U-21

- 분류 : 서비스 관리
- 위험도 : 상

---

1. 점검 내용

- r-command 서비스 비활성화 여부 점검

---

2. 점검 목적

- r-command 사용을 통한 원격 접속은 NET Backup 또는 클러스터링 등 용도로 사용되기도 하나, 인증 없이 관리자 원격접속이 가능하여 이에 대한 보안위협을 방지하고자 하는 목적

---

3. 보안 위협

- rsh, rlogin, rexec 등의 r command를 이용하여 원격에서 인증절차 없이 터미널 접속, 쉘 명령어를 실행이 가능하다

---

4. 참고

- r-command : 인증 없이 관리자의 원격 접속을 가능하게 하는 명령어들
  - rsh(remsh), rlogin, rexec, rsync 등
- NET Backup : 데이터 백업 및 복구를 위한 소프트웨어 시스템
- 클러스터링 : 여러 개의 컴퓨터를 하나의 시스템처럼 동작하게 만드는 기술

---

5. 취약 판단 기준

- 불필요한 r 계열 서비스가 활성화 되어 있는 경우 취약하다고 판단

---

6. 점검 방법

6.1. /etc/xinetd.d/ 디렉터리 점검

```
sudo grep -rE "service rsh|service rlogin|service exec" /etc/xinetd.d/
```

- rsh, rlogin, rexec 서비스 설정을 검색

---

7. 조치 방법

7.1. /etc/xinetd.d/ 디렉터리 수정

```
sudo vim /etc/xinetd.d/rsh
sudo vim /etc/xinetd.d/rlogin
sudo vim /etc/xinetd.d/rexec
sudo systemctl restart xinetd
```

- disable 옵션 yes로 설정 후 재시작

```
service     rlogin
{
          socket_type             = stream
          wait                    = no
          user                    = nobody
          log_on_success          += USERID
          log_on_failure          += USERID
          server                  = /usr/sdin/in.fingerd
          disable                 = yes
}
```