By Adriana Escobar de la Torre

ShellShock
{bashbug}
What is bash?

- Bash is a Unix/Linux shell.
- It is an interpreter that allows a user to orchestrate commands on Unix and Linux systems.
- It can also operate as a parser for CGI scripts on a web server such as we’d typically see running on Apache server.
What is the Bash Bug vulnerability?

- The Bash Bug vulnerability also dubbed as “Shellshock” ([CVE-2014-6271](https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-6271)) was discovered on September 2014.
- Targets include websites, servers, home routers and any other devices that execute or allows bash scripts.
- Stephane Chazelas, the security researcher that discovered the vulnerability, states that it has existed for several decades, stating that it is related to the way Bash handles specially-formatted environment variables, named shell functions.
- It allows the user to type commands into a simple text-based window, which the operating system will then run. Bash can run commands that are passed to it and that is what the vulnerability exploits.
The National Institute of Standards and Technology assigned the severity of the vulnerability as a “10” in a 10-point scale.

It affects GNU Bash versions 1.14 through 4.3 on environments such as OpenSSH, Common-Gateway Interface (CGI) and Apache HTTP Server.

In other words, a system is vulnerable if it uses a Bash shell command in an HTTP server or a CGI. The severity of this vulnerability is very high because it is commonly used on servers and the level of complexity to run an attack is very low.
What can attackers do?

- Deface websites.
- Steal user data.
- Load a virus in a web server that spreads to vulnerable machines that access the server (create a botnet to spread from machine to machine).
- Use botnets to send spam, steal data, or perform denial-of-service attacks.
- Delete files, activate your camera, open a lock, or pretty much anything.
BASH COMMAND → NIX → INTERNET (Download Malware) → ELF_BASHLITE.A (malware executed in affected system) → Backdoor Capabilities (IP Scanner, UDP/TCP Flood, etc.)
Billions of servers affected by the Bash Bug flaw

A day after the vulnerability was discovered. Attackers were already targeting millions of web servers and systems. Also, the vulnerability was exploited through botnets to exploit more machines on the internet.

“The number of vulnerable machines is greater than 3000, as revealed by Graham, who searched for affected servers only querying the port 80 used for normal Web Hypertext Transfer Protocol (HTTP) requests.”[1]
Famous botnet attacks

◊ Botnet attacks networking company Akamai, United States (US) Department of Defense (DoD) networks
◊ “Wopbot” is a botnet that tried to scan vulnerable systems (which included the US DoD) and infect other servers. It launched a denial service attack against the delivery network Akamai. “Analyzing the malware sample in a sandbox, ... the malware had conducted a massive scan on the United States Department of Defense Internet Protocol address range on port 23 TCP or Telnet for brute force attack purpose ... The US DoD network in question is the 215.0.0.0/8 range, with approximately 16.7 million addresses.” [2].
“Thanks-Rob” attack

Hackers “rewrote a proof-of-concept script created by security researcher Robert David Graham” [3]. The script that Graham wrote was designed to measure the problem in a way to send back a “ping”, however attackers rewrote the script in order to send and install malwares on victim machines and even create backdoors.

Yahoo servers infiltrated by Romanian hackers

A security expert Jonathan Hall “had Google-searched a range of codes designed to identify which servers were vulnerable to Shellshock” [4]. He found that two Yahoo servers had been breached by Romanian hackers looking for access points in Yahoo!Games. Also, Hall found that the hackers were using WinZip domain to locate accessible servers.
How to be protected against shellshock attacks?

- Install latest patches to operating systems.
- Monitor system logs.
- Check Internet of Things (IoT) devices.
- Test using dynamic host configuration protocol (DHCP).
- Use Network Intrusion Prevention products.
Resources


