U-04

- 분류 : 계정 관리
- 위험도 : 상

---

1. 점검 내용

시스템의 사용자 계정 정보가 저장된 파일에 사용자 계정 패스워드가 암호화되어 저장되어 있는지 점검

---

2. 점검 목적

- 일부 오래된 시스템의 경우 /etc/passwd 파일에 패스워드가 평문으로 저장 되므로 사용자 계정 패스워드가 암호화되어 저장되어 있는지 점검하여 비인가자의 패스워드 파일 접근 시에도 사용자 계정 패스워드가 안전하게 관리 되고 있는지 확인하기 위한 목적

---

3. 보안 위협

- 사용자 계정 패스워드가 저장된 파일이 유출 또는 탈취 시 평문으로 저장된 패스워드 정보가 노출될 수 있다

---

4. 참고

- 관련 점검 항목 : U-07(상), U-08(상)

---

5. 취약 판단 기준

- 패스워드를 암호화하여 저장하지 않는 경우 취약하다고 판단

---

6. 점검 방법

6.1. /etc/passwd 파일 점검

```
cat /etc/passwd
#패스워드 필드가 x로 설정되지 않은 모든 라인 출력
grep -v '^[^:]*:x:' /etc/passwd
```

- 파일에서 패스워드 필드가 x로 설정되어 있는지 확인한다
  - x 는 패스워드가 /etc/shadow 파일에 암호화 되어 저장된다는 것을 의미한다

6.2. /etc/shadow 파일 점검

```
#암호화 되지 않은 패스워드가 저장된 항목을 출력하고 Not OK 를 붙여준다
cat /etc/shadow
```

- 시스템 계정 들은 일반적으로 로그인이 불가능한 상태로 설정된다
- 만약 사용자 계정(실제로 로그인이 필요한 계정)들이 암호화되지 않은 패스워드를 가지고 있다면 취약

예시

```
hee:$6$ZTGDxLwxwsF22eSS$Daw7bdltW5uL4jSeug.HLt3CexLN4YSv.oAvFd3RxcO9Cb4uayVJdNO8V92/rzaj
C8gGiyMkkUfpIccdzI01k/:19932:0:99999:7:::
```

- hee : 사용자 이름
- (SHA-512 알고리즘)암호화 된 패스워드 6ZTGDxLwxwsF22eSS$Daw7bdltW5uL4jSeug.HLt3CexLN4YSv.oAvFd3RxcO9Cb4uayVJdNO8V92/rzajC8gGiyMkkUfpIccdzI01k/
- 19932 : 마지막 패스워드 변경일 (1970년 1월 1일부터 패스워드가 마지막으로 변경된 날까지의 일수)
- 0 : 최소 일수 (패스워드를 변경할 수 있는 최소 일수 : 현재 얼마든지 패스워드 변경 가능)
- 99999 : 최대 일수 (패스워드를 변경해야 하는 최대 일수 : 패스워드 만료 없음)
- 7 : 경고 일수 (패스워드가 만료되기 전 경고하는 일수)
- () : 만료일 (계정이 만료되는 날짜)
- () : 예약 필드 (파일 구조의 유연성을 보장하기 위해 존재)

---

7. 조치 방법

7.1. pwconv - 쉐도우 패스워드 정책 활성화 조치

- /etc/passwd 파일에서 제거하고 암호화된 패스워드를 /etc/shadow 파일에 저장하도록 전환한다

```
sudo pwconv
```