U-47

- 분류 : 계정 관리
- 위험도 : 중

---

1. 점검 내용

- 시스템 정책에 패스워드 최대(90일 이하) 사용 기간 설정이 적용되어 있는지 점검

---

2. 점검 목적

- 패스워드 최대 사용 기간 설정이 적용되어 있는지 점검하여 시스템 정책에 서 사용자 계정의 장기간 패스워드 사용을 방지하고 있는지 확인하기 위한 목적

---

3. 보안 위협

- 패스워드 최대 사용기간을 설정하지 않은 경우 비인가자의 각종 공격(무작 위 대입 공격, 사전 대입 공격 등)을 시도할 수 있는 기간 제한이 없으므로 공격자 입장에서는 장기적인 공격을 시행할 수 있어 시행한 기간에 비례하 여 사용자 패스워드가 유출될 수 있는 확률이 증가한다

---

4. 취약 판단 기준

- 패스워드 최대 사용 기간이 90일(12주) 이하로 설정되어 있지 않는 경우 취약하다고 판단

---

5. 점검 방법

5.1. /etc/login.defs 파일 점검

```
cat /etc/login.defs
```

- PASS_MAX_DAYS 가 설정되어 있는지 확인

---

6. 조치 방법

6.1. /etc/login.defs 파일 수정 조치

```
sudo vim /etc/login.defs
```

- PASS_MAX_DAYS 90으로 설정