U-03

- 분류 : 계정 관리
- 위험도 : 상

---

1. 점검 내용

- 사용자 계정 로그인 실패 시 계정 잠금 임계값이 설정되어 있는지 점검

---

2. 점검 목적

- 계정 탈취 목적의 무작위 대입 공격 시 해당 계정을 잠금하여 인증 요청에 응답하는 리소스 낭비를 차단하고 대입 공격으로 인한 비밀번호 노출 공격 을 무력화하기 위한 목적

---

3. 보안 위협

- 패스워드 탈취 공격(무작위 대입 공격, 사전 대입 공격, 추측 공격 등)의 인 증 요청에 대해 설정된 패스워드와 일치 할 때까지 지속적으로 응답하여 해 당 계정의 패스워드가 유출 될 수 있다

---

4. 참고

- 사용자 로그인 실패 임계값 : 시스템에 로그인 시 몇 번의 로그인 실패에 로그인을 차 단할 것인지 결정하는 값

---

5. 취약 판단 기준

- 계정 잠금 임계값이 설정되어 있지 않거나, 10회 이하의 값으로 설정되지 않은 경우 취약하다고 판단

---

6. 점검 방법

*이전 버전에서는 pam_tally, pam_tally2 모듈 사용

6.1. /etc/pam.d/common-auth 파일 점검

```
grep "pam_faillock.so" /etc/pam.d/common-auth
```

다음과 같은 설정이 활성화 되어 있는지 확인

auth required pam_faillock.so preauth silent deny=5 unlock_time=600 fail_interval=900

auth [default=die] pam_faillock.so authfail deny=5 unlock_time=600 fail_interval=900

- deny : 허용된 최대 로그인 실패 횟수
- unlock_time : 계정 잠금이 해제되기까지의 시간(초)
- fail_interval : 로그인 실패 간격(초)

---

7. 조치 방법

7.1. /etc/pam.d/common-auth 파일 설정 조치

```
sudo vim /etc/pam.d/common-auth
```

아래 예시 추가

auth required pam_faillock.so preauth silent deny=5 unlock_time=600 fail_interval=900

auth [default=die] pam_faillock.so authfail deny=5 unlock_time=600 fail_interval=900