U-08

- 분류 : 파일 및 디렉터리 관리
- 위험도 : 상

---

1. 점검 내용

- /etc/shadow 파일 권한 적절성 점검

---

2. 점검 목적

- /etc/shadow 파일을 관리자만 제어할 수 있게 하여 비인가자들의 접근을 차단하도록 shadow 파일 소유자 및 권한을 관리하기 위한 목적

---

3. 보안 위협

- 해당 파일의 암호화된 해쉬값을 복호화하여(크래킹) 비밀번호를 탈취할 수 있다

---

4. 참고

- /etc/shadow 파일 : 시스템에 등록된 모든 계정의 패스워드를 암호화된 형태로 저장 및 관리 하고 있는 파일

---

5. 취약 판단 기준

- /etc/shadow 파일의 소유자가 root가 아니거나, 권한이 400 이하가 아닌 경우 취약하다고 판단

---

6. 점검 방법

6.1. /etc/shadow 파일 권한 확인

```
cd /etc
ls -al shadow
```

---

7. 조치 방법

7.1. 파일의 소유자 및 권한 변경 조치

```
chown root /etc/shadow
chmod 400 /etc/shadow
```

- 소유자 root
- 권한 400