U-53

- 분류 : 계정 관리
- 위험도 : 하

---

1. 점검 내용

- 로그인이 불필요한 계정에 쉘 부여 여부 점검

---

2. 점검 목적

- 로그인이 불필요한 계정에 쉘 설정을 제거하여, 로그인이 필요하지 않은 계 정을 통한 시스템 명령어를 실행하지 못하게 하기 위한 목적

---

3. 보안 위협

- 로그인이 불필요한 계정은 일반적으로 OS 설치 시 기본적으로 생성되는 계정으로 쉘이 설정되어 있을 경우, 공격자는 기본 계정들을 이용하여 시스템 에 명령어를 실행 할 수 있다

---

4. 참고

*쉘 부여 : 계정에 기본 쉘 프로그램을 지정한다는 의미이며 일반적으로
시스템 관리자 계정이나 일반 사용자 계정에는 /bin/bash, /bin/sh 와 같은 쉘이 할당되지만, 로그인이 불필요한 시스템 계정에는 /usr/sbin/nologin 또는 /bin/false 와 같은 쉘을 할당한다

4.1. 로그인에 불필요할 수 있는 계정

계정 이름	역할	기본 쉘	불필요할 수 있는 이유
daemon	시스템 서비스 데몬	/usr/sbin/nologin	특정 서비스가 사용되지 않는 경우
bin	기본 명령어 바이너리 소유자	/usr/sbin/nologin	현대 시스템에서는 거의 사용되지 않음
sys	시스템 파일 소유자	/usr/sbin/nologin	현대 시스템에서는 거의 사용되지 않음
sync	시스템 파일 동기화 계정	/bin/sync	현대 시스템에서는 거의 사용되지 않음
games	게임 관련 시스템 계정	/usr/sbin/nologin	게임 서비스가 제공되지 않는 경우
lp	인쇄 서비스 계정	/usr/sbin/nologin	인쇄 서비스를 사용하지 않는 경우
mail	메일 서비스 계정	/usr/sbin/nologin	메일 서비스를 사용하지 않는 경우
news	뉴스 서비스 계정	/usr/sbin/nologin	뉴스 서비스를 사용하지 않는 경우
uucp	유닉스-유닉스 복사 계정	/usr/sbin/nologin	UUCP 서비스가 제공되지 않는 경우
proxy	프록시 서비스 계정	/usr/sbin/nologin	프록시 서비스를 사용하지 않는 경우
www-data	웹 서버 계정	/usr/sbin/nologin	웹 서버가 제공되지 않는 경우
backup	백업 계정	/usr/sbin/nologin	백업 서비스를 사용하지 않는 경우
list	메일링 리스트 계정	/usr/sbin/nologin	메일링 리스트 서비스를 사용하지 않는 경우
irc	IRC 서비스 계정	/usr/sbin/nologin	IRC 서비스를 사용하지 않는 경우
gnats	GNATS 버그 추적 시스템 계정	/usr/sbin/nologin	GNATS 시스템이 사용되지 않는 경우
nobody	권한 없는 사용자 계정	/usr/sbin/nologin	거의 모든 시스템에 필요하지만 사용되지 않는 경우
systemd-network	네트워크 관리 계정	/usr/sbin/nologin	systemd-networkd를 사용하지 않는 경우
systemd-resolve	DNS 해석 서비스 계정	/usr/sbin/nologin	systemd-resolved를 사용하지 않는 경우
syslog	시스템 로그 계정	/usr/sbin/nologin	시스템 로그가 다른 방법으로 관리되는 경우
messagebus	D-Bus 메시지 버스 계정	/usr/sbin/nologin	D-Bus 서비스를 사용하지 않는 경우
uuidd	UUID 생성 데몬 계정	/usr/sbin/nologin	UUID 서비스가 사용되지 않는 경우
dnsmasq	DNS 및 DHCP 서비스 계정	/usr/sbin/nologin	dnsmasq 서비스를 사용하지 않는 경우
avahi	Avahi 서비스 계정	/usr/sbin/nologin	Avahi 서비스를 사용하지 않는 경우
usbmux	USB 장치 연결 관리 계정	/usr/sbin/nologin	usbmuxd 서비스를 사용하지 않는 경우
rtkit	실시간 커널 지원 계정	/usr/sbin/nologin	rtkit 서비스를 사용하지 않는 경우

계정 이름	역할	기본 쉘	불필요할 수 있는 이유
cups-pk-helper	CUPS 정책 키트 계정	/usr/sbin/nologin	CUPS를 사용하지 않는 경우
saned	SANE 데몬 계정	/usr/sbin/nologin	SANE 서비스를 사용하지 않는 경우
nm-openvpn	NetworkManager OpenVPN 계정	/usr/sbin/nologin	OpenVPN을 사용하지 않는 경우
hplip	HP 프린터 관리 계정	/usr/sbin/nologin	HP 프린터를 사용하지 않는 경우
gdm	GNOME 디스플레이 매니저 계정	/usr/sbin/nologin	GNOME 디스플레이 매니저를 사용하지 않는 경우
pulse	PulseAudio 사운드 서버 계정	/usr/sbin/nologin	PulseAudio를 사용하지 않는 경우
sshd	OpenSSH 서버 계정	/usr/sbin/nologin	SSH 서버를 사용하지 않는 경우

4.2. /bin/false 쉘

- 아무 작업도 하지 않고 즉시 종료되는 명령어
- 이 쉘을 사용자 계정에 할당 시 사용자가 로그인을 시도 할 때 아무 작업도 수행되지 않고 즉시 로그아웃 된다
- 주로 시스템 계정이나 로그인이 필요하지 않은 계정에 사용된다

4.3. /sbin/nologin 쉘

- 로그인을 차단하며 사용자가 로그인을 시도할 때 "This account is currently not available." 메세지 출력
- 시스템 계정이나 로그인이 필요하지 않은 계정에 사용되며 로그인 시도 시 명확한 메시지 제공한다

---

5. 취약 판단 기준

- 로그인이 필요하지 않은 계정에 쉘이 부여되지 않은 경우 취약하다고 판단

---

6. 점검 방법

6.1. /etc/passwd 파일 점검

```
cat /etc/passwd
```

- : (콜론) 으로 구분
- 마지막 필드가 계정의 쉘을 나타낸다

---

7. 조치 방법

7.1. /usr/sbin/nologin 쉘로 변경한다

```
sudo usermod -s /usr/sbin/nologin 사용자이름
```

7.2. /bin/false 쉘로 변경한다

```
sudo usermod -s /bin/false 사용자이름
```