

U-58

- 분류 : 파일 및 디렉터리 관리
 - 위험도 : 중
-

1. 점검 내용

- 사용자 계정과 홈 디렉터리의 일치 여부를 점검
-

2. 점검 목적

- /home 이외 사용자의 홈 디렉터리 존재 여부를 점검하여 비인가자가 시스템 명령어의 무단 사용을 방지하기 위한 목적
-

3. 보안 위협

- passwd 파일에 설정된 홈디렉터리가 존재하지 않는 경우, 해당 계정으로 로그인시 홈디렉터리가 루트 디렉터리("/")로 할당되어 접근이 가능하다
-

4. 참고

- 홈 디렉터리: 사용자가 로그인한 후 작업을 수행하는 디렉터리
 - 일반 사용자의 홈 디렉터리 위치: /home/user명
-

5. 취약 판단 기준

- 홈 디렉터리가 존재하지 않는 계정이 발견된 경우 취약하다고 판단
-

6. 점검 방법

6.1. 사용자 계정의 홈 디렉터리 존재 여부 점검

```
awk -F: '{ if ($6 && !system("[ ! -d " $6 " ]")) print $1 " 계정의 홈 디렉터리 없음" }' /etc/passwd
```

7. 조치 방법

7.1. 홈 디렉터리가 존재하지 않는 계정에 홈 디렉터리 생성

```
awk -F: '{ if ($6 && system("[ ! -d " $6 " ]")) system("sudo mkdir -p " $6 " && sudo chown " $1 ":" $1 " " $6) }' /etc/passwd
```

7.2. 홈 디렉터리가 존재하지 않는 계정 삭제

```
awk -F: '{ if ($6 && system("[ ! -d " $6 " ]")) system("sudo userdel " $1) }' /etc/passwd
```