U-02

- 분류 : 계정 관리
- 위험도 : 상

---

1. 점검 내용

- 시스템 정책에 사용자 계정(root 및 일반 계정 모두 해당) 패스워드 복잡성 관련 설정이 되어 있는지 점검

---

2. 점검 목적

- 패스워드 복잡성 관련 정책이 설정되어 있는지 점검하여 비인가자의 공격(무 작위 대입 공격, 사전 대입 공격 등)에 대비가 되어 있는지 확인하기 위한 목적

---

3. 보안 위협

- 복잡성 설정이 되어있지 않은 패스워드는 사회공학적인 유추가 가능 할 수 있으며 암호화된 패스워드 해시값을 무작위 대입공격, 사전대입 공격 등으로 단시간에 패스워드 크렉이 가능하다

---

4. 참고

- 패스워드 복잡성: 사용자 패스워드 설정 시 영문(대문자, 소문자), 숫자, 특수문자가 혼합된 일정 길이 이상으로 패스워드를 설정하는 방법

---

5. 취약 판단 기준

- 패스워드 최소길이 8자리 이상, 영문·숫자·특수문자 최소 입력 기능이 설정된 경우 취약하다고 판단

---

6. 점검 방법

*이전 버전은 /etc/pam.d/common-password 에서 pam_unix.so, pam_cracklib.so 모듈 사용

6.1. /etc/security/pwquality.conf 파일 점검

```
cat /etc/security/pwquality.conf
```

*각 항목에서 -1 값은 반드시 해당하는 문자를 포함시켜야 한다

권장 값	기능	설명
lcredit=-1	최소 소문자 요구	소문자 최소 1자 이상 요구
ucredit=-1	최소 대문자 요구	최소 대문자 1자 이상 요구
dcredit=-1	최소 숫자 요구	최소 숫자 1자 이상 요구
ocredit=-1	최소 특수문자 요구	최소 특수문자 1자 이상 요구
minlen=8	최소 패스워드 길이 설정	최소 8자리 이상 설정
difok=N	기존 패스워드와 비교	기본값 10(50%)

---

7. 조치 방법

7.1. /etc/security/pwquality.conf 파일 수정 조치

```
sudo vim /etc/security/pwquality.conf
```

값

lcredit = -1
ucredit = -1
dcredit = -1
ocredit = -1
minlen = 8
difok = 10