Date: August 15th, 2016

Version: 1.0

Revision	Date	Changes
1.0	August 15th, 2016	Initial release
1.1	September 15th, 2016	Updated to include fixed software versions

Arista Products vulnerability report for security vulnerability CVE-2016-5696 that was released in August, 2016

A problem was identified with the Linux kernel implementation in which the rate of TCP challenge ACK segments were not properly determined in Linux kernel versions prior to 4.7. This allows potential attackers to RST valid connections, as well as inject data on unencrypted connections. This advisory reports the vulnerability assessment for Arista products.

CVE-2016-5696 (TCP off-path attack):

Software	• EOS and CloudVision eXchange - EOS releases starting with 4.14.0F. The list of affected releases is documented in Table-2. • CloudVision Portal - Releases 2015.1.x, 2016.1.0, 2016.1.1
Affected Platforms	All Arista platforms
Status	Vulnerable
CVSS Scores	CVSS v3 Base Score: 5.9 Medium CVSS v2 Base Score: 4.3 MEDIUM
Resolution	Bug166604 tracks this vulnerability for EOS and CloudVision eXchange. A hotfix is available to mitigate this issue but should not be considered a full fix. A software fix is available in 4.16.8M and will be available in the next releases for the 4.15 and 4.17 EOS trains. This advisory will be continue to be updated with the exact software versions once available. Bug166719 tracks this vulnerability for CloudVision Portal. The complete fix will be available in version 2016.1.2

AFFECTED EOS RELEASES:

Table-1: Affected EOS releases

4.17	4.16	4.15	4.14
4.17.0F 4.17.1F	4.16.6M • 4.16.6FX-7512R • 4.16.6FX-7500R.1 • 4.16.6FX-7500R-bgpscale • 4.16.6FX-7500R • 4.16.6FX-7060X • 4.16.6FX-7050X2 4.16.7M • 4.16.7M-L2EVPN • 4.16.7FX-MLAGISSU-TWO-STEP • 4.16.7FX-7500R • 4.16.7FX-7060X	4.15.0F • 4.15.0FX • 4.15.0FXA • 4.15.0FX1 4.15.1F • 4.15.1FXB.1 • 4.15.1FXB • 4.15.1FX-7060X • 4.15.1FX-7260QX 4.15.2F 4.15.3F • 4.15.3FX-7050X-72Q • 4.15.3FX-7060X.1 • 4.15.3FX-7500E3 • 4.15.3FX-7500E3.3 4.15.4F • 4.15.4FX-7500E3 4.15.4.1F 4.15.5M • 4.15.5FX-7500R • 4.15.5FX-7500R-bgpscale 4.15.6M	4.14.0F 4.14.1F 4.14.2F 4.14.3F 4.14.3.1F 4.14.4.F 4.14.4.1F 4.14.4.2F 4.14.5M • 4.14.5FX • 4.14.5FX.1 • 4.14.5FX.2 • 4.14.5FX.3 • 4.14.5FX.4 • 4.14.5.1F-SSU 4.14.6M 4.14.7M 4.14.7.1M 4.14.8M 4.14.8.1M 4.14.9M 4.14.9.1M 4.14.10M 4.14.10.1M 4.14.11M 4.14.12M 4.14.13M 4.14.14M 4.14.15M

		4.15.7M	

Mitigation:

This vulnerability can be exploited only if the attacker can make a legitimate TCP connection. The following recommended best practices for Arista products can help prevent this attack:

- Configuring a control plane ACL that allows only trusted TCP connections from known sources
- Encrypting control plane traffic. Services such as SSH are always encrypted, but others like eAPI should only be used in HTTPS mode.

A hotfix is available for the affected EOS versions that mitigates the issue to a certain extent but should not be considered as the full fix. The hotfix is a single file that can be a installed on any of the affected EOS releases and is non-disruptive to traffic through the switch.

File URL: security-advisory-0023-mitigation.swix

SHA512SUM: d669cd3c2c98d6b59cd9e0e0588baa14f5064eaa9dbdcdacc9b5c52210737f13fcd5d09f064db85074cfd5f15dcdd0eddce0cf9fc8be46c310ea3be7c69b3749

Steps to install the hotfix:

1. Download the patch file and copy the file to the extension partition of the switch using one of the supported file transfer protocols:

```
switch#copy scp://10.10.1.1/security-advisory-0023-mitigation.swix extension:
switch#verify /sha512 extension:security-advisory-0023-mitigation.swix
```

   Verify that the checksum value returned by the above command matches the provided SHA512 checksum for the file
   On modular systems with dual supervisors, download the file to the extension partition of the active supervisor and copy it to the standby supervisor using the following two commands:

```
switch(s1)(config)#copy extension:security-
advisory-0023-mitigation.swix supervisor-peer:/mnt/flash/
switch(s2-standby)#copy flash:security-
advisory-0023-mitigation.swix extension:
```

2. Install the patch using the extension command. The patch takes effect immediately at the time of installation:

```
switch#extension security-advisory-0023-mitigation.swix
```

On modular systems with dual supervisors, the patch has to be installed on the active and standby supervisors:

```
switch(s1)#extension security-advisory-0023-mitigation.swix
switch(s2-standby)#extension security-advisory-0023-EOS-mitigation.swix
```

3. Verify that the patch is installed using the following commands:

```
sq321-22:07:53#show extensions
Name                        Version/Release           Status extension
--------------------------- ------------------------- ------ --------
security-advisory-0023-mitigation.swix 2.7.0/3431682.erahneostru A,I 1
```

4. Make the patch persistent across reloads. This ensures that the patch is installed as part of the boot-sequence. The patch will not install on EOS versions with the security fix.

```
switch#copy installed-extensions boot-extensions
switch#show boot-extensions
security-advisory-0023-mitigation.swix
```

For dual supervisor systems run the above copy command on both active and standby supervisors:

```
switch(s1)#copy installed-extensions boot-extensions
switch(s2-standby)#copy installed-extensions to boot-extensions
```

The patch can be uninstalled using the command:

```
switch#no extension security-advisory-0023-mitigation.swix
switch#copy installed-extensions boot-extensions
```

On modular systems with dual supervisors, the above commands have to be run on the active and standby supervisor. Before upgrading to a release with the complete fix, it is recommended to uninstall the mitigation hotfix using the above commands.

Mitigation for CloudVision Porta and CloudVision Appliance:A script is available for the affected versions that mitigates the issue to a certain extent but should not be considered as the full fix. The script is applicable to CloudVision Portal VM deployments and the CloudVision Appliance and the installation of the script is non-disruptive to the server operations.

File URL: security-advisory-0023-cvp-cva-mitigation.sh

SHA512SUM: d669cd3c2c98d6b59cd9e0e0588baa14f5064eaa9dbdcdacc9b5c52210737f13fc
d5d09f064db85074cfd5f15dcdd0eddce0cf9fc8be46c310ea
3be7c69b3749

Steps to install the script:

1. Download and copy the script to the CloudVision Portal VM or the CloudVision Appliance
2. Change path to the location of the script and allow the script to have the execute permission using the following command:

```
Chmod +x security-advisory-0023-cvp-cva-mitigation.sh
```

3. Execute the script as root user:

```
sudo ./security-advisory-0023-cvp-cva-mitigation.sh
Patch applied successfully!
```

The script ensures that the hotfix is persistent across system reboots.

References:

For more information visit:

https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-5696

http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-5696

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