U-49

- 분류 : 계정 관리
- 위험도 : 하

---

1. 점검 내용

- 시스템 계정 중 불필요한 계정(퇴직, 전직, 휴직 등의 이유로 사용하지 않는 계정 및 장기적으로 사용하지 않는 계정 등)이 존재하는지 점검

---

2. 점검 목적

- 불필요한 계정이 존재하는지 점검하여 관리되지 않은 계정에 의한 침입에 대비하는지 확인하기 위한 목적

---

3. 보안 위협

- 로그인이 가능하고 현재 사용하지 않는 불필요한 계정은 사용 중인 계정보다 상대적으로 관리가 취약하여 공격자의 목표가 되어 계정이 탈취 될 수 있음
  - 퇴직, 전직, 휴직 등의 사유 발생 시 즉시 권한을 회수한다

---

4. 참고

4.1. 불필요할 수도 있는 계정

계정 이름	역할	불필요할 수 있는 이유
daemon	시스템 서비스 데몬	특정 서비스가 사용되지 않는 경우
bin	기본 명령어 바이너리 소유자	현대 시스템에서는 거의 사용되지 않음
sys	시스템 파일 소유자	현대 시스템에서는 거의 사용되지 않음
sync	시스템 파일 동기화 계정	현대 시스템에서는 거의 사용되지 않음
games	게임 관련 시스템 계정	게임 서비스가 제공되지 않는 경우
man	매뉴얼 페이지 관리	매뉴얼 페이지가 변경되지 않는 경우
lp	인쇄 서비스 계정	인쇄 서비스를 사용하지 않는 경우

계정 이름	역할	불필요할 수 있는 이유
mail	메일 서비스 계정	메일 서비스를 사용하지 않는 경우
news	뉴스 서비스 계정	뉴스 서비스를 사용하지 않는 경우
uucp	유닉스-유닉스 복사 계정	UUCP 서비스가 제공되지 않는 경우
proxy	프록시 서비스 계정	프록시 서비스를 사용하지 않는 경우
www-data	웹 서버 계정	웹 서버가 제공되지 않는 경우
backup	백업 계정	백업 서비스를 사용하지 않는 경우
list	메일링 리스트 계정	메일링 리스트 서비스를 사용하지 않는 경우
irc	IRC 서비스 계정	IRC 서비스를 사용하지 않는 경우
gnats	GNATS 버그 추적 시스템 계정	GNATS 시스템이 사용되지 않는 경우
nobody	권한 없는 사용자 계정	거의 모든 시스템에 필요하지만 사용되지 않는 경우
systemd-network	네트워크 관리 계정	systemd-networkd를 사용하지 않는 경우
systemd-resolve	DNS 해석 서비스 계정	systemd-resolved를 사용하지 않는 경우
syslog	시스템 로그 계정	시스템 로그가 다른 방법으로 관리되는 경우
messagebus	D-Bus 메시지 버스 계정	D-Bus 서비스를 사용하지 않는 경우
uuidd	UUID 생성 데몬 계정	UUID 서비스가 사용되지 않는 경우
dnsmasq	DNS 및 DHCP 서비스 계정	dnsmasq 서비스를 사용하지 않는 경우
avahi	Avahi 서비스 계정	Avahi 서비스를 사용하지 않는 경우
usbmux	USB 장치 연결 관리 계정	usbmuxd 서비스를 사용하지 않는 경우
rtkit	실시간 커널 지원 계정	rtkit 서비스를 사용하지 않는 경우
cups-pk-helper	CUPS 정책 키트 계정	CUPS를 사용하지 않는 경우
saned	SANE 데몬 계정	SANE 서비스를 사용하지 않는 경우
nm-openvpn	NetworkManager OpenVPN 계정	OpenVPN을 사용하지 않는 경우
hplip	HP 프린터 관리 계정	HP 프린터를 사용하지 않는 경우
gdm	GNOME 디스플레이 매니저 계정	GNOME 디스플레이 매니저를 사용하지 않는 경우
pulse	PulseAudio 사운드 서버 계정	PulseAudio를 사용하지 않는 경우
sshd	OpenSSH 서버 계정	SSH 서버를 사용하지 않는 경우

---

5. 취약 판단 기준

- 불필요한 계정이 존재하는 경우 취약하다고 판단

---

6. 점검 방법

6.1. 미 사용 계정 및 의심스러운 계정 존재 여부 점검

```
cat /etc/passwd
```

6.2. 최근 로그인하지 않은 계정 및 의심스러운 계정 확인 (log 확인)

```
cat /var/log/wtmp
cat /var/log/sulog
```

---

7. 조치 방법

7.1. 불필요한 계정 삭제

```
userdel 사용자이름
```