

U-19

- 분류 : 서비스 관리
 - 위험도 : 상
-

1. 점검 내용

- finger 서비스 비활성화 여부 점검
-

2. 점검 목적

- Finger 서비스를 통해서 네트워크 외부에서 해당 시스템에 등록된 사용자 정보를 확인할 수 있어 비인가자에게 사용자 정보가 조회 되는 것을 차단하고자 하는 목적
-

3. 보안 위험

- 비인가자에게 사용자 정보가 조회되어 패스워드 공격을 통한 시스템 권한 탈취 가능성이 있으므로 사용하지 않는다면 해당 서비스를 중지하여야 한다
-

4. 참고

- Finger
 - 사용자 정보 확인 서비스
 - who : 현재 사용 중인 사용자들에 대한 간단한 정보만을 보여주는 명령어
 - finger 명령어는 옵션에 따른 시스템에 등록된 사용자 뿐 아니라 네트워크를 통하여 연결되어 있는 다른 시스템에 등록된 사용자들에 대한 자세한 정보를 보여준다
 - Ubuntu 24.04 LTS에서는 finger 서비스가 기본적으로 설치되어 있지 않다
-

5. 취약 판단 기준

- Finger 서비스가 활성화 되어 있는 경우 취약하다고 판단
-

6. 점검 방법

6.1. /etc/inetd.conf 파일 점검

```
cat /etc/inetd.conf | grep finger
```

- 파일이 존재하지 않거나 해당 라인이 주석 처리되어 있으면 비활성화된 것

6.2. 시스템 서비스 상태 확인

```
sudo systemctl status finger
```

- finger 서비스 상태 확인
-

7. 조치 방법

7.1. 패키지 제거

```
sudo apt-get remove finger -y
```

7.2. /etc/inetd.conf 파일 수정

```
sudo vim /etc/inetd.conf
```

- `finger stream tcp nowait ...` 라인을 찾아서 주석 처리