Date: September 29th 2014

Revision	Date	Changes
1.0	September 29th 2014	Initial release
1.1	September 30th 2014	Additional details on maintenance releases
1.2	October 29th 2014	Additional details on fixed releases
1.3	November 4th 2014	Additional details on fixed releases

Shell command Bash code injection vulnerability (CVE-2014-6271, CVE-2014-6278, and CVE-2014-7169)

On September 24th, Arista became aware of a vulnerability affecting all versions of the bash package shipped with Arista EOS. The bash code injection vulnerability could allow for arbitrary code execution, allowing an attacker to gain shell access.

Arista switches are only vulnerable to administrators with current access to the switch CLI. The switch is not vulnerable to remote attack.

A software patch (RPM extension) is available for download. In addition fixes will be integrated for each currently supported version of EOS through regular maintenance releases. Currently supported versions of EOS include 4.9 through 4.14.

BugID's 99948 and 99949 address the issue.

All models of the Arista 7000 Series of fixed and modular systems are affected.

EOS Releases Affected	Fixed in	Status
4.9.0 through 4.9.11	4.9.12	Pending Release
4.10.0 through 4.10.8	4.10.9	Pending Release
4.11.0 through 4.11.10	4.11.11	Released
4.12 through 4.12.8	4.12.9	Released
4.13 through 4.13.8	4.13.9	Released
4.14.0 through 4.14.3	4.14.4F	Released

Workaround:

Available mitigations include restricting access to a set of known trusted users, restricting ssh logins to trusted source IP addresses, and temporarily removing remote access to users with non privileged access.

Customers using Arista's DHCP extensions or using dhclient in a custom setup may wish to disable the extension if it passes DHCP parameters to bash as environment variables.

Verification:
To determine if the version of EOS is vulnerable use the following command:

```
switch# bash
-bash-4.1# X='() ; echo vulnerable' bash -c "echo this is a test"
X='() ; echo vulnerable' bash -c "echo this is a test"
vulnerable
this is a test
```

If the output of the above command contains a line containing the word "vulnerable" 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.

Resolution:

The resolution to this issue is through the installation of a patch, or through upgrading to a version of EOS that contains the resolution. This section will be updated once EOS maintenance releases are available. A patch is currently available.

Download URL for patch:

Instructions to install the patch for Security Advisory 0006

The extension is applicable for all EOS versions 4.9.0 - 4.14.3 inclusive.

Step 1. Copy the file secAdvisory0006.swix to the extension partition of the Arista switch using any of the supported file transfer protocols:

```
switch#copy scp://arista@10.10.10.123/home/arista/secAdvisory0006.swix extension:
```

Step 2. Ensure that the file has been copied to the extensions partition and verify the checksum of the copied file:

```
switch#show extensions
Name          Version/Release          Status<          RPMs
```

```
--------------------------------------------------------------------------------
secAdvisory0006.swix secAdvisory0006.swix          4.1.14Ar/4.fc14          A, NI
      1

A: available | NA: not available | I: installed | NI: not installed | F:forced
```

To verify the extension, compare the following sha512 or md5 checksum with the output of the verify command:

```
sha512sum: 3cf25bb085c3b3bb84430257887e0ee75f4abe52968d093258ce65cad95450e8163b374429
da81db0cecccf344bcb469354fbfa0bc0c9651a33c7b509f89f88f
```

```
md5sum:
084606719ce59e65fb383ad99c50d186
```

verify commands:

```
switch#verify /sha512 extension:secAdvisory0006.swix
verify /sha512 (extension:secAdvisory0006.swix) = 3cf25bb085c3b3bb84430257887e0ee75f4
abe52968d093258ce65cad95450e8163b374429da81db0cecccf344bcb469354fbfa0bc0c9651a33c7b50
9f89f88f
```

```
switch#verify /md5 extension:secAdvisory0006.swix
verify /md5 (extension:secAdvisory0006.swix) =
084606719ce59e65fb383ad99c50d186
```

Step 3. The patch is installed as an extension, and upon installation into a live system will automatically install with the following behavior:

```
switch#extension secAdvisory0006.swix
```

All modular switches with dual supervisors require the extension copying and installing on both supervisors.

Verify that the extension has been installed:

```
switch#show extensions
Name          Version/Release          Status          RPMs
-------------------------------------------------------------

secAdvisory0006.swix          4.1.14Ar/4.fc14          A, I           1

A: available | NA: not available | I: installed | NI: not installed | F: forced
```

Step 4. Post installation, any newly initialized shell sessions will use the fixed version of bash.

Note: As the vulnerability exists only during the startup of a new bash instance, existing running shell instances are unlikely to be affected. Existing bash scripts running as part of a custom setup may be restarted to ensure use of the new version of bash.

Step 5. Make the extension persist across reboots:

```
switch#copy installed-extensions boot-extensions
Copy completed successfully.
switch#show boot-extensions
secAdvisory0006.swix
```

Verification of the bash version after resolution:

```
switch#show version detail  | grep -i bash
bash 4.1.14Ar 4.fc14
```

Arista Networks PSIRT team monitors industry-wide vulnerability reporting and is committed to addressing any additional potential threats.

References:
For More Information on Vulnerability please visit:
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-6271
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-7169

For More Information:
If you require further assistance, or if you have any further questions regarding this security notice, please contact the Arista Networks Technical Assistance Center (TAC) by one of the following methods:

Open a Service Request:
By email: support@arista.com
By telephone: 408-547-5502
866-476-0000