U-16

- 분류 : 파일 및 디렉터리 관리
- 위험도 : 상

---

1. 점검 내용

- 존재하지 않는 device 파일 존재 여부 점검

---

2. 점검 목적

- 실제 존재하지 않는 디바이스를 찾아 제거함으로써 root 파일 시스템 손상 및 다운 등의 문제를 방지하기 위한 목적

---

3. 보안 위협

- 공격자는 rootkit 설정파일들을 서버 관리자가 쉽게 발견하지 못하도록 /dev 에 device 파일인 것처럼 위장하는 수법을 많이 사용한다

---

4. 참고

- /dev 디렉터리: 논리적 장치 파일을 담고 있는 /dev 디렉터리는 /devices 디렉터리에 있는 물리적 장치 파일에 대한 심볼릭 링크이다
  - 예를 들어 rmt0를 rmto로 잘못 입력한 경우 rmto 파일이 새로 생성되는 것과 같이 디바이스 이름 입력 오류 시 root 파일 시스템이 에러를 일으킬 때까지 /dev 디렉터리에 계속해서 파일을 생성한다
- /dev 디렉터리 내 불필요한 device 파일이 존재할 시 삭제 권고

---

5. 취약 판단 기준

- dev에 대한 파일, 미점검 또는, 존재하지 않은 device 파일을 방치한 경우 취약하다고 판단

---

6. 점검 방법

6.1. /dev 디렉터리 내에 존재하지 않는 device 파일 찾기

```
find /dev -type f ! -exec test -c {} \; ! -exec test -b {} \; -print 2>/dev/null
```

---

7. 조치 방법

7.1. major, minor number를 가지지 않는 device 파일 제거

```
find /dev -type f ! -exec test -c {} \; ! -exec test -b {} \; -exec rm -f {} \;
2>/dev/null
```