U-51

- 분류 : 계정 관리
- 위험도 : 하

---

1. 점검 내용

- 그룹 설정 파일에 불필요한 그룹(계정이 존재하지 않고 시스템 관리나 운용에 사용되지 않는 그룹, 계정이 존재하고 시스템 관리나 운용 에 사용되지 않는 그룹 등)이 존재하는지 점검

---

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. 보안 위협

- 계정이 존재하지 않는 그룹은 현재 사용되고 있는 그룹이 아닌 불필요한 그룹으로 삭제 조치가 필요하다

---

4. 참고

- GID(Group Identification) : 다수의 사용자가 특정 개체를 공유할 수 있게 연계 시키는 특정 그룹의 이름으로 주로 계정 처리 목적으로 사용되며, 한 사용자는 여러 개의 GID를 가질 수 있다
  - /etc/group 파일과 /etc/passwd 파일을 비교하여 점검하기를 권고한다

4.1. 불필요할 수 있는 그룹

그룹 이름	역할	불필요할 수 있는 이유
daemon	시스템 서비스 데몬 그룹	특정 서비스가 사용되지 않는 경우
bin	기본 명령어 바이너리 소유자 그룹	현대 시스템에서는 거의 사용되지 않음
sys	시스템 파일 소유자 그룹	현대 시스템에서는 거의 사용되지 않음
games	게임 관련 그룹	게임 서비스가 제공되지 않는 경우
lp	인쇄 서비스 그룹	인쇄 서비스를 사용하지 않는 경우
mail	메일 서비스 그룹	메일 서비스를 사용하지 않는 경우
news	뉴스 서비스 그룹	뉴스 서비스를 사용하지 않는 경우
uucp	유닉스-유닉스 복사 그룹	UUCP 서비스가 제공되지 않는 경우
proxy	프록시 서비스 그룹	프록시 서비스를 사용하지 않는 경우
www-data	웹 서버 그룹	웹 서버가 제공되지 않는 경우
backup	백업 그룹	백업 서비스를 사용하지 않는 경우
list	메일링 리스트 그룹	메일링 리스트 서비스를 사용하지 않는 경우
irc	IRC 서비스 그룹	IRC 서비스를 사용하지 않는 경우
gnats	GNATS 버그 추적 시스템 그룹	GNATS 시스템이 사용되지 않는 경우
systemd-network	네트워크 관리 그룹	systemd-networkd를 사용하지 않는 경우
systemd-resolve	DNS 해석 서비스 그룹	systemd-resolved를 사용하지 않는 경우
syslog	시스템 로그 그룹	시스템 로그가 다른 방법으로 관리되는 경우
messagebus	D-Bus 메시지 버스 그룹	D-Bus 서비스를 사용하지 않는 경우
uuidd	UUID 생성 데몬 그룹	UUID 서비스가 사용되지 않는 경우
dnsmasq	DNS 및 DHCP 서비스 그룹	dnsmasq 서비스를 사용하지 않는 경우
avahi	Avahi 서비스 그룹	Avahi 서비스를 사용하지 않는 경우
usbmux	USB 장치 연결 관리 그룹	usbmuxd 서비스를 사용하지 않는 경우
rtkit	실시간 커널 지원 그룹	rtkit 서비스를 사용하지 않는 경우
cups-pk-helper	CUPS 정책 키트 그룹	CUPS를 사용하지 않는 경우
saned	SANE 데몬 그룹	SANE 서비스를 사용하지 않는 경우
nm-openvpn	NetworkManager OpenVPN 그룹	OpenVPN을 사용하지 않는 경우
hplip	HP 프린터 관리 그룹	HP 프린터를 사용하지 않는 경우
gdm	GNOME 디스플레이 매니저 그룹	GNOME 디스플레이 매니저를 사용하지 않는 경우
pulse	PulseAudio 사운드 서버 그룹	PulseAudio를 사용하지 않는 경우
sshd	OpenSSH 서버 그룹	SSH 서버를 사용하지 않는 경우

5. 취약 판단 기준

- 시스템 관리나 운용에 불필요한 그룹이 존재할 경우 취약하다고 판단

---

6. 점검 방법

6.1. /etc/group 파일 점검

```
cat /etc/group
```

---

7. 조치 방법

7.1. 불필요한 그룹이 있을 경우 제거 조치

```
sudo groupdel 그룹이름
```