U-11

- 분류 : 파일 및 디렉터리 관리
- 위험도 : 상

---

1. 점검 내용

- /etc/syslog.conf 파일 권한 적절성 점검

---

2. 점검 목적

- /etc/syslog.conf 파일의 권한 적절성을 점검하여, 관리자 외 비인가자의 임 의적인 syslog.conf 파일 변조를 방지하기 위한 목적

---

3. 보안 위협

- syslog.conf 파일의 설정 내용을 참조하여 로그의 저장위치가 노출되며 로그를 기록하지 않도록 설정하거나 대량의 로그를 기록하게 하여 시스템 과부 하를 유도할 수 있다

---

4. 참고

- /etc/syslog.conf : syslogd 데몬 실행시 참조되는 설정파일로 시스템 로그 기록의 종류, 위치 및 Level을 설정할 수 있다
- 최신 버전 우분투에서는 /etc/syslog.conf 파일 기본적으로 존재하지 않고 rsyslog나 systemd-journald를 사용한다

---

5. 취약 판단 기준

- rsylog, systemd-journald 관련 파일의 소유자가 root(또는 bin, sys)가 아니거나, 권한이 640 미만이 아닌 경우 취약하다고 판단

---

6. 점검 방법

6.1. rsyslog 관련 파일 권한 확인

```
ls -al /etc/rsyslog.conf
ls -al /etc/rsyslog.d/
```

6.2. systemd-journald 관련 파일 권한 확인

```
ls -al /etc/systemd/journald.conf
```

---

7. 조치 방법

7.1. * 파일의 소유자 및 권한 변경 조치

```
chown root /etc/rsyslog.conf
chown root /etc/rsyslog.d
chown root /etc/systemd/journald.conf

chmod 640 /etc/rsyslog.conf
chmod 640 /etc/systemd/journald.conf
chmod 640 /etc/rsyslog.d/
```