U-33

- 분류 : 서비스 관리
- 위험도 : 상

---

1. 점검 내용

- BIND 최신 버전 사용 유무 및 주기적 보안 패치 여부 점검

---

2. 점검 목적

- 취약점이 발표되지 않은 BIND 버전의 사용 목적

---

3. 보안 위협

- 최신버전(2016.01 기준 9.10.3-P2) 이하의 버전에서는 서비스거부 공격, 버퍼 오버플로우(Buffer Overflow) 및 DNS 서버 원격 침입 등의 취약성이 존재한다

---

4. 참고

- BIND(Berkeley Internet Name Domain) : BIND는 BSD 기반의 유닉스 시스템을 위해 설계된 DNS로 서버와 resolver 라이브러리로 구성되어 있다
  - 네임서버는 클라이언트들이 이름 자원들이나 객체들에 접근하여, 네트워크 내의 다른 객체들과 함께 정보를 공유 할 수 있게 해주는 네트워크 서비스로 사실상 컴퓨터 네트워크 내의 객체들을 위한 분 산 데이터베이스 시스템이다

---

5. 취약 판단 기준

- DNS 서비스를 사용하며 주기적으로 패치를 관리하고 있지 않는 경우 취약하다고 판단

---

6. 점검 방법

6.1. BIND 서비스 실행 중인지 점검

```
ps -ef | grep named
```

6.2. 설치된 BIND 버전 확인

```
named -v
```

---

7. 조치 방법

7.1. DNS 서비스를 사용하지 않는 경우

```
sudo systemctl stop bind9
sudo systemctl disable bind9
```

- 서비스 중지 후 비활성화

7.2. DNS 서비스를 사용할 경우 업데이트 조치

```
sudo apt update
sudo apt install bind9

# 자동 업데이트 설정
sudo apt install unattended-upgrades
sudo dpkg-reconfigure --priority=low unattended-upgrades
```