

U-48

- 분류 : 계정 관리
 - 위험도 : 중
-

1. 점검 내용

- 시스템 정책에 패스워드 최소 사용 기간 설정이 적용되어 있는지 점검
-

2. 점검 목적

- 사용자가 자주 패스워드를 변경할 수 없도록 하고 관련 설정(최근 암호 기억)과 함께 시스템에 적용하여 패스워드 변경 전에 사용했던 패스워드를 재 사용 할 수 없도록 방지하는지 확인하기 위한 목적
-

3. 보안 위협

- 최소 사용기간이 설정되어 있지 않아 반복적으로 즉시 변경이 가능한 경우 이전 패스워드 기억 횟수를 설정하여도 반복적으로 즉시 변경하여 이전 패스워드로 설정이 가능하다
-

4. 참고

- 최근 암호 기억: 사용자가 현재 암호 또는 최근에 사용했던 암호와 동일한 새 암호를 만드는 것을 방지하는 설정. 예를 들어 값 1은 마지막 암호만 기억한다는 의미이며 값 5는 이전 암호 5개를 기억한다는 의미이다
-

5. 취약 판단 기준

- 패스워드 최소 사용 기간이 설정되어 있지 않는 경우 취약하다고 판단
-

6. 점검 방법

6.1. /etc/login.defs 파일 점검

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

PASS_MIN_DAYS 설정 확인

7. 조치 방법

7.1. /etc/login.defs 파일 수정 조치

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

- PASS_MIN_DAYS 1
 - 1 이상의 값