U-30

- 분류 : 서비스 관리
- 위험도 : 상

---

1. 점검 내용

- 취약한 버전의 Sendmail 서비스 이용 여부 점검

---

2. 점검 목적

- Sendmail 서비스 사용 목적 검토 및 취약점이 없는 버전의 사용 유무 점검 목적

---

3. 보안 위협

- 취약점이 발견된 Sendmail 버전의 경우 버퍼 오버플로우(Buffer Overflow) 공격에 의한 시스템 권한 획득 및 주요 정보 요출 가능성이 있다

---

4. 참고

- Sendmail 서비스의 경우 최신버전 (2016.01 기준 8.15.2) 이하 대부분의 버전에서 취약점이 보고되고 있기 때문에 O/S 관리자, 서비스 개발자가 패치 적용에 따른 서비스 영향 정도를 정확히 파악하고 주기적인 패치 적용 정책을 수립하여 적용한다

---

5. 취약 판단 기준

- Sendmail 버전이 최신버전이 아닌 경우 취약하다고 판단

---

6. 점검 방법

6.1. Sendmail 버전 점검

```
sendmail -d0.1 -bv root | grep -oP 'Version \K[0-9\.]+'
```

---

7. 조치 방법

7.1. Sendmail 서비스 중지 / 삭제

```
sudo systemctl stop sendmail
sudo apt-get remove --purge sendmail
```

7.2. Sendmail 패키지 업데이트 후 재부팅

```
sudo apt-get update
sudo apt-get install --only-upgrade sendmail
sudo systemctl start sendmail
```