U-01

- 분류 : 계정 관리
- 위험도 : 상

---

1. 점검 내용

- 시스템 정책에 root 계정의 원격 터미널 접속 차단 설정이 적용되어 있는지 점검

---

2. 점검 목적

- 관리자 계정 탈취로 인한 시스템 장악을 방지하기 위해 외부 비인가자의 root 계정 접근 시도를 원천적으로 차단하기 위한 목적

---

3. 보안 위협

- root 계정은 운영체제의 모든기능을 설정 및 변경이 가능하여(프로세스, 커 널변경 등) root 계정을 탈취하여 외부에서 원격을 이용한 시스템 장악 및 각종 공격으로(무작위 대입 공격) 인한 root 계정 사용 불가 위협이 있다

---

4. 참고

- 무작위 대입 공격(Brute Force Attack) : 특정한 암호를 풀기 위해 가능한 모든 값을 대 입하는 공격 방법
- 사전 대입 공격(Dictionary Attack): 사전에 있는 단어를 입력하여 암호를 알아내거나 암호를 해독하는 데 사용되는 컴퓨터 공격 방법

---

5. 취약 판단 기준

- 원격 터미널 서비스 사용 시 root 직접 접속을 허용한 경우 취약하다고 판단

---

6. 점검 방법

*이전 버전은 원격 접속 시 Telnet을 사용하기도 하였으나 보안 상 SSH 권장

6.1. sshd_config 내 PermitRootLogin 설정 확인

```
grep "^PermitRootLogin" /etc/ssh/sshd_config
```

- PermitRootLogin no 출력 시 root 계정 원격 터미널 접속이 차단되어 있는 것

---

7. 조치 방법

7.1. sshd_config 내 PermitRootLogin 설정

```
sudo vim /etc/ssh/sshd_config
```

- PermitRootLogin no 줄을 추가하여 준다

7.2. SSH 서비스 재시작하여 변경 사항 적용

```
sudo systemctl restart ssh
```