U-36

- 분류 : 서비스 관리
- 위험도 : 상

---

1. 점검 내용

- Apache 데몬이 root 권한으로 구동되는지 여부 점검

---

2. 점검 목적

- Apache 데몬을 root 권한으로 구동하지 않고 별도의 권한으로 구동함으로써 침해사고 발생 시 피해범위 확산 방지 목적

---

3. 보안 위협

- 웹서비스 데몬을 root 권한으로 실행시 웹서비스가 파일을 생성, 수정하는 과정에서 웹 서비스에 해당하지 않는 파일도 root 권한에 의해 쓰기가 가능 하며 해킹 발생 시 root 권한이 노출 될 수 있다

---

4. 취약 판단 기준

- Apache 데몬이 root 권한으로 구동 되는 경우 취약하다고 판단

---

5. 점검 방법

5.1. Apache 데몬이 root 권한으로 구동되는지 점검

```
ps -ef | grep apache2
```

5.2. Apache 설정 파일에서 User 및 Group 지시자 확인

```
sudo grep -E "^\s*User|^\s*Group" /etc/apache2/apache2.conf
```

- 설정 파일에서 User와 Group이 `www-data` 또는 다른 제한된 권한의 사용자 및 그룹으로 설정되어 있어야 한다

---

6. 조치 방법

6.1. Apache 설정 파일 수정 및 재시작

```
sudo vim /etc/apache2/apache2.conf
sudo systemctl restart apache2
```

올바른 예시

```
User root가 아닌 별도 계정명
Group root가 아닌 별도 계정명
```