Bug in bash leaves millions of web servers vulnerable

September 29 2014, by Andrew Smith

Credit: AI-generated image (disclaimer)

A first and quite reasonable thought readers may have will be to wonder: what is bash?

When you use a computer you probably interact with it through a point-and-click, visual interface such as Windows or Mac OS. More advanced

users or specific tasks might require a text-only interface, using typed commands. This command line program is known as a shell, and bash is the acronym for Bourne Again SHell (a successor to the Bourne shell, written by Stephen Bourne – that's geek humour right there), known to everyone as bash.

So what you need to know is that a shell is essential, and that bash as the most common shell in use is installed on pretty much every machine that runs a flavour of Linux or Unix. That includes Mac OS X – which behind its shiny desktop is a Unix-based operating system too.

What has systems administrators hot under the collar right now is the discovery by Red Hat, a firm that produces one of the long-established distributions of Linux favoured by enterprise, of a vulnerability in bash. This bug, which is being called "shellshock", allows under specific conditions a hacker to remotely access and take control of a system running a vulnerable version of bash.

Potentially vulnerable computers running Linux/Unix account for around two-thirds of web servers on the internet. That will include a huge number of online services you use – shops, banks, social networking sites, government services. The police and military, too.

Huge scope online

Now you can see why everyone is panicking and claiming that this is bigger than the Heartbleed bug, a problem that only affected one specific technology (secure socket layers) which is not near-universal like bash. It has been classed as a maximum risk factor 10 of 10.

Red Hat has released a patch to close the loophole and solve the problem, but it's not perfect and still allows an attacker other vectors to exploit. Other Linux and Unix vendors will be on the case as a matter of

urgency and no doubt there will be an update from Apple for its Mac OS systems very soon. It isn't the fault of one organisation – while tempting, there is no cause to bash Apple this time.

This vulnerability, dating back to version 1.13 of the program, has existed for 22 years and it has taken detailed analysis by security experts to find it. Now it has been made public, vendors and system administrators are scrabbling to close the hole while hackers and cybercriminals are trying to exploit it.

In fact within 24 hours of being announced, exploits are already being reported in the wild. The issue is exacerbated by the problem that shell programs such as bash are designed to be connected to remotely, through programs such as SSH or telnet. It isn't too difficult to send commands to a remote device or to encourage users to download an application that uses the same commands.

But that assumes the attacker is able to bypass your perimeter protection such as a firewall and other network security policies. As a network engineer, I know that while there is a weakness on my system that must be resolved, there are other defence mechanisms already surrounding that weakness that still provide protection.

However, those running a web server – whose entire function is to respond to those remote calls (in this case, your web browser's requests for pages on the site you're browsing) – have much more of a problem. This provides a route into the system that can't be blocked with a firewall as it would also block legitimate requests for the web server. Systems administrators are probably very busy at the moment trying to ensure that their bash environments cannot be exploited.

Also of concern are the tens of millions of pieces of networking hardware such as router and switches that connect the internet's

computers together. Almost all run stripped-down versions of Linux-like operating systems optimised for networking, but they also include bash for network engineers to connect and control them. These will need to be patched too.

Desktop users are safe(r)

The rest of us can probably breathe easier. Attackers are more interested in compromising systems that may return financial advantage, which is unlikely to be our desktop computers.

My advice to Apple Mac users is to check firewall settings and take care when downloading any third-party application not available via the App Store. For Linux users the same applies – Ubuntu has a software centre, for example, where the community have checked all available applications to date. In any case, a patch will be available soon. Windows users are unaffected (and it's not often you can say that).

Some are suggesting this bug is a larger problem for Apple desktop devices than it really is. Unless your machine has been set up to allow others remote access to it (it wouldn't do so by default), has also switched off the firewall and is not using a protected network (home broadband routers provide their own protection, for example), then I wouldn't worry – but install whatever recommended updates appear in the days to come.

Source: The Conversation