U-25

- 분류 : 서비스 관리
- 위험도 : 상

---

1. 점검 내용

- NFS(Network File System) 사용 시 허가된 사용자만 접속할 수 있도록 접근 제한 설정 적용 여부 점검

---

2. 점검 목적

- 접근권한이 없는 비인가자의 접근을 통제하기 위한 목적

---

3. 보안 위협

- 접근 제한 설정이 적절하지 않을 경우 인증절차 없이 비인가자의 디렉터리나 파일의 접근이 가능하며, 해당 공유 시스템에 원격으로 마운트하여 중요 파 일을 변조하거나 유출할 위험이 있다

---

4. 참고

- NFS(Network File System) : 원격 컴퓨터의 파일 시스템을 로컬 시스템에 마운트하여 마치 로컬 파일시스템처럼 사용할 수 있는 프로그램
- NFS 서비스 사용 금지가 원칙이나 불가피하게 사용이 필요한 경우 NFS v2, v3은 평문으로 전송되는 취약점이 있기 때문에 **암호화 되는 v4를 사용하는 것을 권고**

---

5. 취약 판단 기준

- 불필요한 NFS 서비스를 사용하고 있고, everyone 공유를 제한하지 않은 경우 취약하다고 판단

---

6. 점검 방법

6.1. /etc/exports 파일 점검

```
cat /etc/exports
```

- 출력 된 내용에서 `everyone` 이나 무제한 접근을 허용하는 설정이 있는지 확인

올바른 예시 출력

```
/shared/directory 192.168.1.0/24(rw,sync,no_subtree_check)
```

- 다음과 같이 특정 IP 또는 네트워크에만 접근을 허용하는 설정이 되어 있어야 한다

---

7. 조치 방법

7.1. NFS 서비스 비활성화 조치

```
sudo systemctl disable nfs-server
sudo systemctl stop nfs-server
```

7.2. /etc/exports 파일 수정 조치

```
sudo vim /etc/exports
```

- 특정 네트워크만 접근 허용하도록 조치 (6.1. 올바른 예시 출력 참고)