U-02 (상)

1. 점검 내용

- 시스템 정책에 사용자 계정 패스워드 복잡성 관련 설정이 되어 있는지 점검

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

---

2. 점검 목적

- 패스워드 복잡성 관련 정책이 설정 되어 있는지 점검하여 비인가자의 공격(무작위 대입 공격, 사전 대입 공격) 에 대비가 되어 있는지 확인하기 위한 목적

---

3. 취약 판단 기준

- 패스워드 최소 길이 8자리 이상, 영문•숫자•특수문자 최소 입력 기능이 설정되지 않은 경우 취약하다고 판단

---

4. 점검 방법

4.1. /etc/security/pwquality.conf 파일

- minlen = 8
  - 최소 패스워드 길이 설정
- dcredit = -1
  - 최소 숫자 요구
- ucredit = -1
  - 최소 대문자 요구
- lcredit = -1
  - 최소 소문자 요구
- ocredit = -1
  - 최소 특수 문자 요구
- difok = 10
  - 기존 패스워드와 10자리 이상 다름을 요구

위와 같이 설정되어있는 지 점검

---

5. 보안 조치

- 계정과 유사하지 않은 8자 이상의 영문, 숫자, 특수 문자의 조합으로 암호 설정 및 패스워드 복잡성 옵션을 설정하도록 조치한다

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

점검 방법을 참고하여 복잡성 옵션 편집