U-22

- 분류 : 서비스 관리
- 위험도 : 상

---

1. 점검 내용

- Cron 관련 파일의 권한 적절성 점검

---

2. 점검 목적

- 관리자 외 cron 서비스를 사용할 수 없도록 설정하고 있는지 점검하는 것을 목적으로 한다

---

3. 보안 위협

- root 외 일반 사용자에게도 crontab 명령어를 사용할 수 있도록 할 경우, 고의 또는 실수로 불법적인 예약 파일 실행으로 시스템 피해를 일으킬 수 있다

---

4. 참고

- Cron 시스템 : 특정 작업을 정해진 시간에 주기적이고 반복적으로 실행하기 위한 데몬 및 설정

디렉토리	파일명	설명
`/etc/crontab`	crontab	예약작업을 등록하는 파일
`/etc/cron.d/`	cron.hourly	시간단위 실행 스크립트 등록
`/etc/cron.d/`	cron.daily	일단위 실행 스크립트 등록
`/etc/cron.d/`	cron.weekly	주단위 실행 스크립트 등록
`/etc/cron.d/`	cron.monthly	월 단위 실행 스크립트 등록
`/etc/cron.allow`	cron.allow	crontab 명령어 허용 사용자
`/etc/cron.deny`	cron.deny	crontab 명령어 차단 사용자

---

5. 취약 판단 기준

- crontab 명령어를 일반 사용자가 사용 가능 하거나, crond 관련 파일 640 이상인 경우 취약하다고 판단

---

6. 점검 방법

6.1. /etc/crontab 파일 점검

```
ls -al /usr/bin/crontab
```

6.2. 기타 cron 관련 파일 점검

```
# /etc/cron.d/ 디렉토리 내 파일들 권한 점검
ls -l /etc/cron.d/

# /etc/cron.hourly/ 디렉토리 내 파일들 권한 점검
ls -l /etc/cron.hourly/

# /etc/cron.daily/ 디렉토리 내 파일들 권한 점검
ls -l /etc/cron.daily/

# /etc/cron.weekly/ 디렉토리 내 파일들 권한 점검
ls -l /etc/cron.weekly/

# /etc/cron.monthly/ 디렉토리 내 파일들 권한 점검
ls -l /etc/cron.monthly/

# 사용자별 crontab 파일들 권한 점검
ls -l /var/spool/cron/crontabs/
```

---

7. 조치 방법

7.1. /usr/bin/crontab 파일 수정 조치

```
sudo chmod 750 /usr/bin/crontab
sudo chown root:crontab /usr/bin/crontab
```

- crontab 명령어 750 이하
- cron 관련 파일 소유자 및 권한 변경(소유자 root, 권한 640 이하)

7.2. cron 관련 파일 수정 조치

```
sudo find /etc/파일명/ -type f -exec chmod 640 {} \;
sudo find /etc/파일명/ -type f -exec chown root:root {} \;
```

- 권한 640 이하
- 소유자 root로 전환