U-06

- 분류 : 파일 및 디렉터리 관리
- 위험도 : 상

---

1. 점검 내용

- 소유자 불분명한 파일이나 디렉터리가 존재하는지 여부를 점검

---

2. 점검 목적

- 소유자가 존재하지 않는 파일 및 디렉터리를 삭제 및 관리하여 임의의 사용 자가 해당파일을 열람, 수정하는 행위를 사전에 차단하기 위한 목적

---

3. 보안 위협

- 소유자가 존재하지 않는 파일의 UID와 동일한 값으로 특정계정의 UID값을 변경하면 해당 파일의 소유자가 되어 모든 작업이 가능하다

---

4. 참고

- 소유자가 존재하지 않는 파일 및 디렉터리
  - 퇴직자의 자료
  - 관리 소홀로 인해 생긴 파일
  - 해킹으로 인한 공격자가 만들어 놓은 악의적인 파일

---

5. 취약 판단 기준

- 소유자가 존재하지 않는 파일 및 디렉터리가 존재하는 경우 취약하다고 판단

---

6. 점검 방법

6.1. 소유자가 존재하지 않는 파일 찾기

```
sudo find / -nouser -type f 2>/dev/null
```

*2>/dev/null : 권한 거부 오류 메시지 제외

6.2. 소유자가 존재하지 않는 디렉터리 찾기

```
sudo find / -nogroup -type f 2>/dev/null
```

---

7. 조치 방법

7.1. 소유자가 존재하지 않는 파일, 디렉터리 삭제 조치

```
rm 파일명
rmdir 디렉터리명
```