Date: November 4th 2015

Revision	Date	Changes
1.0	November 5th, 2015	Initial release

Arista Products vulnerability report for security vulnerabilities released for NTP in October, 2015

The NTP project released the following set of low and medium severity vulnerabilities. As of the date of this advisory, the version of ntpd in EOS release trains 4.15, 4.14, 4.13 and 4.12 is 4.2.6. This advisory documents the vulnerability status of Arista 7000 Products and Arista EOS in response to the vulnerabilities listed below:

CVE-2015-7871: (NAK to the Future: Symmetric association authentication bypass via crypto-NAK)

Vulnerability Status:	Not Affected
Details:	EOS does not use symmetric associations

CVE-2015-7855: (decodenetnum() will ASSERT botch instead of returning FAIL on some bogus values)

Vulnerability Status:	Not Affected
Details:	This vulnerability is exploited by sending crafted mode 6 or mode 7 packets to ntpd containing an unusually long data value. The ntpd configuration in EOS blocks mode 6 and mode 7 packets and hence is not affected.

CVE-2015-7854: (Password Length Memory Corruption Vulnerability)

Vulnerability Status:	Not Affected
Details:	This vulnerability is applicable only when ntpd configuration allows remote configuration requests. The ntpd configuration in EOS does not allow remote configuration requests.

CVE-2015-7853: (Invalid length data provided by a custom refclock driver could cause a buffer overflow)

Vulnerability Status:	Not Affected

Details:	This vulnerability is only applicable when using a custom refclock driver. The ntpd configuration in EOS does not support non-standard refclock drivers.

CVE-2015-7852: (ntpq atoascii() Memory Corruption Vulnerability)

Vulnerability Status:	Not Affected
Details:	This vulnerability is exploited by sending crafted mode 6 packets to ntpd. The ntpd configuration in EOS blocks mode 6 packets and hence is not affected

CVE-2015-7851: (saveconfig Directory Traversal Vulnerability)

Vulnerability Status:	Not Affected
Details:	This vulnerability is applicable only when ntpd configuration allows remote configuration requests. The ntpd configuration in EOS does not allow remote configuration requests.

CVE-2015-7850: (remote config logfile-keyfile)

Vulnerability Status:	Not Affected
Details:	This vulnerability is applicable only when ntpd configuration allows remote configuration requests. The ntpd configuration in EOS does not allow remote configuration requests.

CVE-2015-7849 trusted key use-after-free

Vulnerability Status:	Not Affected
Details:	This vulnerability is applicable only when ntpd configuration allows remote configuration requests. The ntpd configuration in EOS does not allow remote configuration requests.

CVE-2015-7848 mode 7 loop counter underrun

Vulnerability Status:	Not Affected

Details:	This vulnerability is applicable only if ntpd is configured to enable mode 7 packets. The ntpd configuration in EOS blocks mode 7 packets and hence is not affected.

CVE-2015-7701 Slow memory leak in CRYPTO_ASSOC

Vulnerability Status:	Not Affected
Details:	This vulnerability is applicable only if ntpd is configured to use autokey.The ntpd configuration in EOS does not use autokey and hence is not affected.

CVE-2015-7703: (configuration directives "pidfile" and "driftfile" should only be allowed locally)

Vulnerability Status:	Not Affected
Details:	This vulnerability is applicable only when ntpd is configured to allow remote configuration. The ntpd configuration in EOS does not allow remote configuration and hence is not affected.

CVE-2015-7704, CVE-2015-7705: (Clients that receive a KoD should validate the origin timestamp field)

Vulnerability Status:	Affected
Affected Features:	NTP. The attacker could send forged KoD messages causing the ntpd client to delay or stop querying its servers for time updates.
Mitigation	Restrict who can query ntpd to learn who its servers are, and what IPs are allowed to ask your system for the time
Solution	Bug 137693 tracks this issue and a fix will be available in upcoming releases on the supported code trains.

CVE-2015-7691, CVE-2015-7692, CVE-2015-7702: (Incomplete autokey data packet length checks)

Vulnerability Status:	Not Affected

Details:	These vulnerabilities are applicable only if ntpd is configured to use autokey.The ntpd configuration in EOS does not use autokey and hence is not affected.

References:
For additional information about the vulnerability, please visit:

- October 2015 NTP Security Vulnerability Announcement (Medium)

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