U-46

- 분류 : 계정 관리
- 위험도 : 중

---

1. 점검 내용

- 시스템 정책에 패스워드 최소(8자 이상) 길이 설정이 적용되어 있는 점검

---

2. 점검 목적

- 패스워드 최소 길이 설정이 적용되어 있는지 점검하여 짧은(8자 미만) 패스 워드 길이로 발생하는 취약점을 이용한 공격(무작위 대입 공격, 사전 대입 공격 등)에 대한 대비(사용자 패스워드 유출)가 되어 있는지 확인하기 위한 목적

---

3. 보안 위협

- 패스워드 문자열이 짧은 경우 유추가 가능 할 수 있으며 암호화된 패스워드 해시값을 무작위 대입공격, 사전대입 공격 등으로 단시간에 패스워드 크렉이 가능한다

---

4. 참고

- 패스워드 최소 길이를 8자리 이상으로 설정하여도 특수 문자, 대소문자, 숫자를 혼합하여 사용 하여 함

---

5. 취약 판단 기준

- 패스워드 최소 길이가 8자 미만으로 설정되어 있는 경우 취약하다고 판단

---

6. 점검 방법

6.1 /etc/pam.d/common-password 파일에서 최소 길이 점검

```
grep "minlen" /etc/pam.d/common-password
```

- 출력 예시 password requisite pam_pwquality.so retry=3 minlen=8

6.2. /etc/login.defs 파일에서 최소 길이 설정 점검

```
grep "^PASS_MIN_LEN" /etc/login.defs
```

- 출력 예시 PASS_MIN_LEN = 8

---

7. 조치 방법

```
sudo vim /etc/pam.d/common-password
sudo vim /etc/login.defs
```

- minlen=8
- PASS_MIN_LEN 8
  으로 수정조치