U-23

- 분류 : 서비스 관리
- 위험도 : 상

---

1. 점검 내용

- 사용하지 않는 Dos 공격에 취약한 서비스의 실행 여부 점검

---

2. 점검 목적

- 시스템 보안성을 높이기 위해 취약점이 많이 발표된 echo, discard, daytime, chargen, ntp, snmp 등 서비스를 중지하려는 목적

---

3. 보안 위협

- 해당 서비스가 활성화되어 있는 경우 시스템 정보 유출 및 DoS(서비스 거부 공격)의 대상이 될 수 있다

---

4. 참고

- DoS(Denial of Service attack) : 시스템을 악의적으로 공격해 해당 시스템의 자원을 부족 하게 하여 원래 의도된 용도로 사용하지 못하게 하는 공격. 특정 서버에게 수많은 접속 시도를 만들어 다른 이용자가 정상적으로 서비스 이용을 하지 못하게 하거나, 서버의 TCP 연결을 바닥 내는 등의 공격이 이 범위에 포함된다

4.1. DoS 공격에 취약한 서비스

서비스 이름	역할	디도스 공격에 취약한 이유
Echo	디버깅 및 테스트 서비스	대량의 패킷을 반사하여 증폭 공격에 사용될 수 있음
Discard	디버깅 및 테스트 서비스	대량의 패킷을 버려야 하므로 서버 자원을 소모시킬 수 있음
Daytime	시간 및 날짜 서비스	불필요한 대량의 요청으로 서버 자원을 소모시킬 수 있음
Chargen	문자 생성 서비스	대량의 패킷을 생성하여 네트워크 대역폭을 소모시키는 증폭 공격에 사용될 수 있음
NTP (Network Time Protocol)	네트워크 시간 동기화 서비스	대량의 시간 동기화 요청으로 인해 서버 자원이 고갈될 수 있음
DNS (BIND)	도메인 네임 시스템 서비스	대량의 DNS 쿼리를 통해 서버 자원을 소모시키고, 증폭 공격에 사용될 수 있음
SNMP (Simple Network Management Protocol)	네트워크 관리 프로토콜	대량의 관리 요청으로 인해 서버 자원이 고갈될 수 있으며, 잘못된 설정 시 민감한 정보가 유출될 수 있음

---

5. 취약 판단 기준

- 사용하지 않는 DoS 공격에 취약한 서비스가 활성화 된 경우 취약하다고 판단

---

6. 점검 방법

6.1. Echo, Discard, Daytime, Chargen 서비스 점검

```
# xinetd 사용 시
sudo grep -rE "echo|discard|daytime|chargen" /etc/xinetd.d/

# inetd 사용 시
sudo grep -E "echo|discard|daytime|chargen" /etc/inetd.conf
```

6.2. NTP (Network Time Protocol) 점검

```
# ntpd 서비스 상태 확인
sudo systemctl status ntp

# chrony 서비스 상태 확인
sudo systemctl status chrony
```

6.3. DNS(BIND) 점검

```
sudo systemctl status named
```

6.4. SNMP (Simple Network Management Protocol) 점검

```
sudo systemctl status snmpd
```

---

7. 조치 방법

7.1. 필요없는 서비스 비활성화 조치

```
sudo systemctl disable 서비스이름
sudo systemctl stop 서비스이름
```