U-26

- 분류 : 서비스 관리
- 위험도 : 상

---

1. 점검 내용

- automountd 서비스 데몬의 실행 여부 점검

---

2. 점검 목적

- 로컬 공격자가 automountd 데몬에 RPC(Remote Procedure Call)를 보낼 수 있는 취약점이 존재하기 때문에 해당 서비스가 실행중일 경우 서비스를 중 지시키기 위한 목적

---

3. 보안 위협

- 파일 시스템의 마운트 옵션을 변경하여 root 권한을 획득할 수 있으며, 로컬 공격자가 automountd 프로세스 권한으로 임의의 명령을 실행할 수 있다

---

4. 참고

- automountd : 클라이언트에서 자동으로 서버에 마운트를 시키고 일정 시간 사용하지 않으면 unmount 시켜 주는 기능
- RPC(Remote Procedure Call): 별도의 원격 제어를 위한 코딩 없이 다른 주소 공간에서 함수나 프로시저를 실행할 수 있게 하는 프로세스 간 프로토콜

---

5. 취약 판단 기준

- automountd 서비스가 활성화 되어 있는 경우 취약하다고 판단

---

6. 점검 방법

6.1. 서비스 상태 확인

```
sudo systemctl status autofs
```

- 일반적으로 `automountd`는 `autofs` 서비스의 일부로 작동하기 때문

---

7. 조치 방법

7.1. automount 서비스 데몬 비활성화 조치

```
sudo systemctl disable autofs
sudo systemctl stop autofs
```