Bourne Again Shell (Bash) Remote Code Execution Vulnerability

MSS-VE

Prepared By: Managed Services / Revision Number: 1.0

Date: 09/25/2014

Table of Contents

Technical Summary

Multiple advisories have been released by an array of vendors alerting of a vulnerability within Bash, the shell environment used on most Unix-based operating systems. The vulnerability can allow remote code execution to occur on vulnerable hosts using both local execution and attacking applications that could allow for the manipulation of environment variables. The vulnerability is also being coined by the name, "Shell Shock".

Mitre.org has assigned the following CVE numbers:

- GNU Bash versions through 4.3 original vulnerability (CVE-2014-6271)
- GNU Bash secondary vulnerability indicating potential problems with original vulnerability patch (CVE-2014-7169)

Impact

The vulnerability itself is not an application within the operating system but rather the shell execution system. The shell system bash is used widely but in order to execute a successful vulnerability an attacker must first set a variable and further use that variable when executing the program. To remotely exploit this vulnerability, the attacker must find a method of setting a variable before execution. Exploitation will likely occur in older web applications that utilize CGI scripting or other server side processes which retain commands in memory before executing them.

NIST indicates, "GNU Bash through 4.3 bash43-025 processes trailing strings after certain malformed function definitions in the values of environment variables, which allows remote attackers to write to files or possibly have unknown other impact via a crafted environment, as demonstrated by vectors involving the ForceCommand feature in OpenSSH sshd, the mod_cgi and mod_cgid modules in the Apache HTTP Server, scripts executed by unspecified DHCP clients, and other situations in which setting the environment occurs across a privilege boundary from Bash execution."

Affected Versions

GNU Bash through 4.3

1.14.0	1.14.1	1.14.2	1.14.3	1.14.4	1.14.5	1.14.6
1.14.7	2.0	2.01	2.01.1	2.02	2.02.1	2.03
2.04	2.05	2.05:a	2.05:b	3.0	3.0.16	3.1
3.2	3.2.48	4.0	4.0:rc1	4.1	4.2	4.3

Additional vulnerable products are listed below.

The vulnerability **DOES NOT** affect the following major platforms:

- Microsoft Windows

Determining Vulnerability

A number of tools and signatures have been developed to address this vulnerability.

Commercial Vulnerability Scanning Tools

The following scanning vendors have released checks for this vulnerability:

Rapid7 (Nexpose)

Rapid7 has released an additional check within the Nexpose to identify these vulnerabilities. A specific policy can be created to scan specifically for this vulnerability.

Tenable (Nessus)

Tenable has released a check for the Nessus product line. Creating the check is outlined in the included link.

Qualys

Qualys has released a check for their scanner.

Other Methods

Below is a set of steps for the Linux command line to assist in assessing if hosts are vulnerable. These steps apply to most Linux and Apple operating systems.

Linux Command Line

These steps were created by Red Hat and are available in full detail here.

```
To test if your version of Bash is vulnerable to this issue, run the following command:

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

If the output of the above command looks as follows:

vulnerable
this is a test

you are using a vulnerable version of Bash. The patch used to fix this issue ensures that no
code is allowed after the end of a Bash function. Thus, if you run the above example with
the patched version of Bash, you should get an output similar to:

$ env x='() { :;}; echo vulnerable'  bash -c "echo this is a test"
bash: warning: x: ignoring function definition attempt
bash: error importing function definition for `x'
this is a test
```

Appliances/Embedded Devices

Many Linux-based embedded devices and appliances are vulnerable to this attack. It is safe to assume the system is vulnerable based on the massive number of affected bash versions. Refer to the vendor for individual steps to determine vulnerability and steps to address the vulnerability. If the system does not have an interactive console or network facing service the priority to address the issue may be lower than other network facing devices due to reduced attack surface.

Exploitation in the Wild

Scripts are already being developed and posted to readily available websites in attempts to identify and exploit servers susceptible to the vulnerability.

- Rapid 7 Metasploit Exploit Module
- CGI Python Script
- GitHub VT Example

Recommendations

Overview

Accuvant recommends immediately patching any Internet facing Unix based servers with patches identified from the vendor. IDS and IPS systems should be updated with the latest signatures to identify and block any suspicious connections that may be attempting to scan for connections intend to exploit machines that are vulnerable.

Patching

Amazon Linux - https://alas.aws.amazon.com/ALAS-2014-418.html
Apple (Unofficial) - http://nkush.blogspot.com/2014/09/patching-bash-shellshock-on-apple-max.html
CentOS - http://lists.centos.org/pipermail/centos/2014-September/146099.html
Debian - https://www.debian.org/security/2014/dsa-3032
Oracle - http://linux.oracle.com/errata/ELSA-2014-1293.html
RedHat - https://access.redhat.com/solutions/1207723 & https://access.redhat.com/articles/1200223
Ubuntu - http://www.ubuntu.com/usn/usn-2362-1/

Workaround

No known workarounds at this time.

Monitoring/Detection

The following vendors have released signatures for detecting the attack at the time of writing:

Palo Alto Networks

Signature ID – 36729 – Bash Remote Code Execution Vulnerability

Sourcefire

Signature ID – 1:31978 – OS-OTHER Bash CGI environment variable injection attempt.

Accuvant MSS Recommendations

Accuvant Managed Security Solutions is currently developing custom alerting and monitoring to identify any related activity across all of the managed platforms and service lines. Accuvant clients with any of the devices listed in the Monitoring/Detection section of this document with updated signatures will have coverage for this issue.

Strategic Recommendations

To ensure thorough mitigation Accuvant strongly recommends the following additional steps:

- Monitor and Protect Legacy Applications/Systems
  - Monitor HTTP logs and application traffic for references to Bash and other attack strings
  - Monitor network traffic to identify references to bash
  - Limit access to legacy applications that may integrate with shells
  - Review applications that use mod_cgi and php_cgi for potential interaction points with bash.
  - Implement web application firewalls to protect potentially vulnerable applications.
- Limit and Monitor Shell Access to Trusted users
  - Limit access to users with SSH
    - Limit to only SCP/SFTP where possible
    - Use tools such as SE Linux or PMRUN to limit access to specific command line parameters and environment variables.

    - Monitor User Access
        - Monitor user access logs and history files for suspicious access attempts
- Remove Bash on unsupported systems
    - Although undesirable it is possible to remove Bash on systems that are no longer supported. This can be achieved by removing bash from the shells file on Linux systems and modify the user shells to an alternative shell.
    - Ensure that “sh” and other shells on the system are not renamed versions of bash.

References

1. https://access.redhat.com/solutions/1207723
2. https://bugzilla.redhat.com/show_bug.cgi?id=1141597
3. https://community.qualys.com/blogs/laws-of-vulnerabilities/2014/09/24/bash-shellshock-vulnerability
4. https://community.qualys.com/blogs/securitylabs/2014/09/24/bash-remote-code-execution-vulnerability-cve-2014-6271
5. https://community.rapid7.com/community/infosec/blog/2014/09/25/bash-ing-into-your-network-investigating-cve-2014-6271
6. http://lists.centos.org/pipermail/centos/2014-September/146099.html
7. http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2014-6271
8. http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2014-7169
9. https://www.debian.org/security/2014/dsa-3032
10. http://www.ubuntu.com/usn/usn-2362-1/
11. https://www.us-cert.gov/ncas/current-activity/2014/09/24/Bourne-Again-Shell-Bash-Remote-Code-Execution-Vulnerability

Revisions

Release Version:	1.0 – Initial Release
Date:	9/25/2014
Summary of Changes:	Initial release