U-34

- 분류 : 서비스 관리
- 위험도 : 상

---

1. 점검 내용

- Secondary Name Server로만 Zone 정보 전송 제한 여부 점검

---

2. 점검 목적

- 허가되지 않는 사용자에게 Zone Transfer를 제한함으로써 호스트 정보, 시스템 정보 등 정보 유출의 방지를 목적

---

3. 보안 위협

- 비인가자 Zone Transfer를 이용해 Zone 정보를 전송 받아 호스트 정보, 시스템 정보, 네트워크 구성 형태 등의 많은 정보를 파악할 수 있다

---

4. 참고

- DNS Zone Transfer는 Primary Name Server와 Secondary Name Server 간에 Zone 정보를 일관성 있게 유지하기 위하여 사용하는 기능

---

5. 취약 판단 기준

- DNS 서비스를 사용하며 Zone Transfer를 모든 사용자에게 허용한 경우 취약하다고 판단

---

6. 점검 방법

6.1. BIND 설정 파일 Zone Transfer 설정 점검

```
sudo grep -i "allow-transfer" /etc/bind/named.conf*
```

- named.conf 파일과 관련된 파일들에서 allow-transfer 설정을 검색
- 설정 파일에서 allow-transfer 옵션이 있는지 확인
  - 없다면 모든 사용자에게 Zone Transfer 이 허용된 상태일 수 있다

---

7. 조치 방법

7.1. DNS 서비스 사용중이지 않은 경우

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

- 서비스 중지

7.2. DNS 서비스를 사용중인 경우 BIND 설정 파일 수정

```
sudo vim /etc/bind/named.conf
```

- (예시) allow-transfer { 192.0.2.1; 192.0.2.2; }