

U-50

- 분류 : 계정 관리
 - 위험도 : 하
-

1. 점검 내용

- 시스템 관리자 그룹에 최소한(root 계정과 시스템 관리에 허용된 계정)의 계정만 존재하는지 점검
-

2. 점검 목적

- 관리자 그룹에 최소한의 계정만 존재하는지 점검하여 불필요하게 권한이 남용되고 있는지 확인하기 위한 목적
-

3. 보안 위협

- 시스템을 관리하는 root 계정이 속한 그룹은 시스템 운영 파일에 대한 접근 권한이 부여되어 있으므로 해당 관리자 그룹에 속한 계정이 비인가자에게 유출될 경우 관리자 권한으로 시스템에 접근하여 계정 정보 유출, 환경 설정 파일 및 디렉터리 변조 등의 위협이 존재한다
-

4. 취약 판단 기준

- 관리자 그룹에 불필요한 계정이 등록되어 있는 경우 취약하다고 판단
-

5. 점검 방법

5.1. /etc/group 파일 점검

```
cat /etc/group
```

6. 조치 방법

6.1. 불필요한 계정 삭제 조치

```
sudo userdel 사용자이름
```