U-51 (하)

1. 점검 내용

- 그룹(예 /etc/group) 설정 파일에 불필요한 그룹(계정이 존재하지 않는지 점검
- 시스템 관리나 운용에 사용되지 않는 그룹, 계정이 존재하고 시스템 관리나 운용 에 사용되지 않는 그룹 등)이 존재하는지 점검

*GID(Group Identification): 다수의 사용자가 특정 개체를 공유할 수 있게 연계시키는 특정 그룹의 이름으로 주로 계정처리 목적으로 사용되며, 한 사용자는 여러 개의 GID를 가질 수 있다

---

2. 점검 목적

- 시스템에 불필요한 그룹이 존재하는지 점검하여 불필요한 그룹의 소유권으로 설정되어 있는 파일의 노출에 의해 발생할 수 있는 위험에 대한 대비가 되어 있는지 확인하기 위한 목적

---

3. 취약 판단 기준

- 시스템 관리나 운용에 불필요한 그룹이 존재할 경우 취약하다고 판단

---

4. 점검 방법

4.1. cat /etc/group 파일 확인

```
cat /etc/group
```

4.2. cat /etc/passwd 파일 확인

```
cat /etc/passwd
```

4.3. cat /etc/gshadow 파일 확인

```
cat /etc/gshadow
```

---

5. 보안 조치 방법

```
groupdel 그룹이름
```

- 해당 그룹 삭제 시 그룹 권한으로 존재하는 파일이 있는지 확인이 필요하다
- 사용자가 없는 그룹이라 하더라도 추후 권한 할당을 위해 그룹을 먼저 생성하였을 가능성도 존재하므로 무분별한 삭제는 권장하지 않는다
- 신규 생성된 그룹 (GID 500 이상) 중심으로 점검 권고
-
    - **GID 0-99**: 시스템 그룹(예: root, daemon 등)으로 예약되어 있다

- **GID 100-499**: 배포판 및 특정 애플리케이션이 사용하는 그룹에 예약되어 있다
- **GID 500 이상**: 일반 사용자가 생성한 그룹 또는 일반적으로 시스템 관리자가 추가로 생성한 그룹이다
