U-27

- 분류 : 서비스 관리
- 위험도 : 상

---

1. 점검 내용

- 불필요한 RPC 서비스의 실행 여부 점검

---

2. 점검 목적

- 다양한 취약성(버퍼 오버플로우, Dos, 원격실행 등)이 존재하는 RPC 서비스 를 점검하여 해당 서비스를 비활성화 하도록 하는 목적

---

3. 보안 위협

- 버퍼 오버플로우(Buffer Overflow), Dos, 원격실행 등의 취약성이 존재하는 RPC 서비스를 통해 비인가자의 root 권한 획득 및 침해사고 발생 위험이 있 으므로 서비스를 중지하여야 한다

---

4. 참고

- RPC(Remote Procedure Call) : 별도의 원격 제어를 위한 코딩 없이 다른 주소 공간에서 함수나 프로시저를 실행할 수 있게 하는 프로세스 간 프로토콜

4.1. 불필요한 RPC 서비스

서비스 이름	역할	불필요한 이유
rpc.cmsd	캘린더 관리 서비스 데몬	현대적인 캘린더 관리 솔루션이 많이 사용되므로 필요 없음
rpc.ttdbserverd	툴톡 데이터베이스 서버 데몬	오래된 툴톡 데이터베이스 서버, 거의 사용되지 않음
sadmind	솔리스티스 어드민스위트 관리 데몬	Solstice AdminSuite는 거의 사용되지 않음
rusersd	원격 사용자 목록 서비스	rusers 명령을 지원하는 데몬, 보안 위험이 높고 거의 사용되지 않음
walld	모든 사용자에게 메시지를 보낼 수 있게 해주는 데몬	보안 위험이 높고 거의 사용되지 않음
sprayd	네트워크 테스트 도구 spray를 위한 데몬	보안 위험이 높고 거의 사용되지 않음
rstatd	원격 시스템 통계 수집을 위한 데몬	보안 위험이 높고 거의 사용되지 않음
rpc.nisd	네트워크 정보 서비스(NIS) 서버	NIS는 오래된 네트워크 정보 서비스, 보안 위험이 높고 현대적인 LDAP나 다른 솔루션으로 대체됨
rexd	원격 실행을 지원하는 데몬	보안 위험이 높고 거의 사용되지 않음
rpc.pcnfsd	오래된 PC-NFS 프로토콜을 위한 데몬	보안 위험이 높고 거의 사용되지 않음
rpc.statd	NFS 파일 잠금 서비스를 위한 데몬	NFSv4에서는 필요 없음
rpc.ypupdated	NIS 맵을 업데이트하는 데몬	보안 위험이 높고 거의 사용되지 않음
rpc.rquotad	원격 파일 시스템 쿼터를 관리하는 데몬	거의 사용되지 않음
kcms_server	오래된 KCMS(컬러 매니지먼트 시스템) 서버	거의 사용되지 않음
cachefsd	캐시 파일 시스템을 위한 데몬	현대적인 파일 시스템에서는 필요 없음

---

5. 취약 판단 기준

- 불필요한 RPC 서비스가 활성화 되어 있는 경우 취약하다고 판단

---

6. 점검 방법

```
cat /etc/inetd.conf
```

---

7. 조치 방법

7.1. /etc/inetd.d 디렉터리 내 불필요한 RPC 서비스 파일 열기

```
sudo vim /etc/inetd.d/불필요한 RPC 서비스 파일
```

- Disable = yes 설정

```
service finger
{
        disable             = yes
        socket_type         = stream
        wait                = no
```