Date: August 20th 2015

Revision	Date	Changes
1.0	August 20th, 2015	Initial release
1.1	August 24th, 2015	Updated with patch details.
1.2	November 22nd, 2017	Updated with the fixed updated EOS releases

Arista 7000 Series Products and Arista EOS are vulnerable to CVE-2015-5600.

In July 2015, the OpenSSH project issued a security advisory for an authentication brute force vulnerability that bypasses the default max attempts limit. The vulnerability allows for unlimited entries within the login time limit. This permits a brute force attack on weak passwords within the login time period of two minutes.

This issue affects all current OpenSSH versions through 6.9.

All systems using OpenSSH are vulnerable and can be tested using

```
ssh -l  -oKbdInteractiveDevices=`perl -e 'print "pam," x 10000'`
```

and then entering multiple password attempts.

Mitigation

The best workaround until a fix is available is to restrict access to known sources and to ensure all passwords are long and difficult to brute force.
To determine if a system is being probed for this check the following logs "/var/log/secure" under the bash shell for log's that look like the following:

```
Aug 10 10:16:16 switch sshd[4439]: Failed keyboard-
interactive/pam for user_name from hostname port 47884 ssh2
Aug 10 10:16:16 switch sshd[4439]: error: PAM: Authentication failure for user_name f
rom hostname
```

Note that the above logs will only appear under /var/log/secure and not under the switches normal syslogging mechanism. To view this log file, use the following command from the EOS CLI:

```
bash sudo cat /var/log/secure
```

Resolution

Bug ID 129011 tracks this vulnerability. The fix will be available in EOS releases 4.12.11M, 4.13.13M, 4.14.10M and 4.15.2F and later releases. The following patch file can be installed on all affected EOS releases (4.12 through 4.15):

Patch URL: SecurityAdvisory0012.swix

sha512sum: 8586baf27c52e6ccc54d90814451cede5d23230e2a738cc2bfcd8cb182715afbe21cfd0b87660d792aba743c3339baebdb0b90a0ddefa65917ee21463e136a80

Instructions to install patch

1. Download the above patch file to the flash of the switch using any of the supported file transfer protocols:

```
switch#copy scp://arista@10.10.10.123/SecurityAdvisory0012.swix extension:
```

2. Install the patch using the extension command:

```
switch#extension SecurityAdvisory0012.swix
switch#show extensions
Name                                Version/Release           Status Extension
s
---------------------------------- ------------------------ -------- -------
-
SecurityAdvisory0012.swix          5.5p1/2592747.gaevansrele   A, I      1
A: available | NA: not available | I: installed | NI: not installed | F: force
d
```

3. Once the patch is installed, sshd will be restarted as part of the fix. Existing SSH sessions will not be disrupted.
4. To verify that the patch is installed, start an SSH session to the patched switch using the following options:

```
ssh -l  -oKbdInteractiveDevices=`perl -e 'print "pam," x 10000'`
```

   On a patched switch, the above SSH command will disconnect after three attempts.
5. Make the patch persistent across reboots:

```
switch#copy installed-extensions boot-extensions

Copy completed successfully.
```

```
switch#show boot-extensions

SecurityAdvisory0012.swix
```

References:
For additional information about the vulnerability, please visit: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-5600

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