U-20

- 분류 : 서비스 관리
- 위험도 : 상

---

1. 점검 내용

- 익명 FTP 접속 허용 여부 점검

---

2. 점검 목적

- 실행 중인 FTP 서비스에 익명 FTP 접속이 허용되고 있는지 확인하여 접속허용을 차단하기 위한 목적

---

3. 보안 위협

- Anonymous FTP(익명 FTP)를 사용 시 anonymous 계정으로 로그인 후 디렉터리에 쓰기 권한이 설정되어 있다면 악의적인 사용자가 local exploit을 사용하여 시스템에 대한 공격을 가능하게 할 수 있다

---

4. 참고

- Anonymous FTP (익명 FTP)
  - 파일 전송을 위해서는 원칙적으로 상대방 컴퓨터를 사용할 수 있는 계정이 필요하나 누구든지 계정 없이도 anonymous 또는 ftp 라는 로그인 명과 임의의 비밀번호를 사용하여 FTP를 실행할 수 있다

---

5. 취약 판단 기준

- Anonymous FTP (익명 ftp) 접속을 차단하지 않은 경우 취약하다고 판단

---

6. 점검 방법

6.1. /etc/passwd 파일 점검

```
grep -E '^ftp|^anonymous' /etc/passwd
```

- ftp 또는 anonymous 계정의 존재 여부를 확인할 수 있다

6.2. /etc/vsftpd.conf 파일 점검

```
sudo grep anonymous_enable /etc/vsftpd.conf
```

- anonymous_enable 값을 통해 익명 접속 허용 가능
  - YES : 접속 허용
  - NO : 접속 비허용

---

7. 조치 방법

7.1. /etc/passwd 파일 수정

```
sudo usermod -s /usr/sbin/nologin ftp
sudo usermod -s /usr/sbin/nologin anonymous
```

- ftp 및 anonymous 계정의 로그인 셸을 nologin으로 설정하여 해당 계정의 로그인을 차단

7.2. /etc/vsftpd.conf 파일 수정

```
sudo vim /etc/vsftpd.conf
sudo systemctl restart vsftpd
```

- anonymous_enable 라인을 찾아 NO로 변경 후 서비스 재시작