GLOBAL INFORMATION SECURITY INCIDENCE REPORT

SEPTEMBER 2014

1. The Bash Bug: What you need to know about the latest security flaw.

Description:

The Shellshock bug was discovered in a tool known as Bash that is widely used by the UNIX operating system and many of its variants, including Linux open source software and Apple's OSX

Bash stands for Bourne-Again Shell. It's a computer program that allows users to type commands and executes them.

It is a computer program that is installed on millions of computers around the world. There has been a lot of confusion in mainstream media accounts about how the bug works, who's vulnerable, and what users can do about it.

Who is vulnerable?

Bash is installed on many computers running operating systems derived from an ancient operating system called UNIX. That includes Macs, as well as a lot of web servers running operating systems such as Linux.

Whether these computers are actually vulnerable depends on whether they invoke Bash in an unsafe way. We know that this is true of many web servers, and it's believed that other types of network services could also be vulnerable. But it'll take a while for security experts to audit various pieces of software to check for vulnerabilities.

Apple PCs such as MacBook’s don't seem to be running services that use Bash in an unsafe way. That means they are probably not vulnerable to hacks from across the internet. But we won't know that for sure until security experts have had time for a careful audit.

Most Microsoft software doesn't use Bash, so users running Windows PCs, people with Windows phones, as well as websites built using Microsoft software, are probably safe from these attacks. Also, it looks like most Android phones are not vulnerable because they use a Bash alternative.

Mode and basis of attack:

The bug is used to hack into vulnerable servers. Once inside, attackers could deface websites, steal user data, and engage in other forms of mischief.

There's a good chance that hackers will use the vulnerability to create a worm that automatically spreads from vulnerable machine to vulnerable machine. The result would be a botnet, a network of thousands of compromised machines that operate under the control of a single hacker. These botnets, which are often created in the wake of major vulnerabilities can be used to send spam, participate in denial-of-service attacks on websites or to steal confidential data.

How to protect yourself from such an attack:

Apple has just released the OS X Bash Update 1.0 for OS X Mavericks, Mountain Lion, and Lion, a patch that fixes the "Shellshock" bug in the Bash shell. When installed on an OS X Mavericks system, the patch upgraded the Bash shell from version 3.2.51 to version 3.2.53, something that users could already do manually if they were so inclined. The update requires the OS X 10.9.5, 10.8.5, or 10.7.5 updates to be installed on your system first.

The OS X update wasn't yet available from Software Update on Mavericks systems when checked, but in the meantime you can grab the Mavericks, Mountain Lion, and Lion versions of the patch manually from Apple's software downloads site.

http://www.vox.com/2014/9/25/6843949/the-bash-bug-explained

2. Phishing Scam Ensnares eBay Shoppers

Description:

Attackers for months have been using eBay listings to redirect visitors to password-harvesting scam sites, the BBC reported. They use cross-site scripting to hijack eBay shoppers and trick them into handing over personal data.

Smartphones, televisions, hot tubs and clothing are among the items supposedly for sale in listings infected with malicious JavaScript code. When users click on the listings, the code redirects them through a series of other websites to a page requesting their eBay log-in and password.

Basis and mode of attack:

The problem is made possible by the fact that eBay allows sellers to use active content like JavaScript and flash to make their listings on the site more attractive, eBay spokesman Ryan Moore said. However, they are aware that active content may also be used in abusive ways.

Even though cross-scripting is not allowed on eBay, the criminals behind cross-site scripting and phishing activity intentionally adapt their code and tactics to try to stay ahead of the most sophisticated security systems.

EBay is apparently suffering from the losing end of a common 'risk versus convenience' scenario," Mark Stanislav, a security project manager with Duo Security, told the E-Commerce Times.

"By providing the ability for users to add JavaScript and Flash content to improve buyer experiences, they've also allowed attackers to craft code which can manipulate consumer browsers to benefit criminals," he said.

These attacks are similar to recent attacks against ad networks that have allowed JavaScript to be embedded, noted Ken Westin, a security analyst with Tripwire.

Other very similar exploits can do even more damage, Westin told the E-Commerce Times.

"If the attackers target vulnerable browsers and systems with this kind of exploit, it can lead to instant compromise of the system," he explained.

"Since online buyers have become accustomed to interactive content, we'll probably continue to see more of these kinds of attacks; they are lucrative and relatively easy for attackers to implement," Westin observed.

How to handle such incidents:

In the meantime, users should be cautious, warned Duo Security's Stanislav.

"It's very hard for users to know they are being duped into doing something wrong online," he explained. "

1. Paying attention to what your browser address bar says is a very low-tech, high-value means to ensure that if you think you're using eBay.com that you're actually on that website when logging in."
2. On SSL-enabled sites, "pay attention that you're on a site with a valid certificate through the coloring/icons browsers provide to denote that fact," he suggested.
3. "Users can help mitigate the effectiveness of these criminal ploys by utilizing the two-factor authentication provided by the service, which is a security authentication process in which the user provides two means of identification, one of which is typically a physical token, such as a card, and the other of which is typically something memorized, such as a security code." Stanislav recommended, "And it is also applicable for PayPal."

http://www.ecommercetimes.com/story/81082.html

3. **Malvertising Campaign Hits PCs and Macs:**

Description:

A malicious advertising (Malvertising) network is distributing spyware, adware, and browser hijackers to both Macs and PCs, crafting a unique malware bundle for each machine it infects. The network, dubbed "Kyle and Stan" by Cisco's TALOS Security Research, is 700 domains strong, including the likes of amazon.com and youtube.com. "This by all means is most likely just the tip of the iceberg," researchers said in a blog last week.

A malware campaign that began in May 2014 is delivering customized concoctions of spyware, adware, and browser hijacking malware to PCs and Mac users.

Basis and mode of attack:

The website automatically starts the download of a unique piece of malware for every user. The file is a bundle of legitimate software, like a media-player, and compiles malware and a unique-to-every-user configuration into the downloaded file. The attackers are purely relying on social engineering techniques, in order to get the user to install the software package. No drive-by exploits are being used thus far. This technique not only works for Windows, but for Mac operating systems alike.

Getting a malicious ad into an advertising network distribution, even for a short time, can infect many computers, especially if it is on a popular site like Amazon or YouTube. The combination of malware downloaded to each machine is different, which means the checksum varies, thwarting detection.

Malvertising attacks are not new, and have been around for a few years. Generally, criminals use ads on popular sites or networks, such as Spotify or Facebook to spread malware. They place an ad with the network, then change the code in the ad to exploit flaws in the browser which allows them to inject malware on the user’s computer.

How to protect yourself from such attack:

1. To protect yourself against these attacks, it is recommended to run malware detection software (Sophos is distributed for free for MIT users) and to make sure your browser is up to date with the latest security patches.
2. Another option is to filter sites based on their potential threat level. Browser plug-ins such as AdBlock, and Webutation can block ads and warn users if they have accessed a site

that is known to host malware. These plug-ins are free and can be run on different types of browsers.

http://securityfyi.wordpress.com/2014/09/17/malvertising-campaign-hits-pcs-and-macs/

4. Multiple Android applications fail to properly validate SSL certificates.

Description:

Multiple Android applications fail to properly validate SSL certificates provided by HTTPS connections, which may allow an attacker to perform a man-in-the-middle (MITM) attack. When communicating via HTTPS, an application should validate the SSL chain to be sure that the certificate produced by the site was provided by a trusted root certificate authority (CA). Multiple Android applications fail to properly validate SSL certificates. Additional information can be found in the CERT Oracle Secure Coding Standard for Java: DRD19-J. Properly verify server certificate on SSL/TLS

Details of the methodology used to test applications with CERT Tapioca are described in the CERT/CC blog.

Impact, basis and mode of attack:

An attacker on the same network as the Android device may be able to view or modify network traffic that should have been protected by HTTPS. The impact varies based on what the application is doing. Possible outcomes include credential stealing or arbitrary code execution.

Affected applications:

Multiple applications have accessed the domains associated with the applications listed below, indicating the potential use of a library**,** the main ones include: Flurry, Chartboost, Adcolony, MoMinis, Inmobi, Tapjoy, Appsflyer, Gameloft, Zopim, Fiksu and Batch.

Solution:

Do not use affected applications.

Many Android applications are unnecessary in that the content they provide access to is available via other means. For example, while a bank may provide an Android application for accessing its resources, those same resources are usually available by

Apply an update: Please refer to the above mentioned affected applications and the availability of fixes. Links below will help in updating and verification

1. https://batch.com
1. http://www.flurry.com/
2. https://www.chartboost.com/
3. http://www.adcolony.com/
4. http://www.playscape.com/
5. http://www.inmobi.com/
6. http://home.tapjoy.com/
7. http://www.appsflyer.com/
8. http://www.gameloft.com/
9. https://www.zopim.com/
10. http://www.fiksu.com/
11. https://batch.com

If fixes are not available for your application, please consider the following workarounds:

Using a web browser: By using a web browser to access those resources, you can help avoid situations where SSL may not be validated.

Avoid untrusted networks.

Avoid using untrusted networks, including public Wi-Fi. Using your device on an untrusted network increases the chance of falling victim to a Man In The Middle attack.

http://www.kb.cert.org/vuls/id/582497

https://docs.google.com/spreadsheets/d/1t5GXwjw82SyunALVJb2w0zi3FoLRIkfGPc7AMjRF0r4/edit#gid=1053404143)

5. Comcast's open Wi-Fi hotspots inject ads into your browser.

Description:

Comcast Corporation, formerly registered as Comcast Holdings, is the largest broadcasting and cable company in the world by revenue based in the US.

Comcast is giving users a very good reason to demand an HTTPS connection on every site they visit. The Internet service provider has started injecting ads for its services on websites where you wouldn't normally see them when you're using an Xfinity public Wi-Fi hotspot, which is a network of hotspots that allows you to connect at the fastest Wi-Fi speeds around town while conserving usage on your cellular data plan according to their website.

A former Wired editor Ryan Singel reported that while browsing on of his favorite news site suddenly got a pop-up from Comcast at the bottom of his display, a behavior he had never experienced on that site before.

It appears Comcast has actually been doing this for months, but the program only recently came to light after a report by Ars Technica, a publication website devoted to technology that would cater technologists and IT professionals.

Basis and mode of attack:

The injections can either be an alert to let users know they are connected to a Comcast hotspot, or inserted ads to promote Comcast's Xfinity mobile apps, a Comcast spokesperson told Ars. Comcast says it is doing this in part as a way to reassure users that they are connecting to an authentic Comcast hotspot. Security at public Wi-Fi hotspots is certainly an issue as hackers could make a hostile Wi-Fi router look like an authentic Xfinity hotspot.

Unfortunately, injecting JavaScript into a website where the code doesn't normally show up isn't the way to do it. Comcast's intentions may be sincere, but injecting JavaScript into a browser could create unintended security vulnerabilities for a malicious actor to exploit.

JavaScript is one of the building blocks of the modern web and you really can't experience numerous websites without it. But it can also be designed to behave maliciously and your browser can often have a hard time distinguishing between good and bad code.

How to handle such attack:

So what's a user to do when even ISPs are trying to mess with your browser?

Try forcing your browser to connect to websites using HTTPS via a browser extension such as “The Electronic Frontier Foundation's HTTPS Everywhere” for Chrome and Firefox. This removes the opportunity for Comcast to slip its ads into the web content you're viewing midstream, though not all websites support encrypted connections.

And, as always, you should use a virtual private network (VPN) when connecting over public Wi-Fi.

http://www.pcworld.com/article/2604422/comcasts-open-wi-fi-hotspots-inject-ads-into-your-browser.html

http://wifi.comcast.com/faqs.html

http://arstechnica.com/about-us/