U-31

- 분류 : 서비스 관리
- 위험도 : 상

---

1. 점검 내용

- SMTP 서버의 릴레이 기능 제한 여부 점검

---

2. 점검 목적

- 스팸 메일 서버로의 악용 방지 및 서버 과부하의 방지를 위함

---

3. 보안 위협

- SMTP 서버의 릴레이 기능을 제한하지 않는 경우, 악의적인 사용목적을 가 진 사용자들이 스팸메일 서버로 사용하거나 Dos공격의 대상이 될 수 있다

---

4. 참고

- SMTP(Simple Mail Transfer Protocol) 서버 : 인터넷상에서 전자우편(E-mail)을 전송할 때 이용하게 되는 표준 통신 규약을 SMTP라고 하며, SMTP에 의해 전자 메일을 발신 하는 서버(server)를 SMTP 서버라고 한다

---

5. 취약 판단 기준

- SMTP 서비스를 사용하며 릴레이 제한이 설정되어 있지 않은 경우 취약하다고 판단

---

6. 점검 방법

6.1. Postfix 설정 파일 점검

```
grep 'smtpd_recipient_restrictions' /etc/postfix/main.cf
```

- /etc/postfix/main.cf 파일에서 smtpd_recipient_restrictions 옵션 확인
- 출력결과에 reject_unauth_destination 포함 되어 있는지 확인

---

7. 조치 방법

7.1. 릴레이 제한 설정 (/etc/postfix/main.cf 파일 수정 조치)

```
sudo vim /etc/postfix/main.cf
```

- smtpd_recipient_restrictions = permit_mynetworks, permit_sasl_authenticated, reject_unauth_destination 추가

7.2. Postfix 서비스를 재시작

```
sudo systemctl restart postfix
```