

*The following security alert was issued by the Information Security Division of the Mississippi Department of ITS and is intended for State government entities. The information may or may not be applicable to the general public and accordingly, the State does not warrant its use for any specific purposes.*

**DATE(S) ISSUED:**

09/24/2014

**SUBJECT:**

Critical Bourne Again SHell (BASH) Vulnerability Allows for Remote Code Execution

**OVERVIEW:**

A recent vulnerability has been discovered affecting the Bourne Again SHell (BASH). BASH is the default command-line shell processor that is often run in a text window on Linux and UNIX systems. BASH allows users to type commands that cause actions. In addition, BASH has the ability to read commands from a scripted file. Based on the wide use of Linux and UNIX systems, it can be assumed that most distributions running Linux and UNIX, as well Mac OS X, are likely vulnerable.

Successful exploitation could result in an attacker gaining the same privileges as the logged on user. Depending on the privileges associated with the user, an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.

**THREAT INTELLIGENCE:**

Exploit code is currently available and the vulnerability is actively being exploited.

**SYSTEMS AFFECTED:**

Mac OS X

Linux distributions

UNIX distributions

GNU BASH versions 1.14 through 4.3

**RISK:**

**Government:**

Large and medium government entities: **High**

Small government entities: **High**

**Businesses:**

Large and medium business entities: **High**

Small business entities: **High**

**Home users: High**

**TECHNICAL SUMMARY:**

This vulnerability allows unauthorized remote parties to possibly bypass environment restrictions on a network and execute remote code through the execution of various shell commands on vulnerable systems. In order for the vulnerability to be exploited, specially crafted environment variables would need to be created prior to calling the BASH shell.

The following possible attack vectors have been identified by Redhat security:

- The ForceCommand in SSHD configurations, which provides limited command execution capabilities for remote users.

- Apache servers using mod\_cgi or mod\_cgid are affected if CGI scripts are either written in BASH, or spawn subshells. Such subshells are implicitly used by system/popen in C, by os.system/os.popen in Python, system/exec in PHP (when run in CGI mode), and open/system in Perl if a shell is used (which depends on the command string).

- DHCP clients invoke shell scripts to configure the system, with values taken from a potentially malicious server. This would allow arbitrary commands to be run, typically as root, on the DHCP client machine.

- Various daemons and SUID/privileged programs may execute shell scripts with environment variable values set / influenced by the user, which would allow for arbitrary commands to be run.

- Any other application, which is hooked onto a shell or runs a shell script as using BASH as the interpreter.

The following [article](#) contains an example of proof of concept code that can be used to check if your systems are vulnerable.

<https://securityblog.redhat.com/2014/09/24/BASH-specially-crafted-environment-variables-code-injection-attack/>

**RECOMMENDATIONS:**

The following actions should be taken:

- Update vulnerable products **immediately** after appropriate testing.

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

## **REFERENCES:**

### **Redhat:**

<https://securityblog.redhat.com/2014/09/24/BASH-specially-crafted-environment-variables-code-injection-attack/>

<https://rhn.redhat.com/errata/RHSA-2014-1293.html>

<https://rhn.redhat.com/errata/RHSA-2014-1294.html>

<https://rhn.redhat.com/errata/RHSA-2014-1295.html>

[https://bugzilla.redhat.com/show\\_bug.cgi?id=CVE-2014-6271](https://bugzilla.redhat.com/show_bug.cgi?id=CVE-2014-6271)

<https://access.redhat.com/solutions/1207723>

### **GNU Project:**

<http://ftp.gnu.org/pub/gnu/bash/bash-3.0-patches/bash30-017>

<http://ftp.gnu.org/pub/gnu/bash/bash-3.1-patches/bash31-018>

<http://ftp.gnu.org/pub/gnu/bash/bash-3.2-patches/bash32-052>

<http://ftp.gnu.org/pub/gnu/bash/bash-4.0-patches/bash40-039>

<http://ftp.gnu.org/pub/gnu/bash/bash-4.1-patches/bash41-012>

<http://ftp.gnu.org/pub/gnu/bash/bash-4.2-patches/bash42-048>

<http://ftp.gnu.org/pub/gnu/bash/bash-4.3-patches/bash43-025>

### **CentOS:**

<http://lists.centos.org/pipermail/centos-announce/2014-September/020582.html>

<http://lists.centos.org/pipermail/centos-announce/2014-September/020585.html>

<http://lists.centos.org/pipermail/centos-announce/2014-September/020583.html>

### **Debian:**

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

**FreeBSD:**

<http://portaudit.freebsd.org/71ad81da-4414-11e4-a33e-3c970e169bc2.html>

**Gentoo:**

<http://www.gentoo.org/security/en/glsa/glsa-201409-09.xml>

**Novell SUSE:**

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

**Oracle Linux:**

<http://linux.oracle.com/errata/ELSA-2014-1293.html>

<http://linux.oracle.com/errata/ELSA-2014-1294.html>

**Palo Alto:**

<https://securityadvisories.paloaltonetworks.com/Home/Detail/24>

**Ubuntu:**

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

**CVE:**

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-6271>

**SecurityFocus:**

<http://www.securityfocus.com/bid/70103>