U-29

- 분류 : 서비스 관리
- 위험도 : 상

---

1. 점검 내용

- tftp, talk 등의 서비스를 사용하지 않거나 취약점이 발표된 서비스의 활 성화 여부 점검

---

2. 점검 목적

- 안전하지 않거나 불필요한 서비스를 제거함으로써 시스템 보안성 및 리소스의 효율적인 운용을 위한 목적

---

3. 보안 위협

- 사용하지 않는 서비스나 취약점이 발표된 서비스 운용 시 공격 시도 가능

---

4. 참고

서비스	취약할 수 있는 이유	역할
TFTP	인증 및 암호화 기능이 부족하여 데이터 도청 및 무단 접근에 취약함	Trivial File Transfer Protocol(간이 파일 전송 프로토콜)의 약자로, 간단한 파일 전송을 위해 사용되는 프로토콜 - 주로 네트워크 부팅, 라우터 및 스위치의 설정 파일을 전송하는 데 사용됨
Talk	데이터가 평문으로 전송되므로 도청에 취약하며, 인증 절차가 부족하여 스푸핑 공격 가능성 있음	Unix 시스템에서 실시간 채팅을 가능하게 하는 프로그램 - 같은 네트워크 상의 사용자들 간에 대화를 주고받을 수 있음
NTalk	동일하게 평문 전송으로 인한 도청 위험이 있으며, 호환성 문제로 인한 보안 취약점이 존재할 수 있음	Talk 서비스의 개선된 버전으로, 더 많은 기능과 안정성을 제공 - 여러 네트워크를 통해 사용자들 간의 채팅을 지원함

---

5. 취약 판단 기준

- tftp, talk, ntalk 서비스가 활성화 되어 있는 경우 취약하다고 판단

---

6. 점검 방법

6.1. 불필요한 서비스 데몬 확인

```
cat /etc/inetd.conf | grep "tftp|talk|ntalk"
```

---

7. 조치 방법

7.1. 비활성화 및 제거

```
sudo systemctl stop 데몬이름
sudo systemctl disable 데몬이름
sudo apt-get remove --purge 데몬이름
```