U-28

- 분류 : 서비스 점검
- 위험도 : 상

---

1. 점검 내용

- 안전하지 않은 NIS 서비스의 비활성화, 안전한 NIS+ 서비스의 활성화 여부 점검

---

2. 점검 목적

- 안전하지 않은 NIS 서비스를 비활성화 하고 안전한 NIS+ 서비스를 활성화 하여 시스템 보안수준을 향상하고자 하는 목적

---

3. 보안 위협

- 보안상 취약한 서비스인 NIS를 사용하는 경우 비인가자가 타 시스템의 root 권한 획득이 가능하므로 사용하지 않는 것이 가장 바람직하나 만약 NIS를 사용해야 하는 경우 사용자 정보보안에 많은 문제점을 내포하고 있는 NIS보 다 NIS+를 사용하는 것을 권장

---

4. 참고

- NIS 주 서버
  - 정보표를 소유하여 NIS 대응 파일들로 변환하고, 이 대응 파일들이 네 트워크를 통해 제공됨으로써 모든 컴퓨터에 정보가 갱신되도록 한다.
  - 네트워크를 통한 공유로부터 관리자와 사용자들에게 일관성 있는 시스템 환경을 제공한다

---

5. 취약 판단 기준

- NIS 서비스가 활성화 되어 있는 경우 취약하다고 판단

---

6. 점검 방법

6.1. NIS 및 NIS+ 관련 프로세스 점검

```
ps -ef | egrep 'ypserv|ypbind|ypxfrd|rpc.nisd'
```

---

7. 조치 방법

7.1. NIS 서비스 비활성화 조치

```
# NIS 서비스 비활성화
sudo systemctl stop ypserv
sudo systemctl disable ypserv
sudo systemctl stop ypbind
sudo systemctl disable ypbind
sudo systemctl stop ypxfrd
sudo systemctl disable ypxfrd
```

7.2. (필요한 경우) NIS+ 서비스 활성화

```
# NIS+ 서비스 활성화
sudo systemctl start rpc.nisd
sudo systemctl enable rpc.nisd
```