National Computer Board
Computer Emergency Response Team of Mauritius
(CERT-MU)

Advisory

The Shellshock or Bash Bug

Issued on: September 30, 2014

Severity Rating: High

Software Affected:

- GNU Bash versions between 1.14 through 4.3

Systems Affected:

- Apple OS X Lion v10.7.5
- Apple OS X Lion Server v10.7.5
- Apple OS X Mountain Lion v10.8.5
- Apple OS X Mavericks v10.9.5
- Red Hat Enterprise Linux 7
- Red Hat Enterprise Linux 6
- Red Hat Enterprise Linux 5
- Red Hat Enterprise Linux 4
- CentOS-5
- CentOS-6
- CentOS-7
- Ubuntu 14.04 LTS
- Ubuntu 12.04 LTS
- Ubuntu 10.04 LTS
- Debian

- Novell/SUSE

Description:

A critical vulnerability known as the "Shellshock bug" has been identified in GNU's bash shell, which can allow remote attackers to run remote commands on vulnerable systems. The Shellshock flaw affects the Bash shell used across many UNIX-based systems including Mac OS X and variants of Linux.

Successful exploitation of the Shellshock vulnerability can allow attackers to insert malicious pieces of code from a remote location and get full system control of the vulnerable system. Because of Bash's ubiquitous status amongst Linux, BSD, and Mac OS X distributions, many computers are vulnerable to Shellshock - all unpatched Bash versions between 1.14 through 4.3 are at risk.

This vulnerability is regarded as critical, since Bash is widely used in Linux and UNIX operating systems running on Internet-connected computers, such as Web servers. BASH is the default command-line shell processor that is often run in a text window on Linux and UNIX systems. It also allows users to type commands that cause actions and has the ability to read commands from a scripted file.

CVE Information

The CVE provides information about the vulnerability.

CVE-2014-7169

CVE-2014-6271

Check the System for Shellshock Vulnerability

On each of your systems that run Bash, you may check for Shellshock vulnerability by running the following command at the bash prompt:

```
env 'VAR=() { :;}; echo Bash is vulnerable!' 'FUNCTION()=() { :;}; echo
Bash is vulnerable!' bash -c "echo Bash Test"
```

The highlighted `echo Bash is vulnerable!` portion of the command represents where a remote attacker could inject malicious code; arbitrary code following a function definition within an environment variable assignment. Therefore, if you see the following output, your version of Bash is vulnerable and should be updated:

```
Bash is vulnerable!
Bash Test
```

If the output does not include the simulated attacker's payload, i.e. *"Bash is vulnerable"* is not printed as output, you are protected against at least the first vulnerability (CVE-2014-6271), but you may be vulnerable to the other CVEs that were discovered later. However, if there are any bash warnings or errors in the output, then the Bash should be updated to its latest version.

If the output from the test command is the following, then your system's Bash is safe from Shellshock:

```
Bash Test
```

Test the Vulnerability from Remote Sites

The Shellshock Bash Vulnerability can also be tested to check whether websites or specific CGI s scripts are vulnerable. The following tools can be used:

1. Shellshock Bash Vulnerability Test Tool - www.shellshock.brandonpotter.com
2. Shellshock BASH Vulnerability Tester – https://shellshocker.net

Workarounds

1. Users are advised to apply patches to fix the Vulnerability.

   Patches have been released to update the Bash on various Linux distributions, including Ubuntu, Debian, CentOS, Red Hat, and Fedora. Apple has also released OS X bash update 1.0 to address the Shellshock vulnerability.

   The updates are available on:

   Apple

   - http://support.apple.com/kb/DL1769?viewlocale=en_US&locale=en_US

   Centos
   - http://lists.centos.org/pipermail/centos/2014-September/146099.html

   Red Hat
   - https://access.redhat.com/site/solutions/1207723

   Debian
   - https://www.debian.org/security/2014/dsa-3032

   Ubuntu

   - http://www.ubuntu.com/usn/usn-2362-1/

Novell/SUSE

- http://support.novell.com/security/cve/CVE-2014-6271.html

2. Run all software as a non-privileged user (one without administrative privileges) to diminish the effects of a successful attack.

For more information please contact CERT-MU team on:

Hotline No: (+230) 800 2378

Fax No: (+230) 208 0119

Gen. Info. : contact@cert-mu.gov.mu

Incident: incident@cert-mu.gov.mu

Website: http://www.cert-mu.org.mu