U-24

- 분류 : 서비스 관리
- 위험도 : 상

---

1. 점검 내용

- 불필요한 NFS 서비스 사용 여부 점검

---

2. 점검 목적

- NFS(Network File System)를 이용한 침해 사고 위험성이 높으므로 사용하지 않는 경우 중지할 목적

---

3. 보안 위협

- NFS 서비스는 서버의 디스크를 클라이언트와 공유하는 서비스로 적정한 보안설정이 적용되어 있지 않다면 불필요한 파일 공유로 인한 유출위험이 있다

---

4. 참고

- NFS(Network File System) : 원격 컴퓨터의 파일시스템을 로컬 시스템에 마운트하여 마치 로컬 파일시스템처럼 사용할 수 있는 프로그램
- 원칙적으로 사용이 금지되어 있지만 불가피하게 필요한 경우 U-25(상) 항목을 참조하여 통제 해야 한다

4.1. 불필요한 NFS 서비스 관련 데몬

데몬 이름	역할	설명
nfs-server	NFS 서버 데몬	NFS 서버 기능을 제공하여 클라이언트가 원격 파일 시스템에 접근할 수 있도록 함
rpcbind	RPC 포트 매핑 데몬	RPC 프로그램 번호를 포트 번호에 매핑하는 기능을 제공
nfs-mountd	NFS 마운트 데몬	NFS 마운트를 처리하고 클라이언트의 마운트 요청을 관리
nfs-idmapd	NFS ID 매핑 데몬	사용자 및 그룹 ID를 클라이언트와 서버 사이에서 매핑
rpc.statd	NFS 상태 모니터링 데몬	NFS 락 상태를 모니터링하고 상태를 관리
rpc.rquotad	NFS 디스크 할당량 데몬	NFS 클라이언트의 디스크 할당량을 관리
rpc.nfsd	NFS 데몬	NFS 요청을 처리하는 메인 데몬
rpc.lockd	NFS 락 데몬	NFS 파일 잠금을 관리

---

5. 취약 판단 기준

- 불필요한 NFS 서비스 관련 데몬이 활성화 되어 있는 경우 취약하다고 판단

---

6. 점검 방법

6.1. 각 서비스 점검

```
# nfs-server 데몬 상태 확인
sudo systemctl status nfs-server

# rpcbind 데몬 상태 확인
sudo systemctl status rpcbind

# nfs-mountd 데몬 상태 확인
sudo systemctl status nfs-mountd

# nfs-idmapd 데몬 상태 확인
sudo systemctl status nfs-idmapd

# rpc.statd 데몬 상태 확인
sudo systemctl status rpc-statd

# rpc.rquotad 데몬 상태 확인
sudo systemctl status rpc-rquotad

# rpc.nfsd 데몬 상태 확인
sudo systemctl status rpc-nfsd

# rpc.lockd 데몬 상태 확인
sudo systemctl status rpc-lockd
```

---

7. 조치 방법

7.2. 불필요한 데몬 비활성화 조치

```
sudo systemctl disable 데몬이름
sudo systemctl stop 데몬이름
```