Date: March 1st, 2016

Version: 1.0

Revision	Date	Changes
1.0	March 1st, 2016	Initial release. Issue under investigation.
1.1	March 7th, 2016	Updated to include assessment

Arista Products vulnerability report for security vulnerabilities released by OpenSSL on March 1st, 2016

Arista's software products EOS and CloudVision Portal are **not vulnerable** to the following issues, as all features that offer an SSL server have the SSLv2 protocol explicitly disabled:

- Double-free in DSA code (CVE-2016-0705)
- Memory leak in SRP database lookups (CVE-2016-0798)
- BN_hex2bn/BN_dec2bn NULL pointer deref/heap corruption (CVE-2016-0797)
- Fix memory issues in BIO_*printf functions (CVE-2016-0799)
- Side channel attack on modular exponentiation (CVE-2016-0702)
- Bleichenbacher oracle in SSLv2 (CVE-2016-0704)
- Cross-protocol attack on TLS using SSLv2 (DROWN) (CVE-2016-0800)
- Divide-and-conquer session key recovery in SSLv2 (CVE-2016-0703)

CloudVision eXchange is affected only by the following two vulnerabilities:

NOTE: CloudVision eXchange (CVX) is deployed as a virtual appliance and runs an EOS image. Therefore only CVX features leveraging SSLv2 in the EOS releases are vulnerable.

- Cross-protocol attack on TLS using SSLv2 (DROWN) (CVE-2016-0800)
- Divide-and-conquer session key recovery in SSLv2 (CVE-2016-0703)

Product	CloudVision eXchange
Software versions	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
Status	Affected
Resolution	This is tracked by bug 145982 and the fix will be available in EOS releases 4.15.5M. Recommendation is to upgrade CVX instances to the remediated EOS version when available.

Details: SSL profiles are used by CloudVision eXchange (CVX) to encrypt Out-of-Band (OOB) communication which is supported starting EOS-4.15.0F. SSL profiles for Out-Of-Band communication in CVX is used for the following activities between the switch (client) and CVX (server):

- Heartbeat exchange between the CVX clients running on switches and CVX

CVX is vulnerable to CVE-2015-3197 (SSLv2 doesn't block disabled ciphers) as it does not disable the SSLv2 protocol, which allows clients to force SSLv2 connections leading to the DROWN attack. In addition to decrypting the CVX OOB connection, this attack could also allow eAPI traffic from CVX to be decrypted if both eAPI and CVX share the same SSL private key, even across different switches.

To verify if the CVX instance is using the same SSL private key for OOB and eAPI, check the output of the following commands to see if they are using the same SSL profile. In the following outputs the name of the SSL profile is ‘server-ssl’ and both commands indicate that the same SSL profile is being used therefore sharing the same certificate and key:

```
cvx#show cvx
CVX Server
 Status: Enabled
 UUID: beb19142-dfaa-11e4-b996-001c73105347
 Heartbeat interval: 20.0
```

```
 Heartbeat timeout: 60.0
 SSL profile: server-ssl
    Status: Enabled
```

```
cvx#show management api http-commands
Enabled:            Yes
HTTPS server:       running, set to use port 443
HTTP server:        shutdown, set to use port 80
Local HTTP server:  shutdown, no authentication, set to use port 8080
Unix Socket server: shutdown, no authentication
VRF:                default
Hits:               0
Last hit:           never
Bytes in:           0
Bytes out:          0
Requests:           0
Commands:           0
Duration:           0.000 seconds
SSL Profile:        server-ssl
QoS DSCP:           0
URLs
```

Mitigation to protect eAPI traffic from being decrypted: If eAPI is enabled on the CVX instance, it is recommended to configure the two features to use different SSL profiles which in turn use different certificate and keys to protect eAPI traffic from being decrypted. The following options are available to protect eAPI traffic from being decrypted:

- Configure eAPI to use a separate certificate/key by creating a new SSL profile with a new certificate/key

OR

- Configure CVX OOB communication to use a separate certificate/key by creating a new SSL profile with a new certificate/key

Instructions to setup a new SSL profile for eAPI

To configure eAPI to use a new HTTPS certificate, follow these instructions using a different SSL certificate from the one used for CVX. Ensure that a new PEM encoded server certificate and RSA key files are available to copy to the switch:

```
myswitch> enable
```

```
myswitch# copy scp:user@10.10.1.1/path-to-certificate/file-
name certificate:eapiServerCert
myswitch# copy scp:user@10.10.1.1/path-to-key/file-name sslkey:eapiServerKey
myswitch# configure terminal
myswitch(config)# management security
myswitch(config-mgmt-security)# ssl profile eapi
myswitch(config-mgmt-sec-ssl-profile-
eapi)# certificate eapiServerCert key eapiServerKey
myswitch(config-mgmt-sec-ssl-profile-eapi)# management api http-commands
myswitch(config-mgmt-api-http-cmds)# protocol https ssl profile eapi
myswitch(config-mgmt-api-http-cmds)# show management api http-
commands https certificate
   Certificate:
   ...

   Private Key:
   …
```

These instructions can also be viewed in the documentation for eAPI available on the switch - https://<switch-hostname/IP>/overview.html

Instructions to setup a new SSL profile for CVX

To configure a separate SSL profile on CVX for OOB using the following commands:

On the CVX server, copy the server certificate and key and also the CA certificate to verify CVX clients.

```
cvx(config)#!Copy the PEM encoded certificate and RSA key files for CVX server.
cvx(config)#!Lets call them server.crt and server.key
cvx(config)#copy url certificate:server.crt
cvx(config)#copy url sslkey:server.key
cvx(config)#!Copy the PEM encoded CA certificate to verify the certificate of CVX cli
ents.Lets call it ca.crt
cvx(config)#copy url certificate:ca.crt
```

On the CVX server, configure SSL profile with the certificates and key as below.

```
cvx(config)#management security
cvx(config-mgmt-security)#ssl profile cvx
cvx(config-mgmt-sec-ssl-profile-serverssl)#certificate server.crt key server.key
cvx(config-mgmt-sec-ssl-profile-serverssl)#trust certificate ca.crt
```

For additional details please refer to the TOI for CVX secure out-of-band connection.

References:

For more information on these vulnerabilities please visit:

OpenSSL Security Advisory [1st March 2016]

DROWN Attack - CVE-2016-0800

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