Date: June 17th 2015

Revision	Date	Changes
1.0	June 17th, 2015	Initial release
1.1	November 4th, 2015	Updated to reflect versions with the fix for tracked bugs. Change in vulnerability status for CVE-2014-8176

Arista Products Vulnerability report for OpenSSL security updates released on June 11th, 2015.

In June 2015 the OpenSSL project issued seven security updates as part of their scheduled updates. This advisory documents the vulnerability status of Arista 7000 Products and Arista EOS in response to the seven vulnerabilities listed:

CVE-2015-4000 (Logjam Protection)

Vulnerability Status:	Not Affected
Details:	Support for export ciphers is disabled in OpenSSL enabled client/server features in EOS

CVE-2015-1788 (Malformed Elliptical Curve Parameters causes infinite loop)

Vulnerability Status:	Not Affected
Details:	SSL enabled features in EOS do not use elliptic curves

CVE-2015-1789 (Exploitable out-of-bounds read in X509_cmp_time)

Vulnerability Status:	Affected
Affected Features:	XMPP and VMTracer
Mitigation:	Use these features only on a secured network. Using these client features over an unsecured network can cause a Denial of Service attack but will not compromise information being transmitted.

Solution:	Bug 122820 tracks this issue and the fix is available in EOS versions 4.15.2F, 4.14.9M, 4.13.13M and it will be available in the next release of 4.12.

CVE-2015-1790 (PKCS7 crash with missing EnvelopedContent)

Vulnerability Status:	Affected
Affected Features:	EOS client features do not use PKCS7 syntax. EOS Extensions that use PKCS7 are vulnerable.
Mitigation:	Only accept PKCS7 files from trusted sources
Solution:	Bug 122821 tracks this issue and the fix is available in EOS versions 4.15.2F, 4.14.9M, 4.13.13M and will be available in the next release of 4.12.

CVE-2015-1791 (Race condition handling NewSessionTicket)

Vulnerability Status:	Affected
Affected Features:	eAPI (Affects EOS-4.14.0F and later releases)
Mitigation:	This vulnerability is an internal race condition and cannot be remotely exploited.
Solution:	Bug 122822 tracks this issue and the fix is available in EOS versions 4.15.2F, 4.14.9M, 4.13.13M and will be available in the next release of 4.12.

CVE-2015-1792 (CMS verify infinite loop with unknown hash function)

Vulnerability Status:	Not Affected
Details:	Not applicable to any EOS features

CVE-2014-8176 (Invalid free in DTLS)

Vulnerability Status:	Not Affected
Details	CVX does not use DTLS

NOTE: Our initial assessment was that CVX was affected starting 4.15.0F. As of revision 1.1 of this advisory, this assessment has been revised based on further investigation.

References:
For additional information about the vulnerability, please visit:
https://www.openssl.org/news/secadv_20150611.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