U-07

- 분류 : 파일 및 디렉터리 관리
- 위험도 : 상

---

1. 점검 내용

- /etc/passwd 파일 권한 적절성 점검

---

2. 점검 목적

- /etc/passwd 파일의 임의적인 변경을 차단하기 위함을 통해 비인가자가 권 한 상승하는 것을 막기 위한 목적

---

3. 보안 위협

- 관리자(root) 외 사용자가 '/etc/passwd' 파일의 사용자 정보를 변조할 수 있다
  - shell 변경
  - 사용자 추가/삭제 등
  - root를 포함한 사용자 권한 획득이 가능하다

---

4. 참고

- '/etc/passwd' : 사용자의 ID, 패스워드, UID, GID, 홈 디렉터리, 쉘 정보를 담고 있는 파일

---

5. 취약 판단 기준

- /etc/passwd 파일의 소유자가 root가 아니거나, 권한이 644 이하가 아닌 경우 취약하다고 판단

---

6. 점검 방법

6.1. /etc/passwd 파일 권한 확인

```
cd /etc
ls -al passwd
```

---

7. 조치 방법

7.1. 권한 변경 조치

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

- 소유자 root
- 권한 644