# U-32

- 분류 : 서비스 관리
- 위험도 : 상

---

## 1. 점검 내용

- SMTP 서비스 사용 시 일반사용자의 q 옵션 제한 여부 점검

---

## 2. 점검 목적

- 일반사용자의 q 옵션을 제한하여 Sendmail 설정 및 메일큐를 강제적으로 drop 시킬 수 없게 하여 비인가자에 의한 SMTP 서비스 오류 방지 목적

---

## 3. 보안 위협

- 일반 사용자가 q 옵션을 이용해서 메일큐, Sendmail 설정을 보거나 메일큐 를 강제적으로 drop 시킬 수 있어 악의적으로 SMTP 서버의 오류를 발생시 킬 수 있다

---

## 4. 참고

- SMTP(Simple Mail Transfer Protocol): 인터넷상에서 전자우편(E-mail)을 전송할 때 이 용하게 되는 표준 통신 규약을 말한다

---

# 5. 취약 판단 기준

- SMTP 서비스 사용 및 일반 사용자의 Sendmail 실행 방지가 설정되어 있지 않은 경우 취약하다고 판단

---

# 6. 점검 방법

## 6.1. sendmail.cf 또는 submit.cf 파일에서 QueueDirectory 옵션 확인

```
grep -i "QueueDirectory" /etc/mail/sendmail.cf /etc/mail/submit.cf
```

---

# 7. 조치 방법

## 7.1. Sendmail 서비스를 사용하지 않을 경우 서비스 중지 조치

```
sudo systemctl stop sendmail
sudo systemctl disable sendmail
```

## 7.2. Sendmail 서비스를 사용할 경우 설정 파일에 q 옵션 추가 조치

```
sudo vim /etc/mail/sendmail.cf
sudo systemctl restart sendmail #재부팅
```

- O restrictqrun 추가