

# Bash 임의코드 실행 취약점 보안업데이트

Bash 보안업데이트하세요~~

1. 취약내용 : 공격자가 Bash를 사용하여 구현된 기능을 악용하여 임의의 코드를 실행시킬수 있으므로 업데이트 권고
2. 대상 : GNU Bash를 사용하는 서버 (RHEL계열 4이하 버전은 지원이 끝났기 때문에 업데이트 불가능합니다.)
3. RHEL4이하버전은 yum으로 업데이트 불가하고, 대신에 수동으로 패치를 진행해야 합니다.
4. Bash는 리눅스에서 기본으로 사용하고 있는 셸이기 때문에 대부분 업데이트를 진행하셔야 할것 같습니다.

## 패치작업 진행

### 1. 취약점 대상 시스템 여부

```
[root@localhost ~]# env x='()' { :}; echo vulnerable' bash -c "echo this is a test"
vulnerable
this is a test
(vulnerable메시지가 출력되면 업데이트가 필요한 버전입니다.)
```

### 2. 보안업데이트 방법

```
[root@localhost ~]# yum update bash -y
```

### 3. 조치완료여부 확인

```
[root@localhost ~]# env x='()' { :}; echo vulnerable' bash -c "echo this is a test"
this is a test
```

### 4. bash업데이트 이후 서비스의 재시작/재부팅은 필요없으나, 재시작이 필요한 서비스를 확인하고 싶으면 명령어 실행

```
[root@localhost ~]# grep -l -z '[^)]='() {' /proc/[1-9]*/environ | cut -d/ -f3
```

## Reference

- <https://rhn.redhat.com/errata/RHSA-2014-1293.html>
- <https://access.redhat.com/articles/1200223////>

🕒Revision #1

★Created 7 June 2022 02:33:17 by artop0420

✎Updated 24 December 2023 00:40:03 by artop0420