단 방법

■ node 메인 파일에서 헤더 정보 노출 설정 확인

예시)

1) # cat app.js

```
[root@localhost www]# cat app.js | grep powered
app.disable("x-powered-by");
[root@localhost www]#
```

조치 방법

■ node 메인 파일에 헤더 정보 노출 설정 추가

예시)

1) # vi app.js

```
app.use(logger('dev'));
app.use(express.json());
app.use(express.urlencoded({ extended: false }));
app.use(cookieParser());
app.use(express.static(path.join(__dirname, 'public')));
app.disable("x-powered-by");
```

오류 메시지 설정

항목설명

대상 시스템의 정보를 획득하기 위해 고의로 다양한 에러를 유발하여 노출되는 오류 메시지를 통해 웹 프로그램의 구조 및 환경설정을 추정할 수 있다. 필수 에러 코드(400,401,403,404,500)에 대하여 그 내용을 알 수 없도록 일원화된 오류 메시지로 관리하여야 한다.

진단 기준

양호

필수 에러 코드를 유추 불가능하도록 일원화된 오류 메시지를 생성한 경우

취약

필수 에러 코드를 유추 불가능하도록 일원화된 오류 메시지를 생성하지 않은 경우

진단 방법

■ 오류 메시지 설정 확인

예시)

1) # cat app.js

```
app.use(cookieParser());
app.use(express.static(path.join(__dirname, 'public')));

app.use('/', indexRouter);
app.use('/users', usersRouter);

// catch 404 and forward to error handler
app.use(function(req, res, next) {
  next(createError(404));
});

// error handler
app.use(function(err, req, res, next) {
  // set locals, only providing error in development
  res.locals.message = err.message;
  res.locals.error = req.app.get('env') === 'development' ? err : {};

  // render the error page
  res.status(err.status || 500);
  res.render('error');
});

module.exports = app;
```

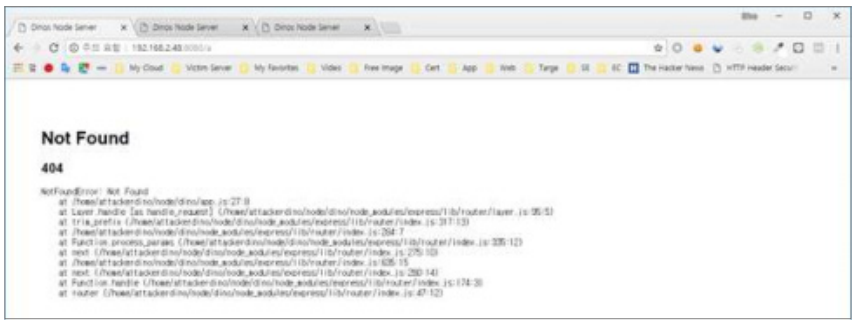
cat views/error.jade

```
extends layout

block content
  h1= message
  h2= error.status
  pre #{error.stack}
```

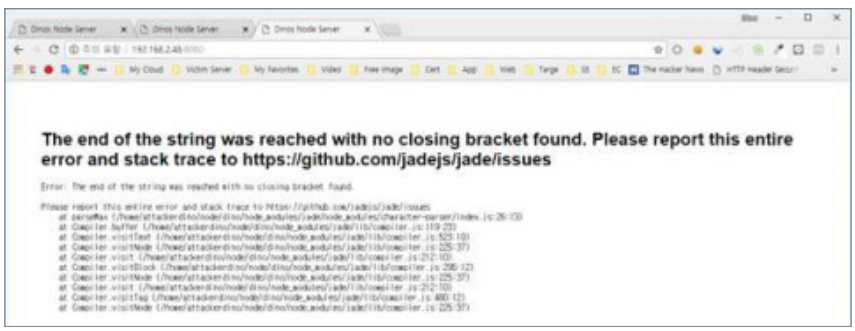
■ 웹 사이트에서 표시되는 오류 메시지 확인

예시)

1) 404 에러 코드 오류 메시지



2) 500 에러 코드 오류 메시지



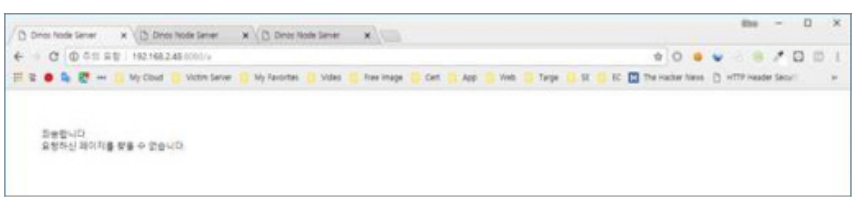
조치 방법

■ 일원화된 오류 메시지 설정

예시)

1) # vi views/error/jade

■ 에러 내용을 알 수 없는 일원화된 오류 메시지



로그 디렉터리 및 파일 권한 설정

항목설명

로그 파일에는 공격자에게 유용한 정보가 들어있어 권한 관리가 필요하므로 일반 사용자에 의한 정보 유출이 불가능하도록 설정을 강화해야 한다.

진단 기준

양호

로그 디렉터리 및 파일의 소유자가 node 전용 계정이고 디렉터리는 750(-rwxr-x---), 파일은 640(-rw-r-----) 이하인 경우

취약

로그 디렉터리 및 파일의 소유자가 root 계정이거나 디렉터리는 750(-rwxr-x---), 파일은 640(-rw-r-----) 초과인 경우

진단 방법

■ 로그 디렉터리 및 로그 파일 접근 권한 확인

1) # ls -ld [node 애플리케이션 로그 디렉터리]

예시)

```
[root@localhost www]# ls -ld log
drwxr-xr-x. 2 root root 20  9월  5 13:43 log
```

2) # ls -ld [node 애플리케이션 로그 파일]

```
[root@localhost www]# ls -l log
합 계 4
-rw-r--r--. 1 root root 1101  9월  5 14:55 app.log
```

조치 방법

■ 로그 디렉터리 및 로그 파일 접근 권한 변경

1) 로그 디렉터리 접근 권한 변경
   # chown nodeLnode [node 애플리케이션 로그 디렉터리]
   # chown 750 [node 애플리케이션 로그 디렉터리]

■ 로그 파일 접근 권한 변경

chown node:node [node 애플리케이션 로그 파일]
chmod 640 [node 애플리케이션 로그 디렉터리]

로그 포맷 설정

항목설명

로그 포맷을 설정하지 않으면 공격 여부 파악, 공격자 사용 툴 파악, 공격자 위치 파악이 불가능하므로 반드시 로그 포맷을 설정해야 한다.

진단 기준

양호

로그 포맷 설정값이 default(또는 combined)이거나 그에 준하는 포맷 토큰 조합으로 설정된 경우

취약

로그 포맷 설정값이 default(또는 combined)가 아니거나 그에 준하는 포맷 토큰 조합으로 설정되어 있지 않은 경우

진단 방법

■ 실시간 콘솔 로그 설정 확인

예시)

Express의 Morgan 모듈을 사용하는 경우

cat app.js

```
var createError = require('http-errors');
var express = require('express');
var path = require('path');
var cookieParser = require('cookie-parser');
var logger = require('morgan');

var indexRouter = require('./routes/index');
var usersRouter = require('./routes/users');

var app = express();

// view engine setup
app.set('views', path.join(__dirname, 'views'));
app.set('view engine', 'jade');

app.use(logger('dev'));
app.use(express.json());
app.use(express.urlencoded({ extended: false }));
app.use(cookieParser());
app.use(express.static(path.join(__dirname, 'public')));

app.use('/', indexRouter);
app.use('/users', usersRouter);
"app.js" 41L, 1075C
```

2) 로그 파일 저장 여부 확인

예시)

Express의 Morgan 모듈을 사용하는 경우

cat app.js

```
//log
var fs = require('fs');

var indexRouter = require('./routes/index');
var usersRouter = require('./routes/users');

var app = express();

// view engine setup
app.set('views', path.join(__dirname, 'views'));
app.set('view engine', 'jade');

app.use(logger('dev'));
app.use(express.json());
app.use(express.urlencoded({ extended: false }));
app.use(cookieParser());
app.use(express.static(path.join(__dirname, 'public')));
app.disable("x-powered-by");

app.use('/', indexRouter);
app.use('/users', usersRouter);

//log
app.use(logger({
  format: 'default',
  stream: fs.createWriteStream('./log/app.log', {'flags': 'w'})
}));
```

조치 방법

■ 실시간 콘솔 로그 설정

예시)

Express의 Morgan 모듈을 사용하는 경우

1) # vi app.js
   var logger = require('morgan');
   ... 중간 생략 ...
   app.use(logger('combined'))

■ 로그 파일 저장 설정

예시)

Express의 Morgan 모듈을 사용하는 경우

1) # vi app.js
   var fs = require('fs');
   ... 중간 생략 ...
   app.use(logger({ format: 'default', stream: fs.createWriteStream('./log/app.log',
   {'flags': 'w'})
   }));

비고

※ morgan이 지원하는 로그 포맷
- default : 표준 combined 로그 출력
- short : 표준 common 로그 출력
- dev : 개발을 위해 response에 따라 색상이 입혀진 축약 로그 출력
- tiny : 최소화된 로그 출력

로그 파일 보관 및 주기적 백업

항목설명

로그 파일은 '정보통신망 이용 촉진 및 정보보호 등에 관한 법률' 등 관련 법률 및 사내 정보보호 정책과 지침에 따라 로그 파일의 저장 기간을 규정 및 준수하여야 한다. 로그 정보는 침해사고 발생 시 해킹의 흔적 및 공격기법을 확인할 수 있는 중요 자료로 이용할 수 있으며 정기적인 로그 분석을 통하여 시스템 침입 흔적과 취약점을 확인할 수 있으므로 주기적인 백업이 필요하다.

진단 기준

양호

로그 보관 주기를 준수하고 주기적으로 백업을 수행하고 있는 경우

취약

로그 보관 주기를 준수하지 않거나 주기적으로 백업이 수행되고 있지 않은 경우

진단 방법

■ 로그 보관주기

1) 로그 보관 및 관리 정책 수립 여부를 확인
2) 주기적인 로그 파일 백업 수행 여부 확인

조치 방법

■ 사용자 접속 기록 보관 기간은 '정보통신망 이용 촉진 및 정보보호 등에 관한 법률', '개인정보보호법'등 관련 법률에 근거하여 보관하여야 함

1) 개인정보 처리 시스템인 경우
   접속 기록 보관 주기 : 1년 이상(5만 명 이상의 정보 주체에 관하여 개인정보를 처리하거나, 민감 정보를 처리하는 경우에는 2년 이상)
   접속 기록에 대한 주기적 점검 : 월 1회 이상
   백업 수행 주기 : 개인정보 처리 시스템 외의 별도 저장 장치에 상시로 접속 기록 백업
   백업 보관 주기 : 관련 사항 없음(재해복구 관점 고려)
2) 로그 백업 정책에 따라 로그 파일을 정기적으로 백업을 수행

비고

※ 적용 시 운영자 협의 필요

최신 보안 패치 적용

항목설명

최신 보안 패치를 적용하지 않으면 해당 버전의 취약점으로 인해 침해사고가 발생할 수 있으므로 주기적으로 공식 릴리즈 사이트를 방문하여 보안 패치를 적용해야 한다.

진단 기준

양호
최신 보안 패치를 적용한 경우

취약
최신 보안 패치를 적용하지 않은 경우

진단 방법

■ Node 버전 확인

1) RPM 설치
rpm –qa | grep nodejs

```
[root@localhost bin]# rpm -qa | grep nodejs
nodejs-8.11.4-1nodesource.x86_64
```

2) Source 설치
node –v

```
[root@localhost bin]# node -v
v8.11.4
```

■ NPM 버전 확인

npm –v

■ Express 버전 확인

express ––version

조치 방법

■ Node.js 사이트를 통해 주기적으로 버전 점검을 하도록 하며 최신 보안 패치 적용 시 충분한 테스트 후 적용

■ NPM 최신 보안 패치 업데이트

1) npm 업데이트
npm install –g npm

2) 업데이트 후 npm 버전 확인

```
[root@localhost bin]# npm -v
6.4.1
```

■ Express 최신 버전 업데이트

npm install express

비고

※ 최신 버전을 사용하도록 권고하고 있으나 시스템 운영상 적용이 어려운 경우 최신이 아닌 취약점이 존재하지 않는 버전도 허용하고 있음

2.33.

Ceph

2.33. Ceph

파일 및 디렉터리 권한(3개 항목), 보안 설정(3개 항목), 패치 관리(1개 항목) 총 3개 영역에서 7개 항목으로 구성된다.

[표 33] Ceph 진단 체크리스트

구분	진단 항목
가. 파일 및 디렉터리 권한	Keyring 파일 소유자 및 권한 확인
	SSH 인증키 파일 관리
	Ceph 설정 파일 소유자 및 권한 확인
나. 보안 설정	Ceph 인증 프로토콜 적용
	root 이외의 관리자 계정 사용
	Selinus 활성화
나. 패치 관리	최신 보안 패치 적용

Keyring 파일 소유자 및 권한 확인

항목설명

Keyring 파일은 인증 정보(패스워드, 권한)가 저장되어 있는 파일이다. 만약 해당 파일에 Other 권한이 존재할 경우 비인가자가 Keyring 파일을 수정하여 시스템 장애를 발생시키거나 인증 정보를 탈취하여 Ceph 시스템에 접속한 후 중요 정보를 열람, 수정, 삭제할 가능성이 존재한다.

진단 기준

양호

Keyring 파일 소유자가 root 또는 관리자 계정이고, 권한이 400(-r--------)으로 설정된 경우

취약

Keyring 파일 소유자가 root 또는 관리자 계정이고, 권한이 400(-r--------)으로 설정되어 있지 않은 경우

진단 방법

■ Keyring 소유자 및 파일 권한 확인

1) # ls [keyring 파일 디렉터리]/keyring 파일

예시)

ls –l /etc/ceph/*.keyring

```
File  Edit  View  Search  Terminal  Help
[root@mgmt ~]# ls -l /etc/ceph/*.keyring
-rw------- 1 ceph ceph 151 Jan  5 21:11 /etc/ceph/ceph.client.admin.keyring
-rw-r--r-- 1 ceph ceph  61 Jan  5 21:14 /etc/ceph/ceph.mgr.admin.keyring
-rw------- 1 ceph ceph 357 Jan  5 21:12 /etc/ceph/ceph.mon.keyring
[root@mgmt ~]#
```

조치 방법

■ Keyring 소유자 및 파일 권한 변경

1) # chown root:root [keyring 파일 디렉터리]/keyring 파일
2) # chmod 400 [keyring 파일 디렉터리]/keyring 파일

SSH 인증키 파일 관리

항목설명

Ceph는 중앙 Management 서버에서 ssh를 이용해 노드들의 설정 변경과 배포를 할 수 있다. 이때 패스워드가 아닌 키를 생성하여 사용하게 되는데, 키는 파일에 기록되어 있다. 만약 비인가자가 키 파일을 수정할 경우 시스템에 장애가 발생할 가능성이 있다.

진단 기준

양호

.ssh 디렉터리 권한이 700(-rwx------)이고 SSH 키 파일에 Other 쓰기 권한이 없는 경우

취약

.ssh 디렉터리 권한이 700(-rwx------)이 아니거나 SSH 키 파일에 Other 쓰기 권한이 있는 경우

진단 방법

■ SSH 디렉터리 권한 확인

1) # ls –ld ~/.ssh

```
[root@mgmt ~]# ls -ld ~/.ssh
drwx------. 2 root root 94 Jan  5 21:06 /root/.ssh
[root@mgmt ~]#
```

■ SSH 키 파일 권한 확인

1) # ls –l ~/.ssh

```
[root@mgmt ~]# ls -l ~/.ssh
total 20
-rw-------. 1 root root 1143 Jan  5 20:44 authorized_keys
-rw-------  1 root root   75 Jan  5 21:06 config
-rw-------. 1 root root 2590 Jan  5 20:43 id_rsa
-rw-r--r--. 1 root root  563 Jan  5 20:43 id_rsa.pub
-rw-r--r--. 1 root root  518 Jan  5 20:44 known_hosts
[root@mgmt ~]#
```

조치 방법

■ .ssh 디렉터리 권한 변경

1) # chmod 700 ~/.ssh

■ ssh 키 파일 권한 변경

1) # chmod 600 ~/.ssh/키 파일

Ceph 설정 파일 소유자 및 권한 확인

항목설명

Ceph 설정 파일을 비인가자가 수정 가능할 경우 시스템 장애가 발생할 가능성이 존재한다.

진단 기준

양호

Ceph 설정 파일 Other 권한에 쓰기 권한이 존재하지 않을 경우

취약

Ceph 설정 파일 Other 권한에 쓰기 권한이 존재할 경우

진단 방법

■ Ceph 설정 파일 권한 확인

1) # ls -l [Ceph 설정 디렉터리]/ceph.conf

```
[root@mgmt ~]# ls -l /etc/ceph/ceph.conf
-rw-r--r-- 1 ceph ceph 574 Jan  5 21:11 /etc/ceph/ceph.conf
[root@mgmt ~]#
```

조치 방법

■ Ceph 설정 파일 권한 변경

1) # chmod o-w [Ceph 설정 디렉터리]/ceph.conf

Ceph 인증 프로토콜 적용

항목설명

Ceph는 CEPHX 프로토콜을 사용해 인증하며, 만약 인증을 사용하지 않을 경우, man-in-the middle 공격을 받아 시스템 장애가 발생하거나 비인가자가 스토리지에 접근하여 중요 정보를 탈취할 가능성이 존재한다.

진단 기준

양호

Ceph 인증 프로토콜을 사용하는 경우

취약

Ceph 인증 프로토콜을 사용하지 않는 경우

진단 방법

■ CEPHX 프로토콜 사용 여부 확인

1) # cat [Ceph 설정 디렉터리]/ceph.conf

```
[root@mgmt ~]# cat /etc/ceph/ceph.conf
[global]
# specify cluster network for monitoring
cluster network = 172.16.0.0/24
# specify public network
public network = 172.16.0.0/24
# specify UUID genarated above
fsid = 50568499-f303-4d44-977a-1cd29a706def
# specify IP address of Monitor Daemon
mon host = 172.16.0.180
# specify Hostname of Monitor Daemon
mon initial members = node01
osd pool default crush rule = -1
```

조치 방법

■ 설정 파일에서 [global] 영역에 CEPHX 프로토콜 적용

1) # vi [Ceph 설정 디렉터리]/ceph.conf

```
[global]
# specify cluster network for monitoring
cluster network = 172.16.0.0/24
# specify public network
public network = 172.16.0.0/24
# specify UUID genarated above
fsid = 50568499-f303-4d44-977a-1cd29a706def
# specify IP address of Monitor Daemon
mon host = 172.16.0.180
auth_cluster_required = cephx
auth_service_required = cephx
auth_client_required = cephx
# specify Hostname of Monitor Daemon
mon initial members = node01
osd pool default crush rule = -1
```

root 이외의 관리자 계정 사용

항목설명

Ceph 설정 및 배포는 root 권한이 필요하다. root 계정을 사용할 경우, ssh의 root 계정 접속 금지 설정 등을 적용할 수 없어 root 계정이 외부로 노출될 수 있다. 따라서 root 권한을 가진 별도의 계정을 생성하여 Ceph를 설정 및 배포해야 한다.

진단 기준

양호

별도의 관리자 계정을 사용하는 경우

취약

root 계정을 통해 Ceph를 관리하는 경우

진단 방법

■ 관리자 계정 생성 여부 확인

1) # cat /etc/sudoers

```
## The COMMANDS section may have other options added to it.
##
## Allow root to run any commands anywhere
root    ALL=(ALL)       ALL

## Allows members of the 'sys' group to run networking, software,
## service management apps and more.
# %sys ALL = NETWORKING, SOFTWARE, SERVICES, STORAGE, DELEGATING,
ATE, DRIVERS
```

조치 방법

■ 별도의 관리자 계정 생성

예시)

1) 계정 생성
   # useradd admin

```
[root@mgmt ~]# useradd admin
[root@mgmt ~]#
```

2) 생성된 계정에 관리자 계정 부여
   # chmod 660 /etc/sudoers 명령어를 통해 sudoers 파일 쓰기 권한 부여
   # vi /etc/sudoers 명령어 입력 후 아래와 같이 작성

```
## Allow root to run any commands anywhere
root    ALL=(ALL)       ALL
admin   ALL=(ALL)       ALL
```

   # chmod 440 /etc/sudoers 명령어를 통해 sudoers 파일 쓰기 권한 제거

비고

※ ceph 계정은 ceph 구동에 사용되는 계정이므로 ceph 이름을 제외한 다른 이름의 관리자 계정을 생성해야 함

Selinux 활성화

항목설명

SELinux는 Linux의 보안 모듈로 신뢰할 수 없는 입력으로부터 프로세스를 보호하고, 데이터의 기밀성, 무결성을 강화할 때 사용된다. Ceph가 설치된 서버에 SELinux를 활성화하여 권한 상승 공격 등을 방어할 수 있다.

진단 기준

양호

SELinux가 활성화된 경우

취약

SELinux가 비활성화된 경우

진단 방법

■ SELinux 활성화 여부 확인

1) # getenforce

```
[root@mon ~]# getenforce
Disabled
[root@mon ~]#
```

조치 방법

■ SELinux 활성화

1) # vi /etc/selinux/config

```
# This file controls the state of SELinux on the system.
# SELINUX= can take one of these three values:
#     enforcing - SELinux security policy is enforced.
#     permissive - SELinux prints warnings instead of enforcing.
#     disabled - No SELinux policy is loaded.
SELINUX=enforcing
# SELINUXTYPE= can take one of these three values:
#     targeted - Targeted processes are protected,
#     minimum - Modification of targeted policy. Only selected processes are pro
tected.
#     mls - Multi Level Security protection.
SELINUXTYPE=targeted
```

최신 보안 패치 적용

항목설명

최신 보안 패치를 적용하지 않으면 해당 버전의 취약점으로 인해 침해사고가 발생할 수 있으므로 주기적으로 공식 릴리즈 사이트를 방문하여 보안 패치를 적용해야 한다.

진단 기준

양호

최신 보안 패치 업데이트를 적용한 경우

취약

최신 보안 패치 업데이트를 적용하지 않은 경우

진단 방법

■ Ceph 버전 확인

1) # ceph -v

```
[root@mgmt ~]# ceph -v
ceph version 15.2.8 (bdf3eebcd22d7d0b3dd4d5501bee5bac354d5b55) octopus (stable)
[root@mgmt ~]#
```

조치 방법

■ 최신 보안 패치 적용

1) 최신 보안 패치 업데이트가 발표되었을 경우, 시스템 영향도를 파악하여 충분한 테스트를 진행한 후 적용 권고

※ 최신 버전을 사용하도록 권고하고 있으나 시스템 운영상 적용이 어려운 경우 최신이 아닌 취약점이 존재하지 않는 버전도 허용하고 있음

2.34.

Hadoop

2.34. Hadoop

파일 및 디렉터리 권한(1개 항목), 파일 및 서비스(1개 항목), 보안 설정(5개 항목), 패치 및 로그 관리(2개 항목) 총 4개 영역에서 9개 항목으로 구성된다.

[표 34] Hadoop 진단 체크리스트

구분	진단 항목
가. 파일 및 디렉터리 권한	로컬 파일 시스템/HDFS 디렉터리 소유자 및 권한 설정
나. 파일 및 서비스 관리	커버로스 인증 시 클러스터의 모든 시스템에서 YARN User 키 테이블/맵리듀스 User 키 테이블 파일 권한 설정
다. 보안 설정	Hadoop Security 활성화
	하둡 ACL 설정
	WebHDFS 비활성화
	RPC 암호화
	데이터 전송 암호화
라. 패치 및 로그 관리	로그 검토 및 관리
	최신 보안 패치 적용

로컬 파일 시스템/HDFS 디렉토리 소유자 및 권한 설정

항목설명

파일에 과도한 사용자 권한이 존재할 경우, 비인가 된 사용자가 해당 파일에 접근하여 HDFS 등 하둡 관련 정보를 수집하여 2차적인 공격에 사용될 위험이 존재한다.

진단 기준

양호

로컬 파일 시스템/HDFS 소유자와 권한이 조치 방법과 같이 설정되어 있는 경우

취약

로컬 파일 시스템/HDFS 소유자가 권한이 조치 방법보다 과도하게 설정되어 있는 경우

진단 방법

■ 로컬 파일 시스템/HDFS 디렉토리 권한 확인

1) hdfs dfs –ls [PATH]

또는

2) # ./bin/hadoop fs –ls [파일명]

```
[hadoop@localhost ~]$ hdfs dfs -ls /data/dfs
2020-09-14 01:57:01,144 WARN util.NativeCodeLoader: Unable to load native-hadoop library for your pl
atform... using builtin-java classes where applicable
Found 1 items
drwxr-xr-x   - hadoop supergroup          0 2020-09-14 01:46 /data/dfs/name
```

조치 방법

■ 로컬 파일 시스템 (예시)

// dfs.namenode.name.dir = hdfs:hadoop (700)

1) # chown –R hdfs:hadoop /home/hadoop/data/dfs/name

2) # chmod 700 /home/hadoop/data/dfs/name

```
[hadoop@localhost ~]$ hdfs dfs -chown -R hadoop:hdfs /data/dfs/name
2020-09-14 02:29:50,918 WARN util.NativeCodeLoader: Unable to load native-hadoop library for your pl
atform... using builtin-java classes where applicable
[hadoop@localhost ~]$ hdfs dfs -chmod 700 /data/dfs/name
2020-09-14 02:30:11,515 WARN util.NativeCodeLoader: Unable to load native-hadoop library for your pl
atform... using builtin-java classes where applicable
[hadoop@localhost ~]$ hdfs dfs -ls /data/dfs
2020-09-14 02:30:20,639 WARN util.NativeCodeLoader: Unable to load native-hadoop library for your pl
atform... using builtin-java classes where applicable
Found 1 items
drwx------   - hadoop hdfs          0 2020-09-14 02:27 /data/dfs/name
[hadoop@localhost ~]$
```

// dfs.namenode.data.dir = hdfs:hadoop (700)
3) # chown –R hdfs:hadoop /home/hadoop/data/dfs/data
4) # chmod 700 /home/hadoop/data/dfs/data

// dfs.journalnode.edits.dir = hdfs:hadoop (700)
5) # chown –R hdfs:hadoop /home/hadoop/data/dfs/journalnode
6) # chmod 700 /home/hadoop/data/dfs/journalnode

// $HADOOP_LOG_DIR = hdfs:hadoop (775)
7) # chown –R hdfs:hadoop /home/hadoop/logs
8) # chmod 775 /home/hadoop/logs

// yarn.nodemanager.local-dirs = yarn:hadoop (755)
10) # chown –R yarn:hadoop /home/hadoop/data/yarn/nm-local-dir
11) # chmod 755 /home/hadoop/data/yarn/nm-local-dir

■ HDFS 디렉토리

1) / = hdfs:hadoop (775)
2) /home/hadoop/bin/hdfs dfs –chown hdfs:hadoop /
3) /home/hadoop/bin/hdfs dfs –chmod 755 /

4) /user = hdfs:hadoop (755)
5) /home/hadoop/bin/hdfs dfs –chown hdfs:hadoop /user
6) /home/hadoop/bin/hdfs dfs –chmod 755 /user

커버로스 인증 시 클러스터의 모든 시스템에서 YARN User 키 테이블/맵리듀스 User 키 테이블 파일 권한 설정

항목설명

하둡 서비스는 티켓을 얻기 위해 암호화된 로그인 사용이 불가능하다. 그러므로 사용자의 인증 자격 증명을 위하여 각 서비스 및 하위 서비스에 Kerberos와 관련 있는 사용자 키 테이블 파일을 통해 인증된 사용자만 접근이 가능하도록 설정하여야 한다.

진단 기준

양호

클러스터의 모든 시스템에 YARN User 키 테이블/맵리듀스 유저 키테이블의 권한이 400(-r--------) 이하이고 소유자가 해당 keytab의 소유자일 경우

취약

클러스터의 모든 시스템에 YARN User 키 테이블/맵리듀스 유저 키테이블의 권한이 400(-r--------) 초과이고 소유자가 root일 경우

진단 방법

■ 수동점검을 통해 직접 hadoop 안에 커버로스 관련 키 테이블이 존재하는지 확인

1) # ls –al [hadoop config 디렉토리] | grep *.keytab

조치 방법

■ root 외의 소유자로 지정, 권한은 400 이하로 설정 (예시)

```
# chown hdfs:hadoop hdfs.keytab
# chmod 400 hdfs.keytab
# chown yarn:hadoop yarn.keytab
# chmod 400 yarn.keytab
# chown mapred:hadoop mapred.keytab
# chmod 400 mapred.keytab
```

Hadoop Security 활성화

항목설명

하둡은 보안을 강화하기 위해 커버로스 프로토콜을 사용할 수 있다.

진단 기준

양호

커버로스가 enable(true) 되어 있는 경우

취약

커버로스가 disable(false) 되어 있는 경우

진단 방법

■ core-site.xml에 kerberos 설정 확인

1) # cat core-site.xml

```
hadoop@ubuntu:/usr/share/doc/util-linux/examples/hadoop-3.3.6/etc/hadoop$ cat core-site.xml
<?xml version="1.0" encoding="UTF-8"?>
<?xml-stylesheet type="text/xsl" href="configuration.xsl"?>
<!--
  Licensed under the Apache License, Version 2.0 (the "License");
  you may not use this file except in compliance with the License.
  You may obtain a copy of the License at

    http://www.apache.org/licenses/LICENSE-2.0

  Unless required by applicable law or agreed to in writing, software
  distributed under the License is distributed on an "AS IS" BASIS,
  WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied.
  See the License for the specific language governing permissions and
  limitations under the License. See accompanying LICENSE file.
-->

<!-- Put site-specific property overrides in this file. -->

<configuration>
</configuration>
```

조치 방법

■ core-site.xml에 kerberos 설정

1) core-site.xml 파일에 아래와 같은 설정 사항 추가
   # vi core-site.xml

```
<property>
        <name>hadoop.security.authentication</name>
        <value>keberos</value>
</property>
<property>
        <name>hadoop.security.authentication</name>
        <value>true</value>
</property>
```

하둡 ACL 설정

항목설명

인가되지 않은 사용자가 접근 가능하도록 설정하였을 경우 침해사고가 일어날 위험이 존재한다.

진단 기준

양호

인가된 계정 및 그룹만 접근 가능하도록 설정되어 있는 경우

취약

모두 접근이 가능하도록 설정되어 있는 경우

진단 방법

■ hadoop-policy.xml ACL 설정 확인

1) # cat hadoop-policy.xml | grep datanode.protocol.acl

```
<property>
  <name>security.client.datanode.protocol.acl</name>
  <value>*</value>
  <description>ACL for ClientDatanodeProtocol, the client-to-datanode protocol
  for block recovery.
  The ACL is a comma-separated list of user and group names. The user and
  group list is separated by a blank. For e.g. "alice,bob users,wheel".
  A special value of "*" means all users are allowed.</description>
</property>
```

※ security.datanode.protocol.acl 값 *로 설정되어 있으면 아무 곳에서나 접근이 가능하다는 의미이므로 취약

조치 방법

■ hadoop-policy.xml ACL 설정 적용

1) # vi hadoop-policy.xml
〈value〉 인가된 계정 및 그룹명 〈/value〉

```
<property>
  <name>security.client.datanode.protocol.acl</name>
  <value>*</value>
  <description>ACL for ClientDatanodeProtocol, the client-to-datanode protocol
  for block recovery.
  The ACL is a comma-separated list of user and group names. The user and
  group list is separated by a blank. For e.g. "alice,bob users,wheel".
  A special value of "*" means all users are allowed.</description>
</property>
```

※ 아무런 설정이 존재하지 않는 경우, default로 모두 접근 가능

WebHDFS 비활성화

항목설명

불필요한 서비스가 구동중일 경우 해당 포트가 활성화되어 공격루트로 이용될 위험이 존재한다,

진단 기준

양호

불필요한 WebHDFS가 구동 중이지 않을 경우

취약

불필요한 WebHDFS가 구동 중일 경우

진단 방법

■ hdfs-site.xml에서 확인

1) # cat hdfs-site.xml

조치 방법

■ WebHDFS를 사용하지 않는 경우 hdfs-site.xml에서 설정

1) # vi hdfs-site.xml

```
<property>
        <name>dfs.webdfs.enabled</name>
        <value>true</value>
</property>
```

비고

■ hdfs-site.xml에 설정이 존재하지 않을 경우

- default = true
- default port = 50070(namenode), 50075(datanode)

RPC 암호화

항목설명

하둡 클라이언트는 하둡 네임노드와 통신하기 위해 하둡 RPC를 이용한다. 하둡 RPC 메커니즘은 SASL 보안을 지원한다. SASL 암호화는 하둡 클라이언트와 네임노드 간의 통신을 보호하고 암호화한다.

진단 기준

양호

rpc 암호화 설정을 적용한 경우

취약

rpc 암호화 설정을 적용하지 않은 경우

진단 방법

■ core-site.xml 파일을 통해 암호화 설정 여부 확인

1) core-site.xml 확인
   # cat core-site.xml

```
<property>
        <name>hadoop.rpc.protection</name>
        <value>privacy</value>
</property>
```

조치 방법

■ core-site.xml 파일 rpc 암호화 설정

1) 아래와 같은 설정 사항 추가

```
<property>
        <name>hadoop.rpc.protection</name>
        <value>privacy</value>
</property>
```

비고

※ dfs.encrypt.data.transfer 속성 변경은 데이터 노드에서만 필요함

데이터 전송 암호화

항목설명

네임노드는 클라이언트에게 첫 블록을 읽고 쓰기 위한 데이터노드의 주소를 알려준다. 데이터의 전송에 이용되는 프로토콜이 DTP이다. 이 값이 네임노드와 모든 데이터노드에 설정되어 있으면 데이터가 암호화되어서 전송되며, 암호화 알고리즘도 설정할 수 있다.

진단 기준

양호

데이터 전송 암호화 설정이 적용되어 있는 경우

취약

데이터 전송 암호화 설정이 적용되어 있지 않은 경우

진단 방법

- hdfs-site.xml 파일에서 데이터 전송 암호화 활성화 확인
- hdfs-site.xml 파일에서 암호화 알고리즘 확인

  # cat hdfs-site.xml

조치 방법

- hdfs-site.xml 파일에서 암호화 설정 활성화

  1) 아래와 같은 설정 사항 추가

```
<property>
        <name>dfs.encrypt.data.transfer</name>
        <value>true</value>
</property>
```

- hdfs-site.xml 파일에서 암호화 알고리즘 설정

  1) 아래와 같은 설정 사항 추가

```
<property>
        <name>dfs.encrypt.data.transfer.cipher.suites</name>
        <value>AES/CTR/NoPadding</value>
</property>
<property>
        <name>dfs.encrypt.data.transfer.cipher.key.bitlength</name>
        <value>256</value>
</property>
```

※ 하둡 v2.6 이전

〈property〉
〈name〉dfs.encrypt.data.transfer.algorithm〈/name〉
〈value〉3des〈/value〉
〈/property〉

로그 검토 및 관리

항목설명

지속적으로 User 활동 및 서비스 활동 감사를 실시하여 보안 사고가 발생할 경우 책임 추적 및 원인 분석을 빠르고 효과적으로 수행할 수 있도록 하여야 한다.

진단 기준

양호

하둡의 로그를 기록하고 있는 경우

취약

하둡의 로그를 기록하고 있지 않은 경우

진단 방법

■ 각 구성 요소의 설정 파일에서 로그 파일 경로 확인

1) hdfs-site.xml에서 로그 파일 경로 확인 ex)

```
root@ubuntu:/# cat /usr/local/hadoop/etc/hadoop/hdfs-site.xml
<?xml version="1.0" encoding="UTF-8"?>
<?xml-stylesheet type="text/xsl" href="configuration.xsl"?>
<!--
  Licensed under the Apache License, Version 2.0 (the "License");
  you may not use this file except in compliance with the License.
  You may obtain a copy of the License at

    http://www.apache.org/licenses/LICENSE-2.0

  Unless required by applicable law or agreed to in writing, software
  distributed under the License is distributed on an "AS IS" BASIS,
  WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied.
  See the License for the specific language governing permissions and
```

```
<configuration>
 <property>
    <name>dfs.replication</name>
    <value>1</value>
  </property>
  <property>
    <name>dfs.name.dir</name>
    <value>file:///usr/local/hadoop/hadoop_data/hdfs/namenode</value>
  </property>
  <property>
    <name>dfs.data.dir</name>
    <value>file:///usr/local/hadoop/hadoop_data/hdfs/datanode</value>
  </property>
</configuration>
```

2) core-site.xml에서 로그 파일 경로 확인
3) yarn-site.xml에서로그 파일 경로 확인
4) mapred-site.xml에서 로그 파일 경로 확인

■ 해당 경로에 로그 파일이 기록되고 있는지 확인

조치 방법

■ 각 파일에 로그 파일 저장 경로를 지정하여 로그를 기록 및 검토

1) hdfs-site.xml에서 로그 파일 경로 설정
2) core-site.xml에서 로그 파일 경로 설정 확인
3) yarn-site.xml에서 로그 파일 경로 설정 확인
4) mapred-site.xml에서 로그 파일 경로 설정 확인

최신 보안 패치 적용

항목설명

최신 보안 패치 및 업데이트를 실시하지 않을 경우, 버전에 따른 잘 알려진 취약점이 존재하며, 해당 취약점을 통해 시스템이 장악될 위험이 존재한다.

진단 기준

양호

최신 보안 패치 및 업데이트를 적용한 경우

취약

최신 보안 패치 및 업데이트를 적용하지 않은 경우

진단 방법

■ Hadoop 버전 확인

1) # hadoop version

```
root@ubuntu:/usr/share/doc/util-linux/examples/hadoop-3.3.6/bin# ./hadoop version
Hadoop 3.3.6
Source code repository https://github.com/apache/hadoop.git -r 1be78238728da9266a4f88195058f08fd012bf9c
Compiled by ubuntu on 2023-06-18T08:22Z
Compiled on platform linux-x86_64
Compiled with protoc 3.7.1
From source with checksum 5652179ad55f76cb287d9c633bb53bbd
This command was run using /usr/share/doc/util-linux/examples/hadoop-3.3.6/share/hadoop/common/hadoop-common-3.3.6.jar
```

조치 방법

■ 보안 패치 적용

1) 보안 취약점이 존재하지 않는 버전으로 보안패치를 적용해야 함

※ 최신 버전을 사용하도록 권고하고 있으나 시스템 운영상 적용이 어려운 경우 최신이 아닌 취약점이 존재하지 않는 버전도 허용하고 있음

비고

※ 보안 패치를 적용할 경우, 시스템 영향도를 파악하여 충분한 테스트 후 적용 권고

2.35.

Network Device

2.35. Network Device

계정관리(3개 항목), 접근 관리(2개 항목), 패치 관리(1개 항목), 기능관리(6개 항목) 총 4개 영역에서 12개 항목으로 구성된다.

[표 35] Network Device 진단 체크리스트

구분	진단 항목
가. 계정 관리	패스워드 설정
	패스워드 복잡성 설정
	암호화된 패스워드 사용
나. 접근 관리	VTY접근(ACL) 설정
	Session Timeout 설정
다. 패치 관리	최신 보안 패치 및 벤더 권고사항 적용
라. 기능 관리	SNMP 서비스 확인
	SNMP community string 복잡성 설정
	SNMP ACL 설정
	SNMP 커뮤니티 권한 설정
	TFTP 서비스 차단
	사용하지 않는 인터페이스의 shutdown 설정

패스워드 설정

항목설명

원격에서 라우터를 관리할 때 사용하는 패스워드를 장비의 초기 설정 그대로 사용할 경우, 누구라도 라우터에 접근할 수 있다. 기본 패스워드는 인터넷상에서 검색을 통해 쉽게 접근할 수 있으므로, 패스워드를 반드시 설정하거나 변경한 후에 사용해야 한다.

진단 기준

양호

장비의 패스워드가 초기 패스워드가 아닌 별도의 패스워드로 설정되어 있는 경우

취약

장비의 패스워드가 초기 설정 그대로 설정되어 있는 경우

진단 방법

[CISCO]

■ 패스워드 설정 정보 확인

(config)# show running-config
line con 0
password 〈password〉
login
line vty 0 4
password 〈password〉
login

```
!
line con 0
!
line aux 0
!
line vty 0 4
 login
!
!
!
end
```

[Juniper]

■ 패스워드 설정 정보 확인

```
R1〉 show configuration
  system {
   root-authentication {
      encrypted-password "password";
      ## SECRET-DATA
   }
   login {
      user mims {
         full-name mims;
         uid 2000;
         class super-user;
         authentication {
            encrypted-password "password";
            ## SECRET-DATA
         }
```

조치 방법

[CISCO]

■ Privileged mode 암호화 설정

(config)# enable secret 〈패스워드〉

```
Router(config)#enable secret nobiz
```

■ vty 패스워드 설정

(config)# line vty 0 4
(config-line)# login
(config-line)# password 〈패스워드〉

```
Router(config)#line vty 0 4
Router(config-line)#login
% Login disabled on line 2, until 'password' is set
% Login disabled on line 3, until 'password' is set
% Login disabled on line 4, until 'password' is set
% Login disabled on line 5, until 'password' is set
% Login disabled on line 6, until 'password' is set
```

■ Console 패스워드 설정

(config)# line console 0
(config-line)# login
(config-line)# password 〈패스워드〉

```
Router(config-line)#line console 0
Router(config-line)#login
% Login disabled on line 0, until 'password' is set
Router(config-line)#password nobiz
```

[Juniper]

■ root 패스워드 설정

R1# set system root-authentication plain-text-password
New Password :
Retype new password:

```
root# set system root-authentication plain-text-password
New password:
Retype new password:
```

■ User 계정 패스워드 설정

R1# edit system login
R1# edit user 계정명
R1# set authentication plain-text-password
New Password :
Retype new password:

```
[edit]
root# edit system login

[edit system login]
root# edit user kseladmin

[edit system login user kseladmin]
root# set authentication plain-text-password
New password:
Retype new password:

[edit system login user kseladmin]
```

비고

※ default 설정은 패스워드가 설정되어 있지 않음

패스워드 복잡성 설정

항목설명

Console, VTY, AUX로 접속하여 enable 모드 접속 시 추측하기 쉬운 패스워드를 사용할 경우, 비인가자가 패스워드 추측을 통해 장비에 접속할 수 있다. 또한, 장비의 설정은 읽기만 하는 권한과 설정을 변경할 수 있는 권한으로 구분되는데, 접속 패스워드와 enable password가 동일할 경우, 하나의 패스워드 추측만으로 장비의 설정을 변경할 수 있으므로 접속 패스워드, enable password, enable secret를 다르게 설정해야 한다.

진단 기준

양호

패스워드가 대・소문자, 숫자, 특수문자가 포함된 8자리 이상으로 설정되어 있는 경우

취약

패스워드가 대・소문자, 숫자, 특수문자가 포함된 8자리 이상으로 설정되어 있지 않은 경우

진단 방법

[CISCO]

■ 패스워드 설정 정보 확인

(config)# show running-config
enable password 〈패스워드〉
line con 0
password 〈패스워드〉

```
Router#show running-config
Building configuration...

Current configuration : 679 bytes
!
version 15.1
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname Router
!
!
!
line con 0
 password nobiz
 login
!
```

[Juniper]

■ 패스워드 설정 정보 확인

```
R1〉 show configuration
system {
    root-authentication {
        encrypted-password "〈password〉"; ## SECRET-DATA
    }
    login {
        class super-user-local {
            idle-timeout 1;
            permissions all;
        }
        user ksel {
            full-name monitor;
            uid 110;
            class super-user-local;
            authentication {
                encrypted-password "〈password〉"; ## SECRET-DATA
```

조치 방법

■ 패스워드 설정을 참고하여 패스워드 설정 시 아래와 같은 규칙을 적용하여 변경

1. 암호는 적어도 8자 이상이어야 함.
2. 사용자 계정 이름이나 표시 이름의 문자를 3개 이상 연속하여 포함하지 않아야 함.
3. 암호에는 다음 네 가지 중 세 가지 범주의 문자가 포함되어야 함.
   - 대문자(A, B, C, ...)
   - 소문자(a, b, c, ...)
   - 숫자(0, 1, 2, 3, 4, 5, 6, 7, 8, 9)
   - 영숫자 이외의 문자와 유니코드 문자

암호화된 패스워드 사용

항목설명

패스워드를 암호화하지 않을 경우, Username Password, Authentication Key Password, Privileged Command Password, Console Access Password, VTY Access Password와 BGP Neighbor Password 등의 패스워드들이 평문으로 저장된다. Config(설정값) 유출 시 장비 접근에 대한 패스워드 노출의 위험성이 있으므로 패스워드 생성 시 암호화하여 저장해야 한다.
구조가 단순한 Vigenere 알고리즘이 사용되므로, enable 패스워드의 경우 Secret 패스워드를 별도로 지정하는 것이 안전하다. 사용자 계정 권한 및 패스워드 관리 미흡으로 인한 불법적인 공격 또는 기밀정보가 유출될 수 있다.

진단 기준

양호
패스워드 암호화 설정이 되어 있을 경우

취약
패스워드 암호화 설정이 되어 있지 않은 경우

진단 방법

[CISCO]

■ 패스워드 설정 정보 확인

(config)# show running-config
no service password-encryption

```
Router#show running-config
Building configuration...

Current configuration : 804 bytes
!
version 16.6.4
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
```

[Juniper]

■ 패스워드 설정 정보 확인

```
R1> show configuration
        password {
          format sha1;
        }
```

조치 방법

[CISCO]

■ 명령어를 통해 패스워드 암호화 설정

(config)# service password-encryption

```
Router(config)#service password-encryption
Router(config)#
```

(config)# enable algorithm-type sha256
(config)# secret cisco

※ 단순 암호화 설정할 경우 취약한 암호화 알고리즘이 적용되므로 SHA2 이상 암호화 알고리즘 적용이 필요

[Juniper]

■ 명령어를 통해 plain-text password 설정 시 암호를 sha2으로 암호화

R# set system login password format sha2

```
[edit]
root# set system login password format sha2
```

비고

※ 해당 OS 버전에서 지원이 가능한 경우, SHA-256 이상 적용 필요

- Cisco IOS15.3(3)M부터 지원(Type8)
  https://learningnetwork.cisco.com/s/article/cisco-routers-password-types
- SHA-256 적용 가능한 Juniper 버전 리스트 아래 페이지 참조
  https://apps.juniper.net/feature-explorer/feature-info.html?fKey=287&fn=Hash%20Algorithms%20SHA-2%20(SHA-256)

VTY 접근(ACL) 설정

항목설명

인터넷으로부터 VTY 접근을 차단하지 않았을 경우 VTY 장치를 통해서 네트워크 접속을 시도할 수 있으며, 원격 접속 패스워드 추측 공격 및 Sniffer 공격을 통해 장비에 접근할 수 있다.

진단 기준

양호
VTY 접근이 차단되어 있는 경우

취약
VTY 접근이 차단되어 있지 않은 경우

진단 방법

[CISCO]

■ 설정 정보 확인

(config)# show running-config

```
!
line con 0
!
line aux 0
!
line vty 0 4
 login
!
!
!
end
```

[Juniper]

■ 설정 정보 확인

```
R2〉Show configuration
firewall {
family inet {
    filter local-access-control {
        term terminal-access {
            from {
                address {
                    192.168.xxx.xxx/24;
                    }
                protocol tcp;
                port [ssh telnet];
                }
             then accept;
        }
```

```
            term terminal-access-denied {
                from {
                    protocol tcp;
                    port [ssh telnet];
                }
                then {
                    log;
                    reject;
                }
            }
            term default-term {
                then accept;
            }
        }
    }
        }
```

조치 방법

[CISCO]

■ 다음 명령어를 통해 VTY 접근 설정

(config)# access-list [1-99] {permit|deny} [Source Network] [WildcardMask]
(config)# access-list [1-99] {deny|permit} any
(config)# line vty 0 4
(config-line)# access-class [1-99] in

```
Router(config)#access-list 1 deny 150.100.7.128 0.0.0.31
Router(config)#access-list 1 permit any
Router(config)#line vty 0 4
Router(config-line)#access-class 1 in
Router(config-line)#
```

[Juniper]

■ 다음 명령어를 통해 VTY 접근 설정

R# edit firewall family inet filter **filter-name**
R# set term **rule-name1** from address 허용 지정 IP/32
R# set term **rule-name1** from protocol tcp
R# set term **rule-name1** from port ssh
R# set term **rule-name1** from port telnet
R# set term **rule-name1** then accept

```
[edit]
root# edit firewall family inet filter Filter_Name1

[edit firewall family inet filter Filter_Name1]
root#

[edit firewall family inet filter Filter_Name1]
root# set term Rule_Name1 from address 192.168.0.100/32

[edit firewall family inet filter Filter_Name1]
root# set term Rule_Name1 from protocol tcp

[edit firewall family inet filter Filter_Name1]
root# set term Rule_Name1 from port ssh

[edit firewall family inet filter Filter_Name1]
root# set term Rule_Name1 from port telnet

[edit firewall family inet filter Filter_Name1]
root# set term Rule_Name1 then accept

[edit firewall family inet filter Filter_Name1]
root#
```

R# set term **rule-name2** from protocol tcp
R# set term **rule-name2** from port ssh
R# set term **rule-name2** from port telnet
R# set term **rule-name2** then log
R# set term **rule-name2** then reject
R# set term default-term then accept
R# exit
R# set interfaces lo0 unit 0 family inet filter input **filer-name**
R# set interfaces lo0 unit 0 family inet address 127.0.0.1/32

```
root# set term Rule_Name2 from port ssh

[edit firewall family inet filter Filter_Name1]
root# set term Rule_Name2 from port telnet

[edit firewall family inet filter Filter_Name1]
root# set term Rule_Name2 then log

[edit firewall family inet filter Filter_Name1]
root# set term Rule_Name2 then reject

[edit firewall family inet filter Filter_Name1]
root# set term default-term then accept

[edit firewall family inet filter Filter_Name1]
root# exit

[edit]
root# set interfaces lo0 unit 0 family inet filter input Filter_Name1

[edit]
root# set interfaces lo0 unit 0 family inet address 127.0.0.1/32

[edit]
root#
```

비고

※ 원격 접속 ACL 설정이 대역으로 설정된 경우 취약
※ Host 단위로 설정된 경우 양호
※ 장비에서 ACL 설정을 제공하지 않고, 방화벽에서 접근 설정을 적용하는 경우 양호

Session Timeout 설정

항목설명

관리자가 장비에 접속하고 장시간 터미널을 이용하지 않고 자리를 비웠을 때, 장기 미사용중인 세션을 악용하여 침해사고가 발생할 수 있으므로, 자동으로 접속을 종료하거나 로그아웃이 되도록 세션을 설정하여야 한다.

진단 기준

양호

Session Timeout이 600초 이하로 설정되어 있는 경우

취약

Session Timeout이 600초 이하로 설정되어 있지 않은 경우

진단 방법

[CISCO]

■ 설정 정보 확인

(config)# show running-config
line con 0
exec-timeout <minute> <second>
line vty 0 4
exec-timeout <minute> <second>

```
!
line con 0
!
line aux 0
!
line vty 0 4
 login
!
!
!
end
```

(config-line)# exec-timeout 0 0

※ Telnet에 대한 timeout이 발생하지 않도록 하는 설정으로 이를 확인

[Juniper]

■ 설정 방법 확인

1) 일반적인 방법으로 확인

R〉 show configuration

system {

root-authentication {

...

}

login {

class super-user-local {

idle-timeout 1;

permissions all;

}

user ksel {

full-name monitor;

uid 110;

class super-user-local;

```
root> show configuration
## Last commit: 2012-05-11 11:54:23 UTC by root
version 12.1R1.9;
system {
    syslog {
        user * {
            any emergency;
        }
        file messages {
            any notice;
            authorization info;
        }
        file interactive-commands {
            interactive-commands any;
        }
    }
    ## Warning: missing mandatory statement(s): 'root-authentication'
}
```

2) 개별 세션들에 대한 방법 확인

R〉 show cli

CLI complete-on-space set to on

CLI idle-timeout set to 5minutes

```
root> show cli
CLI complete-on-space set to on
CLI idle-timeout disabled
CLI restart-on-upgrade set to on
CLI screen-length set to 24
CLI screen-width set to 80
CLI terminal is 'vt100'
CLI is operating in enhanced mode
CLI timestamp disabled
CLI working directory is '/root'
```

조치 방법

[CISCO]

■ 다음 명령어를 통해 Session Timeout 설정

(config)# line vty 0 4
(config-line)# exec-timeout 5 0 → 접속 후 5분 동안 어떠한 입력이 없는 경우

```
Router(config)#line vty 0 4
Router(config-line)#exec-timeout 5 0
```

■ 자동 종료 설정

(config)# line con 0
(config-line)# exec-timeout 〈minute〉 〈second〉
→ idle timeout 시간을 분, 초로 설정

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

(config)# line vty 0 4
(config-line)# exec-timeout 〈minute〉 〈second〉
→ idle timeout 시간을 분, 초로 설정

```
Router(config)#line vty 0 4
Router(config-line)#exec-timeout 5 0
```

[Juniper]

■ Session Timeout 설정

R# set system login class class-name idle-timeout 1
R# set system login class class-name permissions all
R# set system login user 계정명 class class-name

```
root# set system login class Class_Name idle-timeout 1

[edit]
root# set system login class Class_Name permissions all

[edit]
root# set system login user User_Name class Class_Name

[edit]
root#
```

최신 보안 패치 적용

항목설명

최신 취약점에 대한 패치 및 업데이트를 점검한다. 네트워크 장비의 보안 수준을 제고하고 성능 및 기능 향상을 위해서는 지속적인 Version Upgrade 및 보안 Patch 작업을 수행하여 최신 취약점을 보완하는 작업이 필요하다.

진단 기준

양호

최신 보안 패치를 적용한 경우

취약

최신 보안 패치를 적용하지 않은 경우

진단 방법

[Cisco]

■ 다음 명령어를 통해 버전 정보를 확인

(config)# show version

```
Router>show version
Cisco IOS Software [Everest], ISR Software (X86_64_LINUX_IOSD-UNIVERSALK9-M),
Version 16.6.4,RELEASE SOFTWARE (fc3)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2018 by Cisco Systems, Inc.
Compiled Sun 08-Jul-18 04:33 by mcpre
```

[Juniper]

■ 다음 명령어를 통해 버전 정보를 확인

R〉 show version

```
root> show version
Model: olive
JUNOS Base OS boot [12.1R1.9]
JUNOS Base OS Software Suite [12.1R1.9]
JUNOS Kernel Software Suite [12.1R1.9]
JUNOS Crypto Software Suite [12.1R1.9]
JUNOS Packet Forwarding Engine Support (M/T Common) [12.1R1.9]
JUNOS Packet Forwarding Engine Support (M20/M40) [12.1R1.9]
JUNOS Online Documentation [12.1R1.9]
JUNOS Voice Services Container package [12.1R1.9]
JUNOS Border Gateway Function package [12.1R1.9]
JUNOS Services AACL Container package [12.1R1.9]
JUNOS Services LL-PDF Container package [12.1R1.9]
JUNOS Services PTSP Container package [12.1R1.9]
JUNOS Services Stateful Firewall [12.1R1.9]
JUNOS Services NAT [12.1R1.9]
JUNOS Services Application Level Gateways [12.1R1.9]
JUNOS Services Captive Portal and Content Delivery Container package [12.1R1.9]
JUNOS Services RPM [12.1R1.9]
JUNOS Services HTTP Content Management package [12.1R1.9]
JUNOS AppId Services [12.1R1.9]
JUNOS IDP Services [12.1R1.9]
JUNOS Services Crypto [12.1R1.9]
JUNOS Services SSL [12.1R1.9]
JUNOS Services IPSec [12.1R1.9]
JUNOS Runtime Software Suite [12.1R1.9]
JUNOS Routing Software Suite [12.1R1.9]
```

조치 방법

[CISCO], [Juniper] 공통

■ 벤더 사의 권장 버전을 적용

1) 보안의 관점에서 본다면 오랜 기간의 테스트와 수정을 통하여 검증받은 GD 단계의 IOS를 사용하여야 하며, 다른 버전은 꼭 필요한 기능이 있는 경우만 사용해야 한다. IOS의 버전 체계 및 버전별 정보는 아래 사이트를 통하여 얻을 수 있다.
※ CISCO : http://www.cisco.com/web/about/security/intelligence/ios-ref.html
※ JUNIPER:https://kb.juniper.net/InfoCenter/index?page=content&id=KB21476&actp=search

2) 위의 IOS 버전 체계와 더불어 IOS 버전 이름이 붙여지는 방법 또한 IOS 적용을 위하여 꼭 알고 있어야 할 사항이다. "Version 12.2(2)T4"에서 12.2는 Major Release번호를 의미한다. Major Release의 버그 수정은 8주를 주기로 이루어지며 Major Release 번호 옆의 괄호의 번호가 버그 수정이 몇 번째 이루어졌는가를 나타낸다.

비고

※ 벤더사에서 권고하는 최신 보안 패치를 적용할 경우, 시스템 영향도를 파악하여 충분한 테스트 후 적용을 권고함

SNMP 서비스 확인

항목설명

SNMP는 UDP 프로토콜을 사용하기 때문에 SNMP 서비스를 활성화하면 각종 공격, 예를 들어 DOS 공격에 취약해질 뿐만 아니라 보안장비의 성능 저하, 크래쉬, 리로드 등의 위험이 존재한다. 따라서 SNMP 서비스가 불필요한 경우에는 비활성화시키는 것이 좋다.

진단 기준

양호

SNMP 서비스가 비활성화 되어 있는 경우

취약

SNMP 서비스가 활성화 되어 있는 경우

진단 방법

[CISCO]

■ SNMP 설정 현황 확인

show snmp

```
Router#show snmp
%SNMP agent not enabled
```

[Juniper]

■ SNMP 설정 현황 확인

```
R# show configuration
snmp {
  ...
}
```

조치 방법

[CISCO]

■ SNMP 서비스를 사용하지 않을 경우 다음 명령어를 통해 비활성화

```
Router(config)#no snmp server
```

[Juniper]

■ SNMP 서비스를 사용하지 않을 경우 다음 명령어를 통해 비활성화

R# delete snmp

비고

※ 트래픽 모니터링을 위해 SNMP 서비스를 사용하고 있는 경우, 해당 사항 없음(N/A)으로 처리함

SNMP community string 복잡성 설정

항목설명

SNMP의 community string은 데몬(SNMP)과 클라이언트 사이에서 데이터를 교환하기 전, 인증에 사용되는 일종의 패스워드이다. 초기에 설정된 Public, Private과 같은 default string을 사용할 경우, 해당 장비의 Routing Table, MAC Address 등의 중요 정보가 외부로 노출될 가능성이 존재한다. 따라서 community string을 유추하기 어려운 문자열로 변경하여 사용해야 한다.
※ default community string : public, private 등

진단 기준

양호

SNMP community string을 디폴트가 아닌 특정 문자열로 변경하여 사용하고 있는 경우

취약

SNMP community string을 디폴트 문자열로 사용하고 있는 경우

진단 방법

[CISCO]

■ SNMP community string 확인

(config)# snmp-server community community_string RO 2

```
!
snmp-server community public RW
!
```

[Juniper]

■ SNMP ACL 확인

```
R〉 show configuration
community name {
authorization read-only;
```

조치 방법

[CISCO]

■ SNMP ACL 적용

(config)# config terminal
(config)# snmp-server Community 〈커뮤니티 명〉

```
Switch#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#snm
Switch(config)#snmp-server Co
Switch(config)#snmp-server Community nobiz123
```

※ snmp-server community command는 IOS v10.0부터 기능 제공

[Juniper]

■ SNMP community string 변경

R# edit snmp
R# rename community 기존-community-string to community 새로운-community-string

SNMP ACL 설정

항목설명

SNMP 정보를 접근 할 수 있는 인가된 호스트를 제한함으로써 불법적인 접근에 대해 원천적인 차단이 가능하며, SNMP Community String을 이용한 인증 이외에 접근제어가 설정됨으로써 SNMP의 보안성이 한층 더 강화될 수 있다. IP access-list를 활용하여 특정 호스트 혹은 네트워크만이 SNMP 정보를 접근 할 수 있도록 설정해야 한다.

진단 기준

양호

IP access-list가 설정되어 있는 경우

취약

IP access-list가 설정되어 있지 않은 경우

진단 방법

[CISCO]

■ SNMP ACL 확인

(config)#show run
access-list 1 permit xxx.xxx.xxx.xxx
snmp-server community Community_string RO 1

```
access-list 3 permit host 192.168.150.143
access-list 3 deny any
!
!
!
!
snmp-server community public RW
```

[Juniper]

■ SNMP ACL 확인

```
R# show configuration firewall filter
snmp {
  ...
    client-list list0 {
        192.168.100.123/32;
    }
    community snmp-syp {
        protect: authorization read-only;
        protect: client-list-name list0;
      or  clients {
            192.168.40.128/32;
        }

or
```

```
        community "community-ed-10$" {
            client-list-name prefixlist;
        }
    }
    policy-options {
        prefix-list prefixlist{
            192.168.100.32/32;
            192.168.100.40/32;
            192.168.100.80/32;
```

조치 방법

[CISCO]

■ SNMP ACL 적용

(config)# snmp-server community Community_string [ro | rw] [number]
(config)#. access-list [number] permit xxx.xxx.xxx.xxx

```
Router(config)#snmp-server community public RO
Router(config)#access-list 1 permit 192.168.150.143
```

[Juniper]

■ SNMP ACL 적용

1) 첫 번째 적용 방법
R# set snmp client-list client-number 192.168.0.0/24
R# set snmp community [기존-community-string] client-list-name client-number
R# set snmp community [기존-community-string] clients 192.170.0.0/24 restrict

```
[edit]
root# set snmp client-list Client_Number 192.168.0.0/24

[edit]
root# set snmp community Base_Community_String client-list-name Client_Numb...

[edit]
root# set snmp community Base_Community_String clients 192.170.0.0/24 restr...
```

2) 두 번째 적용 방법
R# edit policy-options
R# set prefix-list prefix-list-name 허용 IP/32
R# exit
R# edit snmp
R# community 기존-community-string client-list-name prefix-list-name

비고

※ SNMP 서비스가 비활성화(disable) 되어 있는 경우에는 해당사항없음(N/A) 으로 양호

SNMP 커뮤니티 권한 설정

항목설명

SNMP에서는 RO(Read Only)와 RW(Read Write) 모드를 제공하는데, 대부분 RO 모드를 사용하지만, 일부 관리자들은 SNMP를 이용한 쉬운 관리를 위해 RW(Read/Write) community 문자열을 사용하는 경우도 있다. 이러한 보안 설정을 확실하게 하지 않을 경우, SNMP를 이용하여 설정을 수정할 수 있는 등 심각한 보안 문제를 유발할 수 있으며, SNMP를 이용하면 전체 네트워크의 구성, MAC 주소, IP 주소, SW 정보, HW 정보 등을 알 수 있다.

진단 기준

양호

SNMP community string 권한이 RO로 설정되어 있는 경우

취약

SNMP community string 권한이 RO로 설정되어 있는 경우

진단 방법

[CISCO]

■ SNMP Community 권한 확인

(config)#show run
snmp-server community community_string RO 2

```
!
snmp-server community public RO
!
```

[Juniper]

■ SNMP Community 권한 확인

R〉 show configuration
community name {
authorization read-only;

```
root> show configuration
## Last commit: 2012-05-11 11:54:23 UTC by root
version 12.1R1.9;
system {
    syslog {
        user * {
            any emergency;
        }
        file messages {
            any notice;
            authorization info;
        }
        file interactive-commands {
            interactive-commands any;
        }
    }
    ## Warning: missing mandatory statement(s): 'root-authentication'
}
```

조치 방법

[CISCO]

■ SNMP Community 권한을 Read Only로 설정

(config)# snmp-server community 〈스트링 명〉 RO (읽기 권한)

```
Router(config)#snmp-server community public RO
```

[Juniper]

R# edit snmp
R# set community 기존-community-string authorization read-only

```
[edit]
root# edit snmp

[edit snmp]
root# set community Base_Community_String authorization read-only
```

TFTP 서비스 차단

항목설명

TFTP 서비스는 특정 호스트가 아닌 일반적으로 어느 호스트에게 접근할 수 있게 되며, 특히 서버에 수행되는 데몬 프로세서가 자신의 파일 시스템에 대한 접근을 두지 않는 경우, 읽기 가능한 어느 파일도 외부에 있는 시스템에서 침입 정보를 빼내어 갈 가능성이 있다. TFTP는 인증 과정을 거치지도 않고 누구든지 파일을 읽거나 쓸 수 있도록 허용하기 때문에 가능한 차단 해야한다.

진단 기준

양호

TFTP 서비스가 비활성화되어 있는 경우

취약

TFTP 서비스가 활성화되어 있는 경우

진단 방법

[CISCO]

■ TFTP 설정 현황 확인

```
(config)#show run
 tftp-server
```

[Juniper]

■ TFTP 설정 현황 확인

```
R# show system
services {
    tftp-server;
}
```

조치 방법

[CISCO]

■ TFTP 서비스 비활성화

```
(config)# no tftp-server
```

[Juniper]

■ TFTP 서비스 비활성화

```
R# delete system services tftp-server
```

비고

※ default 설정 : TFTP 비활성화(disable)

사용하지 않는 인터페이스의 shutdown 설정

항목설명

라우터와 스위치에는 많은 포트가 있는데 사용하지 않는 포트에 연결한 인터페이스 상태가 Up이 되어 있다면 다른 외부 침입자에 의해 라우터의 정보와 내부 네트워크망에 손실을 입힐 수 있다. 따라서 사용하지 않는 인터페이스의 Shutdown 설정을 해야 한다.

진단 기준

양호

사용하지 않은 인터페이스의 Shutdown 설정이 되어 있는 경우

취약

사용하지 않은 인터페이스의 Shutdown 설정이 되어 있지 않은 경우

진단 방법

[CISCO]

■ 해당 인터페이스 Shutdown 확인

(config)# show ip interface brief

※ Protocol 필드에 해당 포트가 down/up이 되어 있는지 확인 할 수 있다.

```
R1#show ip interface brief
Interface              IP-Address      OK? Method Status                Protocol
FastEthernet0/0        unassigned      YES unset  up                    up
FastEthernet0/0.10     182.16.255.254  YES manual up                    up
FastEthernet0/0.20     182.30.255.254  YES manual up                    up
FastEthernet0/1        unassigned      YES unset  administratively down down
Serial0/0/0            100.100.100.2   YES manual up                    up
Serial0/0/1            unassigned      YES unset  administratively down down
Vlan1                  unassigned      YES unset  administratively down down
```

[Juniper]

■ 해당 인터페이스 Shutdown 확인

user@juniper〉show configure

조치 방법

[CISCO]

■ 사용하지 않은 인터페이스 차단

(config)# interface fastethernet 0/1
(config-if)# shutdown

```
R1(config)#interface fastEthernet 0/0
R1(config-if)#shutdown
```

[Juniper]

■ 사용하지 않은 인터페이스 차단

[edit interface interface-name] ← 해당 인터페이스 이름 삽입
set disable;

비고

※ 아래 페이지를 참조한다.
http://www.cisco.com/en/US/products/ps6017/products_command_reference_chapter09186a0080882d91.html

※ 사용하지 않는 인터페이스 shutdown 시 시스템 영향도를 고려하여 반영이 필요하다.

2.36.

정보보호시스템

2.36. 정보보호시스템

계정관리(4개 항목), 접근 관리(3개 항목), 패치 관리(1개 항목), 기능관리(6개 항목) 총 4개 영역에서 14개 항목으로 구성된다.

[표 36] 정보보호시스템 진단 체크리스트

구분	진단 항목
가. 계정 관리	정보보호시스템 Default 계정 변경
	정보보호시스템 Default 패스워드 변경
	정보보호시스템 계정별 권한 설정
	정보보호시스템 계정 관리
나. 접근 관리	정보보호시스템 원격 관리 접근 통제
	정보보호시스템 보안 접속
	Session Timeout 설정
다. 패치 관리	최신 보안 패치 적용
라. 기능 관리	정책 관리
	최소한의 서비스만 제공
	이상징후 탐지 경고 기능 설정
	장비 사용량 검토
	SNMP 서비스 확인
	SNMP Community string 복잡성 설정

정보보호시스템 Default 계정 변경

항목설명

디폴트 로그인 계정은 장비 제조업체에서 출고 시 설정되어 나오는 기본 계정 정보를 의미한다. 각 제조사의 장비별 디폴트 계정 리스트는 인터넷 등을 통해 쉽게 구할 수 있으며, 악의적인 사용자가 디폴트 계정을 이용하여 불법적으로 방화벽 장비에 접근할 수 있고, 시스템 침입 경로를 제공하는 등 일반적인 정보시스템 침해사고보다 심각한 피해를 초래할 수 있다.

진단 기준

양호

장비에서 제공하고 있는 디폴트 계정명을 변경하여 사용하는 경우
(ID 변경이 불가능할 경우 패스워드 설정을 통해 보완 필요)

취약

장비에서 제공하고 있는 디폴트 계정명을 변경하지 않고 사용하는 경우

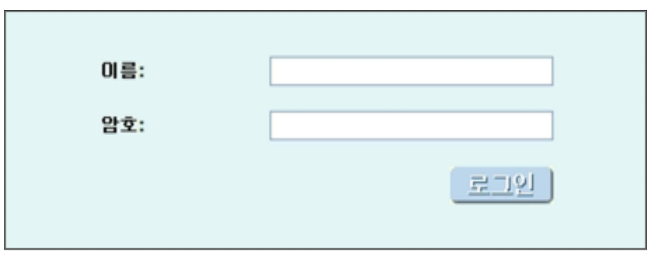
진단 방법

■ Default 계정 확인

1) Web을 통한 접속

2) 디폴트 계정, 비밀번호 입력

3) 접속 확인

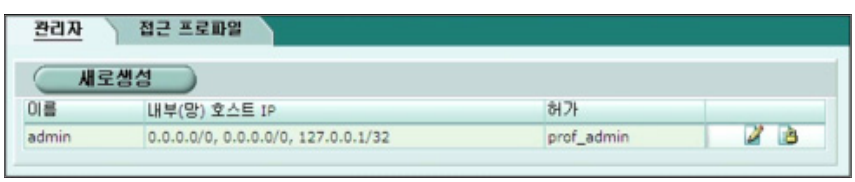


조치 방법

■ Default 계정 변경

1) 보안장비에서 제공하고 있는 계정 메뉴에서 ID 변경

2) ID 변경이 불가능할 경우 보안장비가 제공하는 범위에서 패스워드 보완 필요



정보보호시스템 Default 패스워드 변경

항목설명

디폴트 로그인 패스워드는 장비 제조업체에서 출고 시 설정되어 나오는 기본 로그인 패스워드 정보를 의미한다. 각 제조사의 장비별 디폴트 로그인 패스워드 리스트는 인터넷 등을 통해 쉽게 구할 수 있으므로 악의적인 사용자가 이러한 디폴트 로그인 패스워드를 이용하여 불법적으로 방화벽 장비에 접근할 수 있으며, 시스템 침입 경로를 제공하는 등 일반적인 정보시스템 침해사고보다 심각한 피해를 초래할 수 있다. 따라서 장비 디폴트 패스워드 또는 유추 가능한 패스워드를 사용하지 말아야 한다.

진단 기준

양호

장비 디폴트 패스워드 또는 유추 가능한 패스워드를 사용하지 않은 경우

취약

장비 디폴트 패스워드 또는 유추 가능한 패스워드를 사용하는 경우

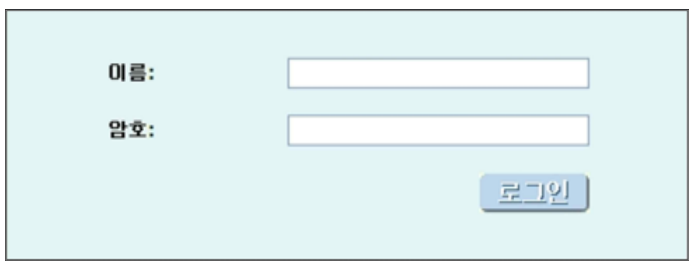
진단 방법

■ Default 패스워드 확인

1) Web을 통한 접속

2) 디폴트 계정, 비밀번호 입력

3) 접속 확인



조치 방법

■ Default 패스워드 변경

1) 패스워드 설정 메뉴에서 패스워드 변경

2) 보안장비가 제공하는 범위에서 패스워드 설정
   - 영문 대/소문자, 숫자, 특수문자 중 2가지 이상 조합 10자리 이상
   - 영문 대/소문자, 숫자, 특수문자 중 3가지 이상 조합 8자리 이상

3) 패스워드 최대 사용 기간 설정
   * 장비에서 패스워드 복잡도 설정 미지원 시 패스워드 최대 사용 기간 설정

정보보호시스템 계정별 권한 설정

항목설명

여러 사용자가 접속하여 사용하는 경우, 계정의 부적절한 권한 설정으로 인해 시스템의 침입 경로가 유출될 수 있다. 예를 들어 보안정책과 관련 없는 사용자에게 보안 정책을 수정할 수 있는 권한이 부여된다면, 의도하지 않게 보안 정책이 수정될 수 있으므로, 계정별 권한의 타당성을 확인해야 한다.

진단 기준

양호

사용자별 계정의 용도 파악 및 적절할 권한을 부여하는 경우

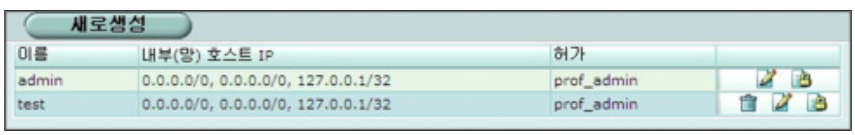
취약

사용자별 계정의 용도 파악 및 적절할 권한을 부여하지 않는 경우

진단 방법

■ 보안장비에서 제공하고 있는 계정 메뉴에서 계정별 권한 확인

예시) 관리자, 운영자, 관제 등의 계정을 분리하여 권한 부여하고 있는지 확인



조치 방법

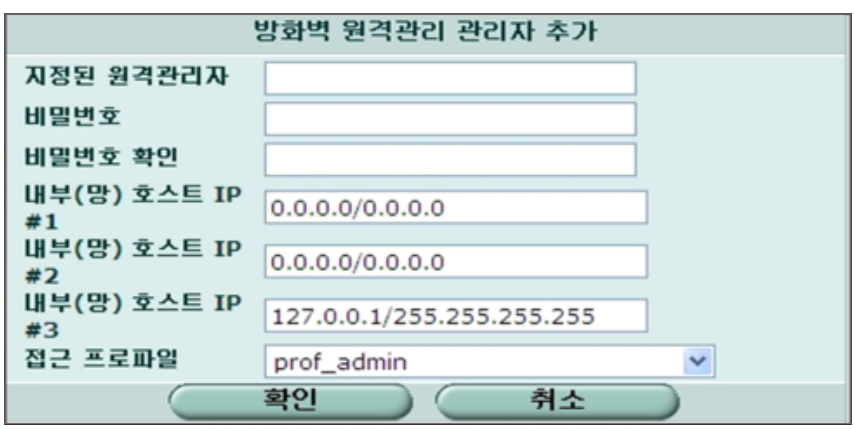
■ 계정별 권한 부여

1) 기존 계정의 권한 검토 필요 (불필요한 권한 삭제)

■ 계정별 권한 생성

1) 보안장비에서 제공하고 있는 계정 메뉴에서 새로운 계정 생성

2) 새로운 계정 담당자에 대한 역할 확인 후 권한 부여



정보보호시스템 계정 관리

항목설명

계정 관리가 미흡한 경우 자신의 업무와 관련 없는 애플리케이션 및 자원에 접속할 수 있기 때문에 보안 사고의 위험이 증가한다. 공용계정 및 휴면계정이 존재하는 시스템은 침해사고 및 장애 발생 시 사후 추적이 어려우므로 공용계정 사용을 금지하고, 사용하지 않는 계정은 즉시 삭제하도록 계정 관리를 해야 한다.

진단 기준

양호

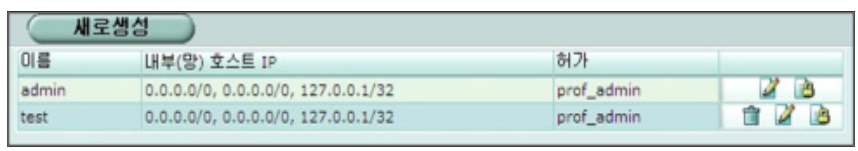
불필요한 공용계정 및 휴면계정을 제거하거나 관리하는 경우

취약

불필요한 공용계정 및 휴면계정을 제거하지 않고 관리하지 않는 경우

진단 방법

■ 보안장비에서 제공하고 있는 계정 메뉴에서 계정 및 담당자 확인



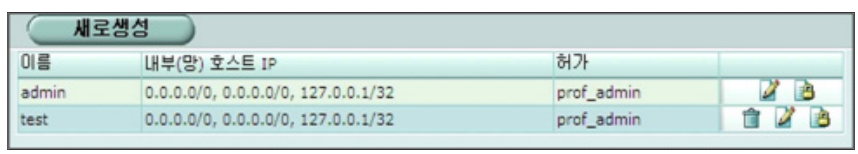
조치 방법

■ 공용계정 및 불필요한 계정 제거

1) 시스템에 대해 1인 1계정 사용을 원칙으로 하고 공용으로 사용하는 계정 사용 금지

2) 사용하지 않는 계정은 삭제하고 시스템 접근 이력을 관리하여 명시적인 계정 관리 설정

※ 시스템이 아닌 사람을 중심으로 하는 통합된 계정 관리가 중요함



정보보호시스템 원격 관리 접근 통제

항목설명

대부분 보안장비는 원격에서 관리하기 위한 관리자 접근 방법을 제공하고 있어 이에 대한 통제가 필요하다. 일반적으로 IP 단위 접근을 제한하여 보안장비에 대한 관리자 접근을 통제한다. 보안장비에서 제공하는 접근 제한 기능을 통해 관리자 단말기 또는 콘솔 장비의 IP를 등록하고 접근을 제한할 수 있다.

진단 기준

양호

원격 관리 시 관리자 IP만 접근할 수 있도록 설정한 경우

취약

원격 관리 시 관리자 IP만 접근할 수 있도록 설정하지 않은 경우

진단 방법

■ 보안장비에서 제공하고 있는 메뉴에서 접속 IP나 계정 제한 확인

조치 방법

■ 특정 IP 및 계정에서만 접속할 수 있도록 설정

비고

※ IP 대역 설정 시 취약하여 반드시 IP 단위로 접근 제한 설정 적용

※ IDS, IPS, VPN의 경우 Host 단위로 원격 관리 접근이 통제될 수 있음

정보보호시스템 보안 접속

항목설명

암호화되지 않은 데이터 전송 시 스니핑 등을 통한 정보 유출 위험이 존재하므로 SSL 인증 등의 암호화 접속을 통해 장비에 접속하도록 설정해야 한다.

진단 기준

양호

보안장비 접속 시 암호화 통신을 하는 경우

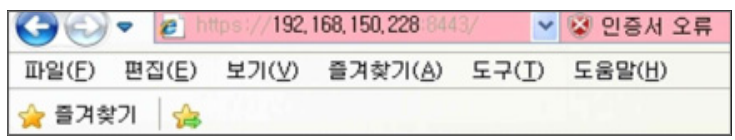
취약

보안장비 접속 시 암호화 통신을 하지 않는 경우

진단 방법

■ https 또는 ssh를 통한 접속 확인

1) https를 통한 접속 확인



2) ssh를 통한 접속 확인

조치 방법

■ 보안장비 접속 시, 가능하다면 SSL 등의 암호화 접속 활용

※ 제품마다 상이하므로 벤더 사에 문의

비고

※ SSL (Secure Socket Layer) : 인터넷 상에서 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 있다.

※ Telnet 포트는 사용 금지

Session Timeout 설정

항목설명

외부에서 서비스 사용자가 일정 시간 동안 통신이 없는 경우, 해당 세션을 종료시키는 것으로 각 TCP/UDP 등에 대하여 time out을 설정해야 한다. 이로 인해 불필요한 session을 정리하고 보안을 강화할 수 있다.

진단 기준

양호

Session Timeout 시간을 10분 이내로 설정한 경우

취약

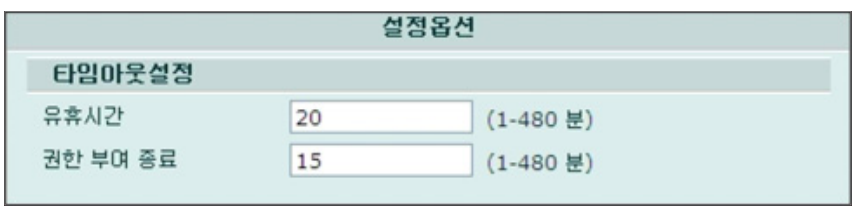
Session Timeout 시간을 10분 초과로 설정한 경우

진단 방법

■ 관리자의 부재 시 불법 사용자들의 접속을 차단하기 위해서 관리자의 logout을 하지 않고 자리를 비우는 실수에도 자동으로 logout 사용 여부를 확인

조치 방법

■ 보안장비가 제공하는 Timeout 기능 활성화



최신 보안 패치 적용

항목설명

보안장비는 지속적으로 취약점이 발생하고 있으며, 이에 대한 패치도 지속해서 제공되고 있으므로 보안장비의 보안 수준을 높이고 성능 및 기능 향상을 위해서는 보안 패치 작업을 수행하여 최신 취약점을 보완하는 작업이 필요하다.

진단 기준

양호

패치 적용 정책을 수립하여 주기적으로 패치를 관리하는 경우

취약

패치 적용 정책을 수립하여 주기적으로 패치를 관리하고 있지 않을 경우

진단 방법

■ 자동 업데이트 기능 설정이 활성화되어 있는지 확인

■ 정기점검 수행 여부와 크리티컬 이슈 발생 시 즉각적으로 패치를 진행하는지 확인이 필요함

※ 정기점검 수행 주기 확인이 필요함

조치 방법

■ 벤더사에 문의하여 자동 업데이트 기능 설정

장비 정보	
호스트 명	Fortigate-200 [변경]
펌웨어 버전	Fortigate-200 2.80,build489,051027 [갱신]
FortiGuard - AV 패턴	6.123(10/26/2005 14:55) [갱신]
FortiGuard - IPS 패턴	2.240(10/20/2005 17:01) [갱신]

비고

※ 벤더사에서 권고하는 최신 보안 패치를 적용할 경우, 시스템 영향도를 파악하여 충분한 테스트 후 적용을 권고함

정책 관리

항목설명

관리자마다 각기 다른 관리 방법을 적용한다면 보안장비의 정책은 다양한 버전이 존재하게 되고 관리자가 퇴사하거나 팀을 옮기게 될 경우, 이는 보안장비 정책 보안성에 심각한 문제를 발생할 수 있으므로 표준 절차와 지침이 필요하다. 관리자에 따라서 개별적인 정책 관리 방법이 존재하지 않도록 표준적인 정책 관리와 지침이 필요하다.

진단 기준

양호

정책에 대한 주기적인 검사로 미사용 및 불필요한 정책을 확인하여 제거 하는 경우

취약

정책에 대한 주기적인 검사를 하지 않고 미사용 및 불필요한 정책을 확인하여 제거하지 않은 경우

진단 방법

■ 정책에 대한 주기적인 검사로 미사용 또는 불필요한 정책을 확인

조치 방법

■ 정책 적용 시 아래와 같이 적용

1) 침입차단 시스템의 정책 관리 시, 객체관리는 관리자의 편의로 발생할 수 있는 오류를 최소화하기 위하여 기존 IP 대신에 관리자가 인식하기 쉬운 “객체명”을 사용함. “객체명”을 이용해서 관리자가 숫자(IP ADDRESS)의 오타나 서버의 착각을 최대한 방지할 수 있음.
2) 객체를 관리할 때 가장 중요한 것은 관리자가 직관적으로 인식할 수 있도록 명명하는 것이며, 다른 관리자들의 혼동을 최소화할 수 있는 “표준 명명 규약”이 있어야 함.
3) 객체 관리와 더불어 정책의 입력 시, 서로 연관성이 있는 서비스들은 비슷한 카테고리로 분류하여 정책 점검 시 검색이 쉬워야 하며 관리자마다 같은 정책 내의 세부 규칙을 여러 곳에 분산시키지 않도록 해야 함. 추가로 정책 내의 세부 규칙에 대한 카테고리가 존재하는지, 그리고 관리자가 다르더라도 그 카테고리 내에서 정렬 규칙이 존재하는지 등에 대해서 “정책 명명 방식”의 차이가 최소화되도록 해야 함. 즉, 어떤 관리자가 정책을 변경하더라도 같은 방법으로 정책을 변경할 수 있는 정책 변경/관리 세부 지침이 존재해야 함.
4) 정책 입력 시, 정책이 침입차단시스템의 성능과의 관계를 고려하였는가에 대해서 점검해야 함. 일반적으로 가장 정책의 적용을 많이 받게 되는 공개 서비스군 카테고리가 정책의 최고 상단에 존재하며 그 다음으로 접근이 많은 서비스군 카테고리가 존재하는 것이 바람직함.

비고

※ 패턴 기반 정보보호시스템의 경우, 패턴 업데이트가 주기적으로 이루어지는지 확인

최소한의 서비스만 제공

항목설명

방화벽은 기본적으로 all deny 설정으로 허용할 포트 및 IP를 추가함으로써 관리 포인트가 축소되며, 불필요한 포트를 차단하여 침입자의 침입 가능성을 낮출 수 있어 최소한의 서비스만을 제공하는 것이 필요하다.

진단 기준

양호

all deny 설정을 하고, 방화벽에 최소한의 서비스만 허용할 경우

취약

all deny 설정이 되어 있지 않거나, 방화벽에 불필요한 서비스를 허용할 경우

진단 방법

■ 방화벽에서 허용되지 않은 포트 접속 확인

조치 방법

■ 아래의 보안설정방법에 따라 설정을 변경

방화벽 기본 정책인 all deny에 최소한의 서비스만 허용 확인

※ 허용된 IP 및 서비스 포트만 오픈, IP 및 서비스 ANY 적용 금지

비고

※ 패턴 기반 정보보호시스템의 경우 해당 항목은 해당 사항 없음(N/A)로 처리함

이상징후 탐지 경고 기능 설정

항목설명

유해 트래픽은 정상적인 네트워크 운용 및 서비스에 지장을 주는 공격성 패킷과 바이러스 패킷을 의미한다. 유해 트래픽을 대응하기 위하여, 이상징후를 탐지하기 위한 24시간 모니터링 또는 이메일, SMS를 통한 경고 기능 설정이 필요하다.

진단 기준

양호

이상징후 탐지 시 관리자에게 이메일이나 SMS로 통보되는 경우

취약

이상징후 탐지 시 관리자에게 이메일이나 SMS로 통보되지 않는 경우

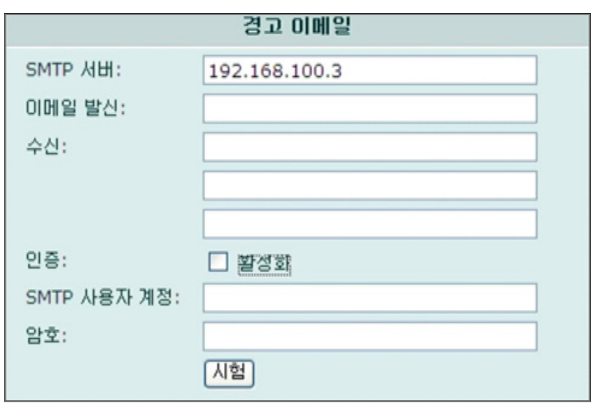
진단 방법

■ 정보보호시스템 담당자 인터뷰 및 UI 설정을 통해 정보보호시스템 이상징후 발생 시 알람 기능을 설정하고 있는지 확인

환경설정 → 관리자관리 → 전자우편

조치 방법

■ 24시간 모니터링을 통한 감시가 여건상 어려울 경우 이메일이나 SMS을 통한 경고 기능 설정으로 대체



비고

※ 24시간 관제가 이루어지고 있는 경우 양호함

장비 사용량 검토

항목설명

장비 사용량에 대한 검토로 인해 네트워크 트래픽의 수준 파악이 가능하며, 그에 따른 가용성 향상을 고려해볼 수 있다. 그러므로 보안장비의 Web Dash Board 모니터링을 통해 장비의 가용성에 대한 실시간 검토가 필요하다.

진단 기준

양호

장비 사용량을 정기적으로 모니터링 및 검토할 경우

취약

장비 사용량을 정기적으로 모니터링 및 검토하지 않을 경우

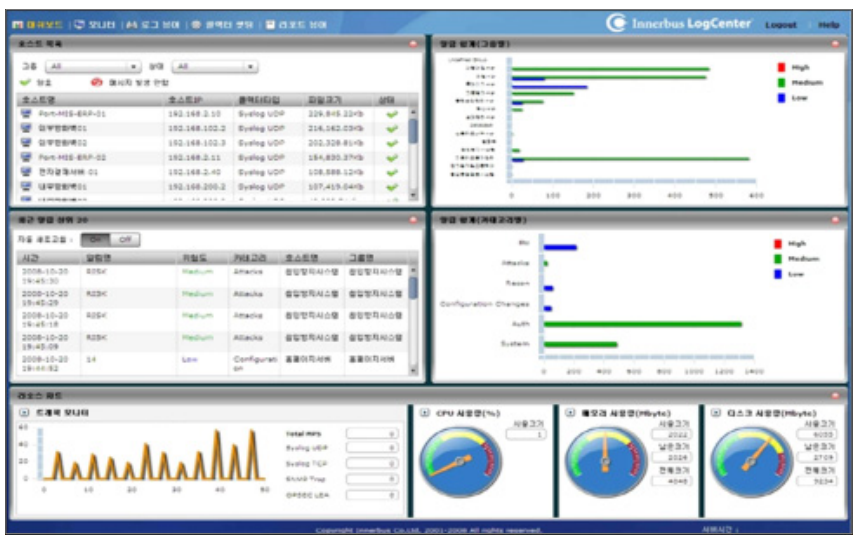
진단 방법

■ 보안장비의 Web Dash Board 모니터링 UI 확인

■ 보안장비의 실시간 알람, 이메일, SMS 경고 기능 설정 확인

조치 방법

■ 보안장비의 Web Dash Board 모니터링



비고

※ 24시간 관제가 이루어지고 있는 경우 양호함

SNMP 서비스 확인

항목설명

SNMP는 UDP 프로토콜을 사용하기 때문에 SNMP 서비스를 활성화하면 각종 공격, 예를 들어 DOS 공격에 취약해질 뿐만 아니라 보안장비의 성능 저하, 크래쉬, 리로드 등의 위험이 존재한다. 불필요하다면 SNMP 서비스를 중지하고, 관리를 위해 NMS 솔루션과의 연동이 필요하다면 Community String을 유추 불가능하게 설정한다.

진단 기준

양호

SNMP 서비스를 불필요하게 사용하지 않는 경우

취약

SNMP 서비스를 불필요하게 사용하는 경우

진단 방법

■ 보안장비의 SNMP 설정 메뉴에서 확인

조치 방법

■ 불필요하다면 SNMP 서비스를 중지하고, 관리를 위해 NMS 솔루션과의 연동이 필요하다면 SNMP 설정

비고

※ 장비 모니터링 또는 솔루션 연동을 위해 필요한 경우 양호함

SNMP Community string 복잡성 설정

항목설명

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 존재한다. 따라서 추측하기 어려운 Community string으로 변경하는 작업이 필요하다. 또한 SNMP Community string을 유지하기 어렵도록 설정하여 네트워크 상에서 시스템 정보가 비인가자에게 노출되지 않도록 해야한다.

진단 기준

양호

SNMP 서비스를 사용하지 않거나, 유추하기 어려운 Community string을 설정한 경우

취약

디폴트 Community string을 변경하지 않거나, 유추하기 쉬운Community string을 설정한 경우

진단 방법

■ 보안장비의 SNMP 설정 메뉴에서 Community string을 확인

■ 어플라이언스 제품을 제외한 소프트웨어 방식의 시스템인 경우, 자체 OS 취약점 점검이 이루어지고 있는지 확인

조치 방법

■ 아래와 같이 SNMP Community string 변경

1) 보안장비의 SNMP로써의 취약성이 존재하므로 SNMP Community string을 누구나 추측하기 어렵고 의미가 없는 문자열, 영문자 혼합으로 변경을 권고한다.

※ SNMP 버전 v1, v2, v3가 존재하며 v1과 v2는 암호화를 지원하지 않아 텍스트 열로 전송되나, v3는 암호화를 지원하며 해쉬 값으로 전송 된다.

2) 보안장비의 SNMP 설정에서 커뮤니티 이름 변경

비고

※ Public, Private과 같은 Default Community string 사용 금지

2.37.

스토리지

2.37. 스토리지

계정 관리(5개 항목) 총 1개 영역에서 5개 항목으로 구성된다.

[표 37] 스토리지 진단 체크리스트

구분	진단 항목
가. 계정 관리	root 계정 원격 접속 제한
	패스워드 복잡도 설정
	계정 잠금 임계값 설정
	패스워드 최대 사용 기간 설정
	불필요한 계정

root 계정 원격 접속 제한

항목설명

root 계정으로 직접 로그인을 하도록 허용하면 불법적인 침입자의 목표가 될 수 있으므로 root 계정 원격 접속을 금지해야 한다. 또한, 일반 사용자 계정 접속 후 관리자 계정으로의 변경 시 로그가 남지만, 관리자 계정으로 바로 접속하는 경우 어느 사용자가 접속했는지 알 수 없으므로 문제 발생 시 책임소재를 파악할 수 없다.

진단 기준

양호
root 계정의 원격 접속이 제한되어 있는 경우

취약
root 계정의 원격 접속이 제한되어 있지 않은 경우

진단 방법

■ root 계정의 원격 접속 제한 설정

1) 인터뷰를 통해 root 계정에 원격으로 접속 가능한지 확인

조치 방법

■ root 계정의 원격 접속 제한 설정을 적용

패스워드 복잡도 설정

항목설명

사용자 계정(root 및 일반 계정 모두)의 암호 설정 시, 일반적으로 유추하기 쉬운 암호를 설정하여, 비인가 사용자의 시스템 접근을 허용할 수 있다. 따라서 영문(대문자, 소문자), 숫자, 특수문자가 혼합된 8자리 이상의 패스워드로 설정하여 공격자가 추측하기 어려운 패스워드를 사용하거나 영문(대문자, 소문자), 숫자, 특수문자 중 2가지가 혼합된 10자리 이상의 패스워드로 설정해야 한다.

진단 기준

양호

패스워드를 영문, 숫자, 특수문자 중 3가지 조합으로 8자리 이상 또는 2가지 조합으로 10자리 이상 사용하여 복잡하게 설정한 경우

취약

패스워드가 존재하지 않거나 패스워드를 영문, 숫자, 특수문자를 혼합하지 않거나 8자리 미만으로 설정한 경우

진단 방법

■ 패스워드 복잡도 설정 만족

1) 인터뷰를 통해 패스워드가 복잡도 설정을 만족하고 있는지 확인

조치 방법

■ 패스워드 복잡도 설정 만족

1) 패스워드 복잡도 기준을 만족하도록 패스워드를 설정

계정 잠금 임계값 설정

항목설명

침입자에 의한 패스워드 무작위 대입 공격(Brute Force Attack)이나 패스워드 추측 공격(Password Guessing) 발생 시 암호입력 실패 횟수를 적정하게 제한함으로 자동공격을 차단하고 공격 시간을 지체시켜 패스워드 유출 위험을 줄일 수 있다.

진단 기준

양호

패스워드 입력 횟수를 5회 이하로 제한한 경우

취약

패스워드 입력 횟수를 설정하지 않거나, 5회 초과로 제한한 경우

진단 방법

■ 계정 잠금 임계값 설정

1) 인터뷰를 통해 계정 잠금 임계값 설정을 확인

조치 방법

■ 계정 잠금 임계값 설정

1) 계정 잠금 임계값을 5회 이하로 설정

패스워드 최대 사용 기간 설정

항목설명

패스워드 최대 사용 기간을 설정하지 않은 경우, 일정 기간 경과 후에도 유출된 패스워드로 접속이 가능하다. 악의적인 사용자로부터 무분별한 접속을 차단하기 위해 패스워드 최대 사용 기간을 설정하여 주기적으로 변경해야 한다.

진단 기준

양호

보안 정책에 따른 최대 사용 기간(90일 이내)이 설정되어 있는 경우

취약

보안 정책에 따른 최대 사용 기간이 설정되어 있지 않거나, 90일 초과인 경우

진단 방법

■ 패스워드 최대 사용 기간 설정 확인

1) 인터뷰를 통해 패스워드 최대 사용 기간을 확인

조치 방법

■ 패스워드 최대 사용 기간 설정

1) 패스워드 최대 사용 기간을 90일 이하로 설정

불필요한 계정 제거

항목설명

인가되지 않은 계정, 퇴직자 계정, 테스트 계정 등 실질적으로 업무에 사용하지 않은 불필요한 계정들이 있는 경우 비인가자가 쉽게 스토리지에 접속하여 데이터를 열람, 삭제, 수정할 위험이 있다.

진단 기준

양호

Default로 생성되는 계정 및 테스트 계정, 의심스럽거나 불필요한 계정이 없는 경우

취약

Default로 생성되는 계정 및 테스트 계정, 의심스럽거나 불필요한 계정이 있는 경우

진단 방법

■ 불필요한 계정 확인

1) 인터뷰를 통해 계정 목록을 확인하고 각 계정의 사용 목적을 확인

조치 방법

■ 불필요한 계정 제거

1) 불필요하거나 의심스러운 계정, 테스트 계정, 디폴트 계정인 경우 해당 계정을 제거

2.38.

BOSH(Director)

2.38. BOSH(Director)

보안 설정(3개 항목), 로그 관리 및 보안 패치(2개 항목) 총 2개 영역에서 5개 항목으로 구성된다.

[표 38] BOSH(Director) 진단 체크리스트

구분	진단 항목
가. 보안 설정	사용자 계정 생성 여부
	사용자 권한 관리
	SSL 인증서 구성
나. 로그 관리 및 보안 패치	로그 활성화
	최신 보안 패치 적용

사용자 계정 생성 여부

항목설명

사용자 계정이 BOSH Director에 구성되어 있지 않은 경우, 디폴트 계정(admin) 자격증명을 통해 로그인이 가능하다. 따라서 BOSH Director 사용자 계정을 구성해야 한다.

진단 기준

양호

사용자 계정이 존재하며 사용자 관리를 UAA 서버에 위임한 경우

취약

사용자 계정이 존재하지 않으면서 사용자 관리를 UAA 서버에 위임하지 않은 경우

진단 방법

■ 사전 구성 (Preconfigured Users)

1) Director의 배포 매니페스트 파일 확인

```
properties:
director:
user_management:
provider: local
local:
users:
- {name: admin, password: admin-password}
- {name: hm, password: hm-password}
```

조치 방법

■ 기본 구성 (사용자 계정 생성 방법)

```
bosh create user some-operator
 # 새 비밀번호 입력 : ********
# 새 비밀번호 확인 : ********
#`some-operator '사용자가 생성되었습니다.
```

■ 사전 구성 (설치 프로파일 내 사용자 계정 생성 방법)

1) Director의 배포 매니페스트 파일 수정 및 재배포

```
    director:
    user_management:
    provider: local
    local:
    users:
    - {name: admin, password: admin-password}
    - {name: hm, password: hm-password}
```

비고

※ 사용자 관리를 UAA 서버에 위임한 경우에는 해당사항 없음(N/A)

사용자 권한 관리

항목설명

ID 관리를 UAA 서버에 위임한 경우, UAA는 사용자가 BOSH Director에 로그인할 때 사용자의 권한을 자동으로 확인한다. 따라서 계정별 불필요한 권한이 부여되지 않았는지 점검한다.

진단 기준

양호
불필요한 권한이 존재하는 경우

취약
불필요한 권한이 존재하지 않는 경우

진단 방법

■ 계정별 권한 확인

```
# uaac users
```

조치 방법

■ 불필요한 권한 제거 또는 불필요한 계정 제거

```
# uaac user delete [불필요한 계정명]
```

비고

※ BOSH Teams 계정 권한 종류
Full Admin: bosh.admin
Full Read-only: bosh.read
Stemcell uploader: bosh.stemcells.upload
Release uploader: bosh.releases.upload
Anonymous: Users with no UAA scope

SSL 인증서 구성

항목설명

사용자 관리를 위해 UAA를 사용하는 경우 Director 및 UAA에 대해 SSL 인증서를 구성해야 한다.

진단 기준

양호

Director와 UAA 간 SSL 설정이 적용되어 있는 경우

취약

Director와 UAA 간 SSL 설정이 적용되어 있지 않은 경우

진단 방법

■ Director 배포 매니페스트 파일 확인

```
---
jobs:
- name: bosh
  properties:
    director:
      ssl:
        key: |
          -----BEGIN RSA PRIVATE KEY-----
          MII...
          -----END RSA PRIVATE KEY-----
        cert: |
          -----BEGIN CERTIFICATE-----
          MII...
          -----END CERTIFICATE-----
...
```

조치 방법

■ SSL 인증서를 생성하고 해당 인증서를 사용하도록 Director 구성

로그 활성화

항목설명

로그 기능을 활성화함으로써 침해 사고 및 장애 발생 시 로그 자료를 분석하여 원인을 파악해야 한다.

진단 기준

양호

로그가 활성화되어 있는 경우

취약

로그가 비활성화되어 있는 경우

진단 방법

■ 이벤트 로그 활성화 여부 확인

```
properties:
  director:
    events:
      record_events: true
```

■ API접근 로그 활성화 여부 확인

```
properties:
  director:
    log_access_events_to_syslog: true
```

※ default 설정 : false

조치 방법

■ 이벤트 로그 활성화 여부 확인

1) director.events.record_events를 true로 설정

```
properties:
  director:
    events:
      record_events: true
```

■ API 접근 로그 활성화 여부 확인

1) director.log_access_events_to_syslog(director.log_access_events)를 true로 설정

```
properties:
  director:
    log_access_events_to_syslog: true
```

비고

※ API 접근 로그의 경우, log_access_events_to_syslog → director.log_access_events으로 변경

최신 보안 패치 적용

항목설명

최신 보안 패치 및 업데이트를 수행하지 않을 경우 버전 취약점이 존재할 수 있으며 해당 취약점을 통해 시스템이 장악될 위험이 존재한다. 따라서 사용 버전에 취약점 존재 여부를 주기적으로 확인하고 최신 보안 업데이트를 수행해야 한다.

진단 기준

양호
최신 보안 패치를 적용한 경우

취약
최신 보안 패치를 적용하지 않은 경우

진단 방법

■ BOSH 버전 확인

```
# bosh env
```

조치 방법

■ 최신 보안 패치 적용 시 시스템 영향도를 파악하여 충분한 테스트 후 적용 권고

※ 최신 버전을 사용하도록 권고하고 있으나 시스템 운영상 적용이 어려운 경우 최신이 아닌 취약점이 존재하지 않는 버전도 허용하고 있음

2.39.

BOSH(UAA)

2.39. BOSH(UAA)

보안 설정(4개 항목), 로그 관리 및 보안 패치(2개 항목) 총 2개 영역에서 6개 항목으로 구성된다.

[표 39] BOSH(UAA) 진단 체크리스트

구분	진단 항목
가. 보안 설정	계정 잠금 임계값 설정
	패스워드 복잡도 설정
	세션 타임아웃 설정
	https 사용 여부 확인
나. 로그 관리 및 보안 패치	로그 설정
	최신 보안 패치 적용

계정 잠금 임계값 설정

항목설명

침입자로부터 패스워드 무작위 대입 공격이나 패스워드 추측 공격에 대하여 암호입력 실패 시도 횟수를 제한함으로써 전수 및 사전 공격을 차단하고 공격 시도 가용시간을 지연시킬 수 있다. 따라서 계정 잠금 임계값을 적절하게 설정해야 한다.

진단 기준

양호

계정 잠금 임계값 설정이 5회 이하로 설정된 경우

취약

계정 잠금 임계값 설정이 5회 초과로 설정된 경우

진단 방법

■ 계정 잠금 임계값 설정 확인

1) uaa.yml 파일을 확인하여 파일 내 authentication.policy.global.lockoutAfterFailures 설정 확인

조치 방법

■ 계정 잠금 임계값 설정

1) uaa.authentication.policy.global.lockoutAfterFailures 속성에 5 설정
lockoutAfterFailures: 5

패스워드 복잡도 설정

항목설명

추측 가능한 패스워드 및 default 패스워드를 사용할 경우, 공격자가 패스워드를 탈취 후 시스템에 접속하여 악의적인 영향을 줄 수 있으므로 패스워드 복잡도 설정을 만족하여 패스워드를 설정해야 한다.

진단 기준

양호

패스워드 복잡도 설정(영문자, 숫자, 특수문자 중 3가지 조합 8자리 이상 또는 2가지 조합 10자리 이상)이 적용된 경우

취약

패스워드 복잡도 설정이 적용되지 않은 경우

진단 방법

■ 패스워드 복잡도 설정 확인

1) 대시보드 또는 uaa.yml 파일을 확인하여 client.secret.policy.global 설정 확인

```
uaa:
  client:
    secret:
      policy:
        global:
          maxLength: 255
          minLength: 0
          requireDigit: 0
          requireLowerCaseCharacter: 0
          requireSpecialCharacter: 0
          requireUpperCaseCharacter: 0
```

※ 참고)
maxLength: 최대 문자 수 (default: 255)
minLength: 최소 문자 수 (default: 0)
requireDigit: 최소 숫자 수 (default: 0)
requireLowerCaseCharacter: 최소 소문자 수 (default: 0)
requireSpecialCharacter: 최소 특수문자 수 (default: 0)
requireUpperCaseCharacter: 최소 대문자 수 (default: 0)

조치 방법

■ 패스워드 복잡도 설정 설정

1) uaa.yml 파일 내 패스워드 복잡도 설정(client.secret.policy.global)

```
uaa:
  client:
    secret:
      policy:
        global:
          minLength: 8
          requireDigit: 1
          requireLowerCaseCharacter: 1
          requireSpecialCharacter: 1
          requireUpperCaseCharacter: 1
```

세션 타임아웃 설정

항목설명

일정 시간 동안 통신이 없는 경우, 해당 세션을 종료시킬 수 있도록 적절한 타임아웃을 설정해야 한다. 이로 인해 불필요한 세션을 정리하고 보안을 강화할 수 있다.

진단 기준

양호

세션 타임아웃 설정이 10분 이하로 설정된 경우

취약

세션 타임아웃 설정이 10분 초과로 설정된 경우

진단 방법

■ 세션 타임아웃 설정값 확인

1) uaa.yml 파일을 확인하여 uaa.servlet.idle-timeout 설정 확인
idle-timeout: 1800

※ default 설정 : 1800(30분)

조치 방법

■ 세션 타임아웃 설정

1) uaa.yml 파일의 uaa.servlet.idle-timeout 속성값을 600초(10분)로 설정

```
uaa:
  client:
    secret:
      policy:
        global:
          minLength: 8
          requireDigit: 1
          requireLowerCaseCharacter: 1
          requireSpecialCharacter: 1
          requireUpperCaseCharacter: 1
```

https 사용 여부 확인

항목설명

HTTP 통신 시 통신채널을 보호하고 안전한 통신을 사용할 수 있도록 http 프로토콜을 사용하지 않고 https 프로토콜을 사용해야 한다.

진단 기준

양호

https 프로토콜을 사용하는 경우

취약

https 프로토콜을 사용하지 않는 경우

진단 방법

■ https 설정 여부 확인

1) uaa.yml 파일을 확인하여 login.protocol 설정 확인

조치 방법

■ https 설정

1) uaa.파일을 login.protocol 속성에 https 설정
   login.protocol: https

로그 설정

항목설명

로그 기능을 활성화함으로써 침해 사고 및 장애 시 로그 자료를 분석할 수 있다.

진단 기준

양호
로깅 레벨이 INFO 이상으로 적용된 경우

취약
로깅 레벨이 INFO 미만으로 적용된 경우

진단 방법

■ 로깅 레벨 적용 확인

1) uaa.yml 파일을 확인하여 uaa.logging_level 설정값 확인

```
uaa:
  logging_level: WARN
```

조치 방법

■ 로깅 레밸 적용

1) uaa.yml 파일을 확인하여 uaa.logging_level 속성값 'INFO' 이상으로 설정

```
uaa:
  logging_level: INFO
```

비고

※ Logging Level : Trace → DEBUG → INFO → WARN → ERROR → FATAL → OFF

최신 보안 패치 적용

항목설명

신 보안 패치를 수행하지 않을 경우 버전 취약점이 존재할 수 있으며 해당 취약점을 통해 시스템이 장악될 위험이 존재한다. 따라서 사용하고 있는 버전에 취약점 존재 여부를 주기적으로 확인하고 최신 보안패치를 수행해야 한다.

진단 기준

양호

최신 보안 패치를 적용한 경우

취약

최신 보안 패치를 적용하지 않은 경우

진단 방법

■ UAA 버전 확인 (예시)

1) 설치 디렉터리 내 uaa.yml 파일 내용 확인

참고) bosh-lite 사용
설치 디렉터리: /root/workspace
bosh-lite 다운로드 파일: paasta-5.0
uaa.yml 경로: root/workspace/paasta-5.0/deployment/bosh-deployment/uaa.yml

```
- path: /releases/-
  release: uaa
  type: replace
  value:
    name: uaa
    sha1: 24fc5c63c99a594a537732bd897f10b8589096ff
    url: file:///home/((inception_os_user_name))/workspace/paasta-5.0/release/bo
sh/uaa-73.5.0-ubuntu-xenial-315.64-20190709-215817-751355338-20190709215839.tgz
    version: 73.5.0
- path: /instance_groups/name=bosh/properties/director/user_management/provider
  type: replace
  value: uaa
- path: /instance_groups/name=bosh/properties/director/user_management/local
  type: remove
- path: /instance_groups/name=bosh/properties/director/user_management/uaa?/url
  type: replace
  value: https://((internal_ip)):8443
```

조치 방법

■ 최신 보안 패치 적용 시 시스템 영향도를 파악하여 충분한 테스트 후 적용 권고

※ 최신 버전을 사용하도록 권고하고 있으나 시스템 운영상 적용이 어려운 경우 최신이 아닌 취약점이 존재하지 않는 버전도 허용하고 있음

클라우드 취약점 점검 가이드

KISA 한국인터넷진흥원
KOREA INTERNET & SECURITY AGENCY