Date: May 6th, 2016

Version: 1.2

Revision	Date	Changes
1.0	May 6th, 2016	Initial release
1.1	May 12th, 2016	Updated to include assessment for CVX and CVP. Change in vulnerability status for CVE-2016-2107.
1.2	May 20th, 2016	Updated to include hotfix to address CVE-2016-2108. Updated the EOS Software versions that are vulnerable to CVE-2016-2108.

Arista Products vulnerability report for security vulnerabilities announcement from the OpenSSL project on May 3rd, 2016

In May 2016, the OpenSSL project issued a series of security advisories. This advisory reports the vulnerability assessment for Arista products.

Vulnerability report for EOS and CloudVision eXchange (CVX):

EOS and CVX are **not affected** by the following vulnerabilities:

- **CVE-2016-2105** (EVP_EncodeUpdate overflow)
- **CVE-2016-2106** (EVP_EncryptUpdate overflow)
- **CVE-2016-2109** (ASN.1 BIO excessive memory allocation)
- **CVE-2016-2176** (EBCDIC overread)
- **CVE-2016-2107** (Padding oracle in AES-NI CBC MAC check) - Version 1.0 of the advisory documented that EOS was affected by this vulnerability. The advisory has been updated (v1.1) to record an updated assessment.

EOS and CloudVision eXchange are vulnerable to the following:

CVE-2016-2108 (Memory corruption in the ASN.1 encoder):

Software versions	All EOS releases starting 4.15.0F . The list of affected releases is documented in Table-2.
Status	Vulnerable

Affected Features	eAPI Client certificate
Details	This vulnerability revealed that the ASN.1 parser (specifically, d2i_ASN1_TYPE) can misinterpret a large universal tag as a negative zero value. Large universal tags are not present in any common ASN.1 structures (such as X509) but are accepted as part of ANY structures. Therefore, if an application deserializes untrusted ASN.1 structures containing an ANY field, and later re-serializes them, an attacker may be able to trigger an out-of-bounds write. This has been shown to cause memory corruption that is potentially exploitable with some malloc implementations.
Mitigation	To mitigate against this vulnerability do not configure client certificates in eAPI.
Resolution	Bug 156374 tracks this vulnerability for EOS. A software fix will be available in upcoming versions for the currently active EOS software trains. This advisory will be updated once the exact SW version is available.

Resolution

Patch file download URL: secAdvisory0020.swix
sha512sum secAdvisory0020.swix
bb4f22f54d244d2711b56dcf16ae710750da8060e1a94297d875daea0228cfb597253057b625a2e848f90bd5bf5d8ec2e89a75d4f3177d900729ae0d15bba0a2 secAdvisory0020.swix

NOTE

- This hotfix can be installed on all affected versions of EOS.
- Installing the patch will temporarily disrupt nginx and eAPI sessions when applied
- A reload of the switch is **not required** for the patch to take effect

Instructions to install the patch

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://10.10.0.1/secAdvisory0020.swix extension:
switch#verify /sha512 extension:secAdvisory0020.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:secAdvisory0020.swix supervisor-
peer:/mnt/flash/
switch(s2-standby)#copy flash:secAdvisory0020.swix extension:
```

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

```
switch#extension secAdvisory0020.swix
```

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

```
sswitch(s1)#extension secAdvisory0020.swix
switch(s2-standby)#extension secAdvisory0020.swix
```

If eAPI is enabled, the eAPI agent or the uwsgi service will restart after the patch has been installed.

3. Users running eAPI in a VRF namespace will have to cycle nginx to restart the API management service correctly after the patch installation.

```
switch(config)#management api http-commands
switch(config-mgmt-api-http-cmds)#vrf MGMT
switch(config-mgmt-api-http-cmds-vrf-MGMT)#shutdown
switch(config-mgmt-api-http-cmds-vrf-MGMT)#no shutdown
switch(config-mgmt-api-http-cmds-vrf-MGMT)#end
```

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

```
switch#show extensions
Name                                          Version/Release           S
tatus extension
--------------------------------------------- ------------------------- -
----- ----
secAdvisory0020.swix                          1.0.0e.Ar/3187103.CVE2016 A
, I      1
A: available | NA: not available | I: installed | NI: not installed |
F: forced
```

5. 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
secAdvisory0020.swix
```

6. 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
```

AFFECTED EOS RELEASES:

Table-2: Affected EOS releases

4.15
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-7060QX

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

* First EOS release to support CloudVision eXchange
** First EOS release to support eAPI with client certificates

Vulnerability report for CloudVision Portal (CVP)

CloudVision Portal is only **affected** by the following vulnerabilities:

- **CVE-2016-2107** (Padding oracle in AES-NI CBC MAC check)
- **CVE-2016-2108** (Memory corruption in the ASN.1 encoder)

This is tracked by bug 157236 which will be fixed in release 2016.1.1.

References:

For more information on these vulnerabilities please visit:

https://www.openssl.org/news/secadv/20160503.txt

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