Date: October 4th, 2016

Version: 1.0

Revision	Date	Changes
1.0	October 4th, 2016	Initial release

Arista Products vulnerability report for security vulnerabilities announcement from the OpenSSL project on September 22nd, 2016

Product: EOS and CloudVision eXchange

These products are not vulnerable to the following

- CVE-2016-6305 (SSL_peek() hang on empty record)
- CVE-2016-6303 (OOB write in MDC2_Update())
- CVE-2016-6302 (Malformed SHA512 ticket DoS)
- CVE-2016-2182 (OOB write in BN_bn2dec())
- CVE-2016-2180 (OOB read in TS_OBJ_print_bio())
- CVE-2016-2177 (Pointer arithmetic undefined behaviour)
- CVE-2016-2181 (DTLS replay protection DoS)
- CVE-2016-6306 (Certificate message OOB reads)
- CVE-2016-6307 (Excessive allocation of memory in tls_get_message_header())
- CVE-2016-6308 (Excessive allocation of memory in dtls1_preprocess_fragment())

EOS and CloudVision eXchange are vulnerable to the following:

- CVE-2016-6304 (OCSP Status Request extension unbounded memory growth)
    - **Affected Software versions:** EOS-4.17.0F, 4.17.1F, 4.17.1.1F, 4.17.1FX-VRRP6LL
    - **CVSS Scores:**
        - CVSS v3 Base Score: 7.5 (High)
        - CVSS v2 Base Score: 7.8 (High)
    - **Affected Features:** eAPI, CVX HA, VMtracer
    - **Impact**: A malicious attacker could cause a server that uses SSL (in this case EOS or CloudVision eXchange running the affected features) to run out of memory and have the service be rendered temporarily unavailable as a result. The switch or the VM would then come back, in about a minute or so, though repeated attacks could potentially increase the time before the service starts up again.
    - **Mitigation**: Use control plane ACLs to limit only known, secure devices to connect to the affected services.
    - **Resolution**: Bug 171788 tracks this issue and the fix will be available in the next version of supported EOS release trains.

- CVE-2016-2183 (SWEET32 Mitigation)
  - **Affected Software versions:** Table-1 documents the affected EOS releases
  - **CVSS Scores:**
    - CVSS v3 Base Score: 5.3 (Medium)
    - CVSS v2 Base Score: 5.0 (Medium)
  - **Affected Features:** CVX (OVSDB Connections) (Client), EOS copy command (Client), XMPP (Client)
  - **Impact**: To exploit this vulnerability both the OpenSSL server and client have to use 3DES to encrypt data over SSL. Only after 32GB have been transferred, the attacker can begin to decrypt data.
  - **Mitigation**: All affected features are SSL clients. To mitigate the issue, the SSL server that the clients are connecting to should not use the 3DES cipher.
  - **Resolution**: Bug 167755 tracks this issue and the fix will be available in the next version of supported EOS release trains.

- CVE-2016-2178 (Constant time flag not preserved in DSA signing)
  - **Affected Software versions**: Table-1 documents the affected EOS releases
  - **CVSS Scores**:
    - CVSS v3 Base Score: 5.5 (Medium)
    - CVSS v2 Base Score: 2.1 (Low)
  - **Affected Features:** SSH
  - **Impact**: This vulnerability can allow an attacker to recover the DSA private key under certain conditions. Since SSH supports DSA as an option, this can allow the attacker to recover the DSA key used on an sshd server.
  - **Mitigation**: It is recommended not to use DSA as a hostkey in the SSH server (i.e. on the switches or VMs running affected EOS versions)
  - **Resolution**: Bug 171791 tracks this issue and the fix will be available in the next version of supported EOS release trains.

AFFECTED EOS RELEASES:

Table-1: Affected EOS releases

4.17	4.16	4.15	4.14	Older release trains
4.17.0F 4.17.1F • EOS-4.17.1FX-VRRP6LL 4.17.1.1F	4.16.6M • EOS-4.16.6FX-7512R • EOS-4.16.6FX-7500R.1 • EOS-4.16.6FX-75	4.15.0F • 4.15.0FX • 4.15.0FXA • 4.15.0FX1 4.15.1F	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 4.14.5F	All releases from 4.10.1

	00R-bgpscale • EOS-4.16.6FX-7500R • EOS-4.16.6FX-7060X • EOS-4.16.6FX-7050X2.2 • EOS-4.16.6FX-7050X2 4.16.7M • EOS-4.16.7M-L2EVPN • EOS-4.16.7FX-MLAGISSU-TWO-STEP • EOS-4.16.7FX-7500R • EOS-4.16.7FX-760X 4.16.8M • EOS-4.16.8FX-MLAGISSU-TWO-STEP • EOS-4.16.8FX-7500R • EOS-4.16.8FX-7060X	• 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.2 4.15.6M 4.15.7M 4.15.8M	• 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	

Product: CloudVision Portal, CloudVision Appliance

CloudVision Portal and CloudVision Appliance are not vulnerable to the following:

- CVE-2016-6304 (OCSP Status Request extension unbounded memory growth)
- CVE-2016-6305 (SSL_peek() hang on empty record)
- CVE-2016-6303 (OOB write in MDC2_Update())
- CVE-2016-6302 (Malformed SHA512 ticket DoS)
- CVE-2016-2180 (OOB read in TS_OBJ_print_bio())
- CVE-2016-6307 (Excessive allocation of memory in tls_get_message_header())
- CVE-2016-6308 (Excessive allocation of memory in dtls1_preprocess_fragment())

CloudVision Portal and CloudVision Appliance are vulnerable to the following. Bug 171280 tracks patching OpenSSL for the following vulnerabilities and a fix will be available in the next release for CloudVision Portal. The recommendation is to upgrade to the software release once available. The advisory will be updated with the software version that will contain the fix.

- CVE-2016-2183 (SWEET32 Mitigation)
  - **CVSS Scores:**
    - CVSS v3 Base Score: 5.3 (Medium)
    - CVSS v2 Base Score: 5.0 (Medium)
  - **Mitigation:** It is recommended to not use 3DES ciphers for SSL connections
- CVE-2016-2182 (OOB write in BN_bn2dec())
  - **CVSS Scores:**
    - CVSS v3 Base Score: 9.8 (High))
    - CVSS v2 Base Score: 7.5 (High)
- CVE-2016-2177 (Pointer arithmetic undefined behaviour)
  - **CVSS Scores:**
    - CVSS v3 Base Score: 5.9 (Medium)
    - CVSS v2 Base Score: 4.3 (Medium)
- CVE-2016-2178 (Constant time flag not preserved in DSA signing)
  - **CVSS Scores:**
    - CVSS v3 Base Score: 5.5 (Medium)
    - CVSS v2 Base Score: 2.1 (Low)
  - **Mitigation:** It is recommended not to use DSA as a hostkey in the CloudVision Portal or CloudVision Appliance.
- CVE-2016-2181 (DTLS replay protection DoS)
  - **CVSS Scores:**
    - CVSS v3 Base Score: 7.5 (High)
    - CVSS v2 Base Score: 5.0 (Medium)
- CVE-2016-6306 (Certificate message OOB reads)
  - **CVSS Scores:**
    - CVSS v3 Base Score: 5.9 (Medium)
    - CVSS v2 Base Score: 4.3 (Medium)

References:

OpenSSL Security Advisory [22 Sep 2016]

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