"긴급 송부(보안경고 2014-019)" GNU Bash(Bourne Again Shell) 코드 인젝션 취약점 관련 금융회사 자체점검 및 패치 적용 권고 - (V2.0)

보안서비스본부 민상식 팀장, 조병열 인턴 / 2014. 9. 30

□ 개 요

o Bash(Bourne Again Shell) 코드 인젝션 취약점이 발견됨[1]에 따라 조속한 조치가 요구되므로 이를 전파함

□ 위험도 및 긴급도

구분	위험도	긴급도
등급	상	상

□ 취약점 내용

o GNU Bash 명령 인젝션 취약점(CVE-2014-6271, 일명 "Shellshock")[2]

o CVE-2014-6271 보안 업데이트가 불완전하여 여전히 취약점 존재(CVE-2014-7169)[3]

o 원격지에서 DOS 공격 등이 가능한 취약점(CVE-2014-7186, CVE-2014-7187)[4][5]

구분	내용
공격 위협	· 계정의 기본 쉘이 bash 쉘이고, 취약한 버전을 사용하고 있을 경우(현재까지 나온 4.3이하 모두 취약), 취약점에 의한 원격지 또는 내부자에 의한 공격이 가능하므로 관리자의 조치 필요
영향 받는 소프트웨어	· GNU Bash 4.3 이하 버전을 사용하는 시스템 (리눅스, Mac OS X, Cygwin 등 Bash를 기본으로 시용하는 운영체제 또는 AIX, Solaris, HP-UX, FreeBSD등 bash 쉘이 기본 쉘은 아니지만 설정에 의해 이용할 수 있는 운영체제)
기타	· Bash 명령어가 실행 가능한 모든 서비스에서 코드 인젝션, DoS 공격 가능 · 해당 취약점을 이용한 Exploit 코드가 공개됨 · 해당 취약점을 이용한 공격이 해외에서 발견됨

※ 쉘의 종류에는 Bourne Shell(sh, 1977년 Unix V7의 기본 쉘), C Shell(csh, 1978년 발표), Korn Shell(ksh, 1983년 발표),GNU Bourne-Again Shell(bash, 1989년 발표) 등이 있음.

※ AIX는 Bourne Shell(version 3까지)과 Korn Shell(version 4)를 기본 쉘로 이용

1) 2014년 9월 24일(미국 현지 기준) 취약점 내용이 공개됨
2) http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2014-6271 (미국 현지시간으로 9.24 발표)
3) http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2014-7169 (미국 현지시간으로 9.24 발표)
4) http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2014-7186 (미국 현지시간으로 9.28 발표)
5) http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2014-7187 (미국 현지시간으로 9.28 발표)

□ 대응 권고 사항

o 긴급 조치 권고

- Apache HTTP Server를 실행시키는 계정의 기본 쉘이 bash이고, mod_cgi, mod_cgid 모듈을 활용하는 경우 원격지에서 악의적인 코드 실행이 가능하고,
- 원격지에서 DoS 공격이 가능한 취약점이 추가로 발견되어 서비스 거부공격 등의 위협이 있어,
- bash 쉘을 기본 쉘로 이용하고 있는 계정으로, 중요 서비스 프로그램(웹 서버 실행, 서비스 프로그램 실행 등)을 실행시키는 경우 긴급한 패치가 필요함

※ 금융회사 외부에서 원격공격 가능성이 있어 즉시 관련조치를 수행할 필요가 있음
(각 계정의 기본 쉘을 조사하여 bash인 경우를 파악하고, 계정이 수행하는 역할을

o 일반 대응 권고

※ 금융회사 외부에서 원격공격은 어려우나 해당 취약점에 대한 패치계획을 수립하고 업데이트를 수행할 필요가 있음

- 외부에서 금융회사 서버로 SSH 접근(OpenSSH sshd)이 가능하고, 해커가 계정정보까지 알고 있는 경우
  => 제한된 명령만 실행가능하게 하는 ForceCommand 제약을 우회할 수 있음
- DHCP 서버에 악의적 코드가 추가된 경우[6)]
  => Bash 취약점에 의해 다수의 DHCP Client 장비에서 동시에 임의의 명령이 실행될 수 있음
- 서버에 접근이 가능한 내부자가 "권한을 가지는 데몬"에서 쉘 스크립트를 실행할 수 있는 경우
  => 이 취약점을 이용하여 데몬의 권한으로 임의의 명령을 실행할 수 있음

6) https://www.trustedsec.com/september-2014/shellshock-dhcp-rce-proof-concept/

o 현 시점에서 대응방안

- **(보안 업데이트) Bash 쉘 관련 패치 실시**
- **(네트워크 방어) F/W, IDS, IPS 등의 방어장비를 이용하여 원격지에서 들어오는 Bash 관련 취약점 공격방어를 위한 룰(Rule) 업데이트**
  ※ 무선 AP, 네트워크 장비에서 Bash 쉘을 이용하는 경우에 대하여 상세 확인이 필요할 것으로 보임
- (서버설정 변경) 불필요한 CGI 관련 기능은 DISABLE
- (서버설정 변경) Bash 쉘을 다른 쉘로 변경하여 이용하는 것도 가능하나 추가적인 영향을 신중히 고려하여야 함

[붙임1] Bash 쉘 취약점 관련 상세 점검 및 대응방안[7]

□ Bash 쉘 이용여부 확인

o 이용 중인 쉘 종류 확인

```
$ echo $SHELL
/bin/bash
```

o Bash 이용하는 경우 버전 확인 : GNU Bash 4.3 및 이전 버전이면 취약

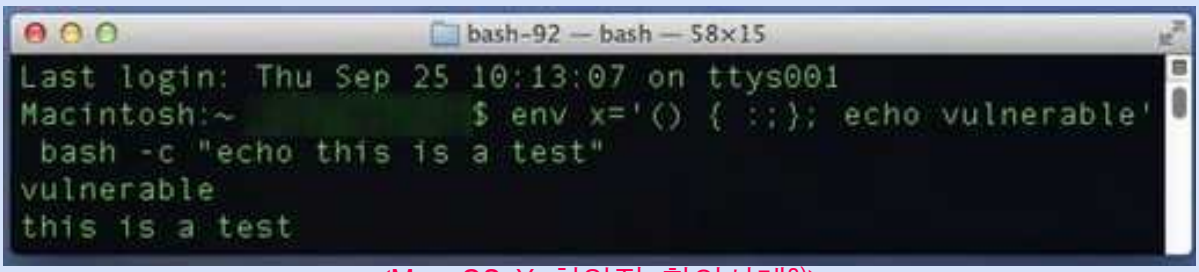
```
"bash -v" 또는 "bash —version" 또는 "echo $BASH_VERSION" 명령어 입력
(예시) $ echo $BASH_VERSION
        4.2.37(1)-release
```

□ CVE-2014-6271, CVE-2014-7169 취약점 확인방법

o CVE-2014-6271 취약점 점검방법

```
[명령어 입력]
env x='() { :;}; echo VULNERABLE' bash -c :
```

[결과] - 취약한 경우
VULNERABLE



<Mac OS X 취약점 확인사례[8]>

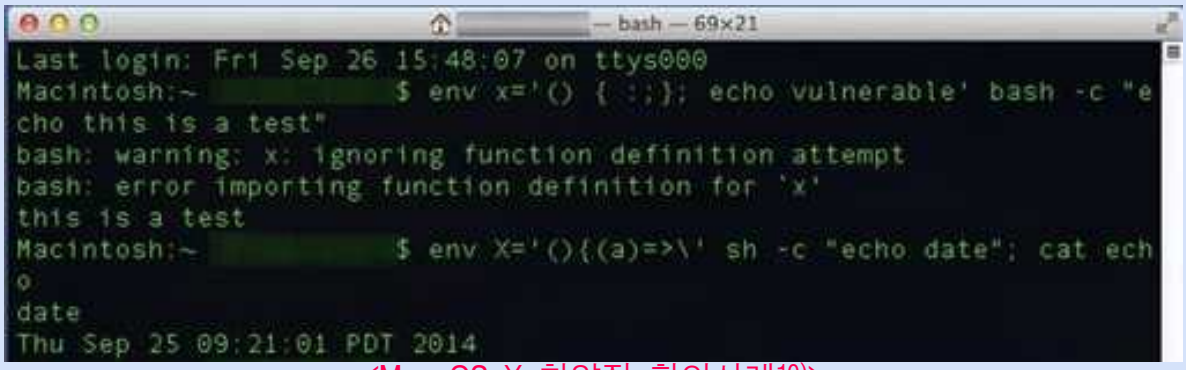
[결과] - 패치된 경우
bash: warning: x: ignoring function definition attempt
bash: error importing function definition for 'x'

o CVE-2014-7169 취약점 점검방법 - (Redhat 기준예제)[9]

```
[명령어 입력]
cd /tmp; rm -f /tmp/echo; env 'x=() { (a)=>\' bash -c "echo date"; cat /tmp/echo
```

7) KISA 취약점분석팀 "GNU Bash 원격명령 실행 취약점 대응방안 권고, 2014.9.26" 자료 일부 인용
http://boho.or.kr/upload/file/EpF854.pdf
8) http://mac-how-to.wonderhowto.com/how-to/every-mac-is-vulnerable-shellshock-bash-exploit-heres-patch-os-x-0157606/
9) https://access.redhat.com/articles/1200223

[결과] - 취약한 경우
bash: x: line 1: syntax error near unexpected token '='
bash: x: line 1: ''
bash: error importing function definition for 'x'
Fri Sep 26 11:49:58 GMT 2014



<Mac OS X 취약점 확인사례[10]>

[결과] - 패치된 경우
date
cat: /tmp/echo: No such file or directory

o CVE-2014-7186, 7187 취약점 점검방법

(조사중)

□ (운영체제별) 상세 패치정보

o AIX : http://www.perzl.org/aix/index.php?n=Main.Bash

※ CVE-2014-6271, CVE-2014-7169 패치 : bash-4.3-8, 4.2-16
CVE-2014-6271 만 패치 : bash-4.3-7, 4.2-15, 4.1-9

o Solaris : http://www.oracle.com/technetwork/topics/security/alert-cve-2014-7169-2303276.html (상세정보는 로그인 계정 필요)

o HP-UX : http://hpux.connect.org.uk/hppd/hpux/Shells/bash-4.3.026/ , HPSBNS03114 rev.1 - HP NonStop CLIM running Bash Shell, Remote Code Execution (9.29 발표) [11]

※ CVE-2014-6271, CVE-2014-7169 패치

o FreeBSD : http://serverfault.com/questions/631410/shellshock-pkg-upgrade-bash-doesnt-install-bash-4-3-25 (공식 홈페이지 아님)

o CentOS : http://lists.centos.org/pipermail/centos/2014-September/146154.html

10) http://mac-how-to.wonderhowto.com/how-to/every-mac-is-vulnerable-shellshock-bash-exploit-heres-patch-os-x-0157606/
11) https://h20565.www2.hp.com/portal/site/hpsc/template.PAGE/public/kb/docDisplay/?spf_p.tpst=kbDocDisplay&spf_p.prp_kbDocDisplay=wsrp-navigationalState%3DdocId%253Demr_na-c04466552-1%257CdocLocale%253D%257CcalledBy%253D&javax.portlet.begCacheTok=com.vignette.cachetoken&javax.portlet.endCacheTok=com.vignette.cachetoken

- o Debian : https://www.debian.org/security/2014/dsa-3035
- o Redhat : https://rhn.redhat.com/errata/RHSA-2014-1306.html
- o Ubuntu : http://www.ubuntu.com/usn/usn-2363-2/
- o Novell/SUSE : http://support.novell.com/security/cve/CVE-2014-6271.html
- o Mac OS X : http://support.apple.com/kb/DL1769 (OS X bash Update 1.0, 현지시각 9.29 발표, OS X Mavericks v10.9.5 or later)

□ 취약점 업데이트 방법(리눅스 OS)

o 리눅스 종류별 업데이트 방법(다른 OS는 위의 링크 참조)

OS 종류	내용
FreeBSD	pkg info bash pkg upgrade bash
CentOS	yum clean al && yum update bash
Redhat	yum clean al && yum update bash
Ubuntu	sudo apt-get update sudo apt-get instal ?only-upgrade bash
Fedora	(1) 페도라 21 알파 su -c "yum -y instal koji" koji download-build -arch=$(uname -m) bash-4.3.25-2.fc21 su -c "yum localinstal bash-4.3.25-2.fc21.$(uname ?m).rpm" (2) 페도라 20 su -c "yum -y instal koji" koji download-build -arch=$(uname -m) bash-4.2.48-2.fc20 su -c "yum localinstal bash-4.2.48-2.fc20.$(uname -m).rpm" (3) 페도라 19 su -c "yum -y instal koji" koji download-build -arch=$(uname -m) bash-4.2.48-2.fc19 su -c "yum localinstal bash-4.2.48-2.fc19.$(uname -m).rpm"
Oracle Linux	yum list-security ¦ grep bash

※ 현재 Bash 버전에 따라 취약점 2가지 중 1가지만 패치된 경우가 있음을 주의

o 네트워크 탐지룰 설정 방법(CVE-2014-6271)[12)]

[Suricata Format]

alert http $EXTERNAL_NET any -> $HOME_NET any (msg:"Volex ? Possible CVE-2014-6271 bash Vulnerability Requested (header)"; flow:established,to_server; content:"() { "; http_header; threshold:type limit, track by_src, count 1, seconds 120; sid:2014092401;)

12) 출처 : http://www.volexity.com/blog/?p=19

[Snort Format]

alert tcp $EXTERNAL_NET any -> $HOME_NET $HTP_PORTS (msg:" Volex ? Posible CVE-2014-6271 bash Vulnerabilty Requested (header) ";
flow:established,to_server; content:" () { "; htp_header; threshold:type limit, track by_src, count 1, seconds 120; sid:2014092401;)

※ Suricata, Snort는 오픈소스 IDS/IPS/NMS임[13)]

host=127.0.0.1 program=bro_http class=BRO_HTTP srcip=10.246.50.2 srcport=43616 dstip=10.246.50.6
uri=/exploitable.cgi referer=- user_agent=() { ::}; /bin/ping -c1 10.246.50.2 mime_type=text/html

<내부 Ping 스캔 명령 예시[14)]>

13) Suricata is a high performance Network IDS, IPS and Network Security Monitoring engine, Snort is a free and open source network intrusion prevention system (NIPS) and network intrusion detection system (NIDS) created by Martin Roesch in 1998

14) http://blog.securityonion.net/2014/09/bash-vulnerability-part-3.html?m=1

[붙임2] 해당 취약점 관련 참고정보 정리

□ 보안취약점 상세정보

o CVE-2014-6271 취약점 정보

bash 쉘을 통한 원격코드(정확히는 명령) 실행 취약점

GNU Bash through 4.3 processes trailing strings after function definitions in the values of environment variables, which allows remote attackers to execute arbitrary code via a crafted environment, as demonstrated by vectors involving the ForceCommand feature in OpenSSH sshd, the mod_cgi and mod_cgid modules in the Apache HTTP Server, scripts executed by unspecified DHCP clients, and other situations in which setting the environment occurs across a privilege boundary from Bash execution, aka "ShellShock." NOTE: the original fix for this issue was incorrect;

http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2014-6271

- [CVE-2014-6271] GNU Bash 원격코드 인젝션 취약점 - (Apache 서버 취약점 관련)
  http://hacksum.net/vuln/cve-2014-6271-gnu-bash-gnu-bash-원격코드-인젝션-취약점/
- [CVE-2014-6271] ShellShock Remote Code Execution Vulnerability - (SSH 관련)
  http://forensic.n0fate.com/?p=1256
- [CVE-2014-6271] Shellshock DHCP RCE Proof of Concept - (DHCP 관련)
  https://www.trustedsec.com/september-2014/shellshock-dhcp-rce-proof-concept/

o CVE-2014-7169 취약점 정보

bash 쉘을 통한 원격코드(정확히는 명령) 실행 취약점

GNU Bash through 4.3 bash43-025 processes trailing strings after certain malformed function definitions in the values of environment variables, which allows remote attackers to write to files or possibly have unknown other impact via a crafted environment, as demonstrated by vectors involving the ForceCommand feature in OpenSSH sshd, the mod_cgi and mod_cgid modules in the Apache HTTP Server, scripts executed by unspecified DHCP clients, and other situations in which setting the environment occurs across a privilege boundary from Bash execution. NOTE: this vulnerability exists because of an incomplete fix for CVE-2014-6271.

http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2014-7169

o CVE-2014-7186 취약점 정보

원격지에서 DOS 공격 등이 가능

The redirection implementation in parse.y in GNU Bash through 4.3 bash43-026 allows remote attackers to cause a denial of service (out-of-bounds array access and application crash) or possibly have unspecified other impact via crafted use of here documents, aka the "redir_stack" issue.

http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2014-7186

o CVE-2014-7187 취약점 정보

원격지에서 DOS 공격 등이 가능

Off-by-one error in the read_token_word function in parse.y in GNU Bash through 4.3 bash43-026 allows remote attackers to cause a denial of service (out-of-bounds array access and application crash) or possibly have unspecified other impact via deeply nested for loops, aka the "word_lineno" issue.

http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2014-7187

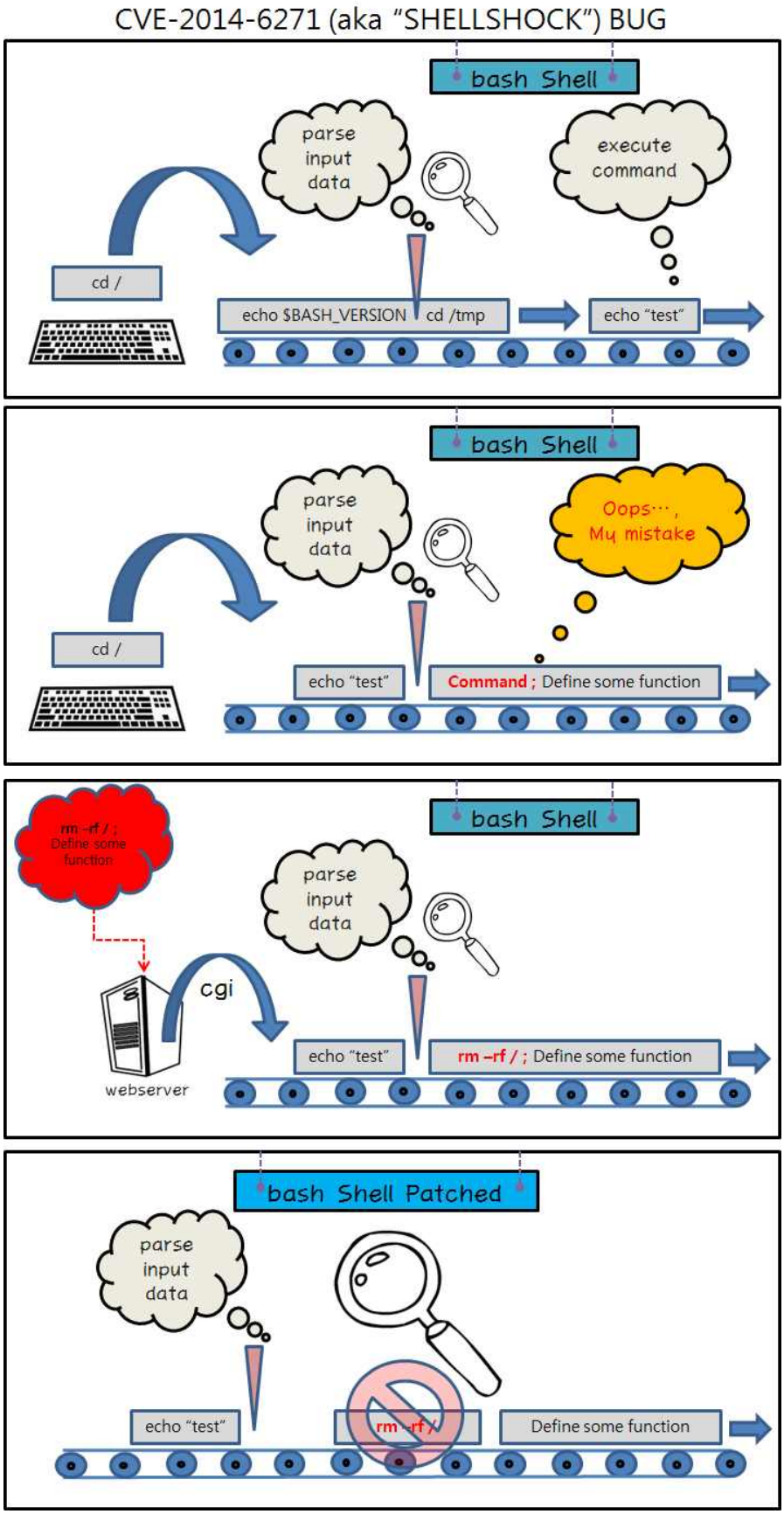
□ 보안경고 및 관련 기사

o [KISA] Bourne Again Shell (Bash) 임의코드 실행 취약점 보안 업데이트 권고 (2차) 2014.09.26

http://krcert.or.kr/kor/data/secNoticeView.jsp?p_bulletin_writing_sequence=21984

http://boho.or.kr/upload/file/EpF854.pdf

[붙임3] CVE-2014-6271 설명(Easy Version)



SHELLSHOCK shortcut (CVE-2014-6271)