U-45

- 분류 : 계정 관리
- 위험도 : 하

---

1. 점검 내용

- su 명령어 사용을 허용하는 사용자를 지정한 그룹이 설정되어 있는지 점검

---

2. 점검 목적

- su 관련 그룹만 su 명령어 사용 권한이 부여되어 있는지 점검하여 su 그룹 에 포함되지 않은 일반 사용자의 su 명령 사용을 원천적으로 차단하는지 확 인하기 위한 목적

---

3. 보안 위협

- 무분별한 사용자 변경으로 타 사용자 소유의 파일을 변경 할 수 있으며 root 계정으로 변경하는 경우 관리자 권한을 획득 할 수 있다

---

4. 취약 판단 기준

- su 명령어를 모든 사용자가 사용하도록 설정되어 있는 경우 취약하다고 판단

---

5. 점검 방법

5.1. /etc/pam.d/su 파일 점검

```
grep pam_wheel.so /etc/pam.d/su
```

- 특정 그룹의 사용자만 su 명령이 사용 가능 하도록 설정이 가능하다

예시

```
auth required pam_wheel.so use_uid
```

- wheel 그룹의 사용자만 su 명령어를 사용할 수 있도록 설정한 것

---

6. 조치 방법

6.1. /etc/pam.d/su 파일 수정 조치

```
sudo vim /etc/pam.d/su
```

- (예시) auth required pam_그룹이름.so use_uid 추가

6.2. 사용자를 su 명령을 허용할 그룹에 추가

```
sudo usermod -aG 그룹이름 사용자이름
```