AUTOISMS 개별 조치 보고서

날짜·시간	2026-02-20 11:59 (한국기준)
OS 타입	rocky
OS 버전	9.7
IP	172.20.10.12
HostName	target2

기존 취약 8건 → **조치 후 취약** 8건

파일 및 디렉터리 관리

U-19 /etc/hosts 파일 소유자 및 권한 설정 HIGH

기존 설정 | **조치 후 설정**

설정 비교

```
{'점검항목': '권한 설정', '상태': '취약', '세부내용': '취약: 권한이 644 입니다. (기준: 600 이하)', '점검명령어': "stat -c '%U %a' /etc/hosts; ls -ld /etc/hosts", '전체내용': '-rw-r--r--. 1 root root 158 Jun 23  2020 /etc/hosts'}
```

```
-
```

세부사항

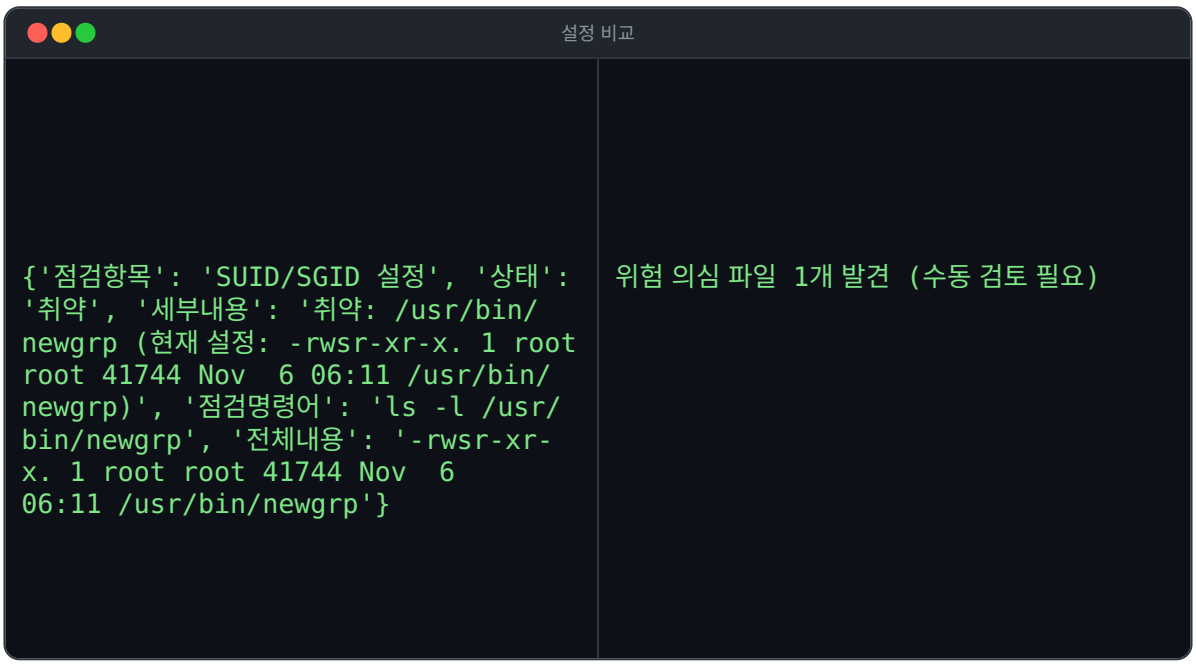
- {'점검항목': '소유자 설정', '상태': '양호', '세부내용': '양호: 소유자가 root 입니다.', '점검명령어': "stat -c '%U %a' /etc/hosts; ls -ld /etc/hosts", '전체내용': '-rw-r--r--. 1 root root 158 Jun 23 2020 /etc/hosts'}
- {'점검항목': '권한 설정', '상태': '취약', '세부내용': '취약: 권한이 644 입니다. (기준: 600 이하)', '점검명령어': "stat -c '%U %a' /etc/hosts; ls -ld /etc/hosts", '전체내용': '-rw-r--r--. 1 root root 158 Jun 23 2020 /etc/hosts'}

수동 조치 필요

U-23 SUID/SGID/Sticky bit 설정 점검 HIGH

기존 설정 | **조치 후 설정**

설정 비교



세부사항

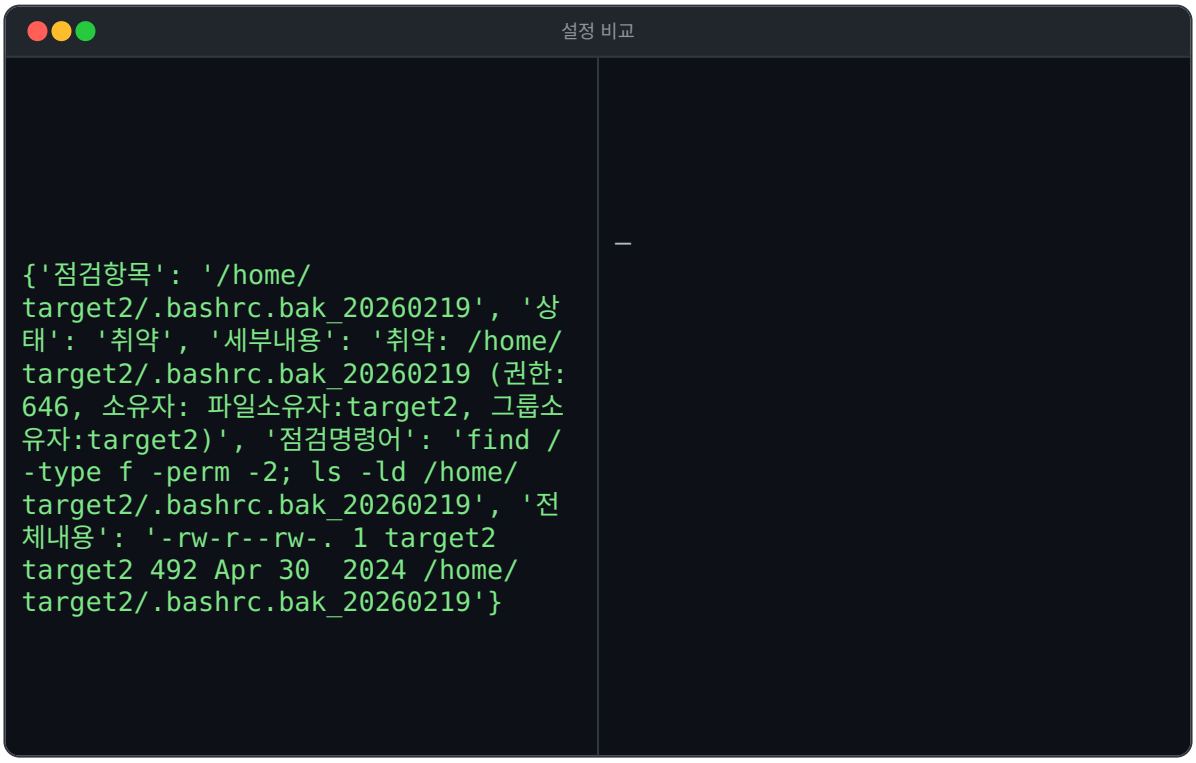
- {'점검항목': 'SUID/SGID 설정', '상태': '취약', '세부내용': '취약: /usr/bin/newgrp (현재 설정: -rwsr-xr-x. 1 root root 41744 Nov 6 06:11 /usr/bin/newgrp)', '점검명령어': 'ls -l /usr/bin/newgrp', '전체내용': '-rwsr-xr-x. 1 root root 41744 Nov 6 06:11 /usr/bin/newgrp'}

수동 조치 필요

U-25 world writable 파일 점검 HIGH

기존 설정 **조치 후 설정**

설정 비교



세부사항

- {'점검항목': '/home/target2/.bashrc.bak_20260219', '상태': '취약', '세부내용': '취약: /home/target2/.bashrc.bak_20260219 (권한: 646, 소유자: 파일소유자:target2, 그룹소유자:target2)', '점검명령어':

'find / -type f -perm -2; ls -ld /home/target2/.bashrc.bak_20260219', '전체내용': '-rw-r--rw-. 1 target2 target2 492 Apr 30 2024 /home/target2/.bashrc.bak_20260219'}
- {'점검항목': '/etc/passwd.bak_20260219', '상태': '취약', '세부내용': '취약: /etc/passwd.bak_20260219 (권한: 666, 소유자: 파일소유자:root, 그룹소유자:root)', '점검명령어': 'find / -type f -perm -2; ls -ld /etc/passwd.bak_20260219', '전체내용': '-rw-rw-rw-. 1 root root 944 Feb 11 17:29 /etc/passwd.bak_20260219'}

수동 조치 필요

서비스 관리

U-37 crontab 권한 설정 HIGH

기존 설정 | **조치 후 설정**

설정 비교

```
{'점검항목': '권한 설정', '상태': '취약', '세부내용': '취약: /usr/bin/crontab (권한: 4755, 소유자: root:root) - 750 초과', '점검명령어': "stat -c '%U %a' /usr/bin/crontab; ls -ld /usr/bin/crontab", '전체내용': '/usr/bin/crontab:owner=root:root,perm=4755'}
```

```
총 10개 중 취약 10개, 안전 0개
```

세부사항

- {'점검항목': '권한 설정', '상태': '취약', '세부내용': '취약: /usr/bin/crontab (권한: 4755, 소유자: root:root) - 750 초과', '점검명령어': "stat -c '%U %a' /usr/bin/crontab; ls -ld /usr/bin/crontab", '전체내용': '/usr/bin/crontab:owner=root:root,perm=4755'}
- {'점검항목': '권한 설정', '상태': '취약', '세부내용': '취약: /bin/crontab (권한: 4755, 소유자: root:root) - 750 초과', '점검명령어': "stat -c '%U %a' /bin/crontab; ls -ld /bin/crontab", '전체내용': '/bin/crontab:owner=root:root,perm=4755'}
- {'점검항목': '권한 설정', '상태': '취약', '세부내용': '취약: /etc/cron.deny (권한: 644, 소유자: root:root) - 640 초과', '점검명령어': "stat -c '%U %a' /etc/cron.deny; ls -ld /etc/cron.deny", '전체내용': '/etc/cron.deny:owner=root:root,perm=644'}
- {'점검항목': '권한 설정', '상태': '취약', '세부내용': '취약: /etc/crontab (권한: 644, 소유자: root:root) - 640 초과', '점검명령어': "stat -c '%U %a' /etc/crontab; ls -ld /etc/crontab", '전체내용': '/etc/crontab:owner=root:root,perm=644'}
- {'점검항목': '권한 설정', '상태': '취약', '세부내용': '취약: /etc/cron.d (권한: 755, 소유자: root:root) - 640 초과', '점검명령어': "stat -c '%U %a' /etc/cron.d; ls -ld /etc/cron.d", '전체내용': '/etc/cron.d:owner=root:root,perm=755'}
- {'점검항목': '권한 설정', '상태': '취약', '세부내용': '취약: /etc/cron.daily (권한: 755, 소유자: root:root) - 640 초과', '점검명령어': "stat -c '%U %a' /etc/cron.daily; ls -ld /etc/cron.daily", '전체내용': '/etc/cron.daily:owner=root:root,perm=755'}

- {'점검항목': '권한 설정', '상태': '취약', '세부내용': '취약: /etc/cron.hourly (권한: 755, 소유자: root:root) - 640 초과', '점검명령어': "stat -c '%U %a' /etc/cron.hourly; ls -ld /etc/cron.hourly", '전체내용': '/etc/cron.hourly:owner=root:root,perm=755'}
- {'점검항목': '권한 설정', '상태': '취약', '세부내용': '취약: /etc/cron.monthly (권한: 755, 소유자: root:root) - 640 초과', '점검명령어': "stat -c '%U %a' /etc/cron.monthly; ls -ld /etc/cron.monthly", '전체내용': '/etc/cron.monthly:owner=root:root,perm=755'}
- {'점검항목': '권한 설정', '상태': '취약', '세부내용': '취약: /etc/cron.weekly (권한: 755, 소유자: root:root) - 640 초과', '점검명령어': "stat -c '%U %a' /etc/cron.weekly; ls -ld /etc/cron.weekly", '전체내용': '/etc/cron.weekly:owner=root:root,perm=755'}
- {'점검항목': '권한 설정', '상태': '취약', '세부내용': '취약: /var/spool/cron (권한: 700, 소유자: root:root) - 640 초과', '점검명령어': "stat -c '%U %a' /var/spool/cron; ls -ld /var/spool/cron", '전체내용': '/var/spool/cron:owner=root:root,perm=700'}

수동 조치 필요

U-42 불필요한 RPC 서비스 비활성화 HIGH

기존 설정 | **조치 후 설정**

설정 비교

```
{'점검항목': 'walld', '상태': '취약',
'세부내용': '취약: walld - 실행 중
(PID: 845, 사용자: root) - 위협:
Write All Daemon (DoS)', '점검명령
어': "ps aux | grep 'walld' | grep
-v grep", '전체내용': 'root
845  0.0  2.1 346072
43332 ?        Ssl  09:24   0:04 /
usr/bin/python3 -s /usr/sbin/
firewalld --nofork --nopid'}
```

```
총 2개 중 취약 1개, 안전 1개
```

세부사항

- {'점검항목': 'walld', '상태': '취약', '세부내용': '취약: walld - 실행 중 (PID: 845, 사용자: root) - 위협: Write All Daemon (DoS)', '점검명령어': "ps aux | grep 'walld' | grep -v grep", '전체내용': 'root 845 0.0 2.1 346072 43332 ? Ssl 09:24 0:04 /usr/bin/python3 -s /usr/sbin/firewalld --nofork --nopid'}
- {'점검항목': 'RPC 서비스', '상태': '양호', '세부내용': '양호: rpcinfo 명령어 없음', '점검명령어': 'command -v rpcinfo', '전체내용': 'not installed'}
- {'점검항목': 'xinetd 설정', '상태': '양호', '세부내용': '양호: xinetd/inetd 설정에 취약 서비스 없음', '점검명령어': "ls /etc/xinetd.d 2>/dev/null; grep -v '^#' /etc/inetd.conf 2>/dev/null", '전체내용': ''}
- {'점검항목': 'RPC 서비스', '상태': '양호', '세부내용': '양호: systemd에 취약 RPC 서비스 없음', '점검명령어': "systemctl list-unit-files | grep -E 'rpc.cmsd|sadmind|rusersd|walld'", '전체내용': ''}
- {'점검항목': 'DNS 설정', '상태': '양호', '세부내용': '양호: rpcbind - 비활성화', '점검명령어': 'systemctl is-active rpcbind || pgrep rpcbind', '전체내용': 'inactive'}

수동 조치 필요

계정 관리

U-06 사용자 계정 su 기능 제한 HIGH

기존 설정 **조치 후 설정**

설정 비교

```
{'점검항목': 'PAM su 설정', '상태': '취약', '세부내용': '취약: pam_wheel.so 설정이 주석 처리되어 있음', '점검명령어': "grep -E '^[[:space:]]*#.*auth.*required.*pam_wheel\\\\.so' /etc/pam.d/su", '전체내용': '#auth\t\trequired\tpam_wheel.so use_uid'}
```

```
—
```

세부사항

- {'점검항목': 'PAM su 설정', '상태': '취약', '세부내용': '취약: pam_wheel.so 설정이 주석 처리되어 있음', '점검명령어': "grep -E '^[[:space:]]*#.*auth.*required.*pam_wheel\\\\.so' /etc/pam.d/su", '전체내용': '#auth\t\trequired\tpam_wheel.so use_uid'}

수동 조치 필요

U-07 불필요한 계정 제거 LOW

기존 설정 **조치 후 설정**

설정 비교

```
{'점검항목': '불필요한 계정', '상태': '취약', '세부내용': '취약: 불필요한 계정(lp)이 존재함', '점검명령어': "grep '^lp:' /etc/passwd", '전체내용': 'lp'}
```

```
—
```

세부사항

- {'점검항목': '불필요한 계정', '상태': '취약', '세부내용': '취약: 불필요한 계정(lp)이 존재함', '점검명령어': "grep '^lp:' /etc/passwd", '전체내용': 'lp'}
- {'점검항목': '불필요한 계정', '상태': '양호', '세부내용': '양호: 불필요한 계정(uucp)이 없음', '점검명령어': "grep '^uucp:' /etc/passwd", '전체내용': ''}
- {'점검항목': '불필요한 계정', '상태': '양호', '세부내용': '양호: 불필요한 계정(nuucp)이 없음', '점검명령어': "grep '^nuucp:' /etc/passwd", '전체내용': ''}
- {'점검항목': '불필요한 계정', '상태': '취약', '세부내용': '취약: 불필요한 계정(games)이 존재함', '점검명령어': "grep '^games:' /etc/passwd", '전체내용': 'games'}

수동 조치 필요

패치 관리

U-64 주기적 보안 패치 적용 HIGH

기존 설정	조치 후 설정
{'점검항목': '보안패치 점검', '상태': '취약', '세부내용': '취약: 적용되지 않은 최신 보안 패치가 존재합니다.', '점검명령어': 'dnf check-update --security', '전체내용': 'Last metadata expiration check: 1:28:05 ago on Fri 20 Feb 2026 10:29:53 AM KST. \n\nbinutils.x86_64 2.35.2-67.el9_7.1 baseos\nbinutils- gold.x86_64 2.35.2-67.el9_7.1 baseos\ncurl.x86_64 7.76.1-35.el9_7.3 baseos\nexpat.x86_64 2.5.0-5.el9_7.1 baseos\nglib2.x86_64 2.68.4-18.el9_7.1 baseos\ngnupg2.x86_64 2.3.3-5.el9_7 baseos\nkernel.x86_64 5.14.0-611.30.1.el9_7 baseos\nkernel- core.x86_64 5.14.0-611.30.1.el9_7 baseos\nkernel-	미적용 보안 패치 존재

```
modules.x86_64
5.14.0-611.30.1.el9_7
baseos\nkernel-modules-
core.x86_64
5.14.0-611.30.1.el9_7
baseos\nkernel-
tools.x86_64
5.14.0-611.30.1.el9_7
baseos\nkernel-tools-
libs.x86_64
5.14.0-611.30.1.el9_7
baseos\nlibbrotli.x86_64

1.0.9-9.el9_7
baseos\nlibcurl.x86_64

7.76.1-35.el9_7.3
baseos\nlibssh.x86_64

0.10.4-17.el9_7
baseos\nlibssh-
config.noarch
0.10.4-17.el9_7
baseos\nlibxml2.x86_64

2.9.13-14.el9_7
baseos\nopenssl.x86_64

1:3.5.1-7.el9_7
baseos'}
```

세부사항

- {'점검항목': '보안패치 점검', '상태': '취약', '세부내용': '취약: 적용되지 않은 최신 보안 패치가 존재합니다.', '점검명령어': 'dnf check-update --security', '전체내용': 'Last metadata expiration check: 1:28:05 ago on Fri 20 Feb 2026 10:29:53 AM KST.\n\nbinutils.x86_64 2.35.2-67.el9_7.1 baseos\nbinutils-gold.x86_64 2.35.2-67.el9_7.1 baseos\ncurl.x86_64 7.76.1-35.el9_7.3 baseos\nexpat.x86_64 2.5.0-5.el9_7.1 baseos\nglib2.x86_64 2.68.4-18.el9_7.1 baseos\ngnupg2.x86_64 2.3.3-5.el9_7 baseos\nkernel.x86_64 5.14.0-611.30.1.el9_7 baseos\nkernel-core.x86_64 5.14.0-611.30.1.el9_7 baseos\nkernel-modules.x86_64 5.14.0-611.30.1.el9_7 baseos\nkernel-modules-core.x86_64 5.14.0-611.30.1.el9_7 baseos\nkernel-tools.x86_64 5.14.0-611.30.1.el9_7 baseos\nkernel-tools-libs.x86_64 5.14.0-611.30.1.el9_7 baseos\nlibbrotli.x86_64 1.0.9-9.el9_7 baseos\nlibcurl.x86_64 7.76.1-35.el9_7.3 baseos\nlibssh.x86_64 0.10.4-17.el9_7 baseos\nlibssh-config.noarch 0.10.4-17.el9_7 baseos\nlibxml2.x86_64 2.9.13-14.el9_7 baseos\nopenssl.x86_64 1:3.5.1-7.el9_7 baseos'}

수동 조치 필요