Date: April 25th, 2018

Version: 1.1

Revision	Date	Changes
1.0	May 3rd, 2016	Initial release
1.1	April 25th, 2018	Updated vulnerability information for CVE-2016-1549

Arista Products vulnerability report for security vulnerabilities announcement from the NTP project on April 26th, 2016

In April 2016, the Network Time Foundation issued a series of security advisories detailing low- and medium-severity vulnerabilities in ntpd, their network time synchronization daemon. EOS and CloudVision Portal use this daemon for time synchronization. This advisory reports the vulnerability assessment for Arista products.

Vulnerability report for EOS and CloudVision eXchange

Both EOS and CloudVision eXchange are not affected by the following vulnerabilities:

- **CVE-2016-1551** (Refclock impersonation vulnerability, AKA: refclock-peering)
- **CVE-2016-2516** (Duplicate IPs on unconfig directives will cause an assertion botch)
- **CVE-2016-2517** (Remote configuration trustedkey/requestkey values are not properly validated)
- **CVE-2016-2518** (Crafted addpeer with hmode > 7 causes array wraparound with MATCH_ASSOC)
- **CVE-2016-2519** (ctl_getitem() return value not always checked)
- **CVE-2015-7704** (KoD fix: peer associations were broken by the fix for NtpBug2901, AKA: Symmetric active/passive mode is broken)
- **CVE-2016-1549** (Sybil vulnerability: ephemeral association attack, AKA: ntp-sybil)

EOS and CloudVision eXchange are vulnerable to the following vulnerabilities:

CVE-2016-1548 (Interleave-pivot):

Software versions	All EOS releases shipped prior to the date of this release are affected. The list of affected releases is documented in Table-2.
Status	Vulnerable
Details	This vulnerability exposes the possibility for a remote attacker to change the time of an ntpd

	client or deny service to an ntpd client by forcing it to change from basic client/server mode to interleaved symmetric mode. An attacker can spoof a packet from a legitimate ntpd server with an origin timestamp that matches the peer->dst timestamp recorded for that server. Following this, the client will reject all future legitimate server responses.
Mitigation	In order to protect against this vulnerability we recommend configuring a shared key with the trusted ntp servers and configuring "ntp authentication-key" with a password key on EOS; this enables the use of NTP's symmetric key authentication method in EOS to prevent people from outside the set of authorized personnel from sending in rogue NTP packets to try and exploit the issues. Example: switch(config)#ntp server 2.2.2.2 key 3333 switch(config)#ntp authentication-key 3333 sha1 cleartext
Resolution	Bug 155380 tracks this vulnerability for EOS. A software fix will be available in upcoming versions for the currently active EOS software trains.

CVE-2015-8138 (Zero Origin Timestamp Bypass, AKA: Additional KoD Checks):

Software versions	All EOS releases shipped prior to the date of this release are affected. The list of affected releases is documented in Table-2.
Status	Vulnerable
Details	This vulnerability exposes the possibility of a logic error that can allow packets with an origin timestamp of zero to bypass client attempts to check for legitimate peer responses.
Mitigation	In order to protect against this vulnerability we recommend configuring a shared key with the trusted ntp servers and configuring "ntp authentication-key" with a password key on EOS; this enables the use of NTP's

	symmetric key authentication method in EOS to prevent people from outside the set of authorized personnel from sending in rogue NTP packets to try and exploit the issues. Example: switch(config)#ntp server 2.2.2.2 key 3333 switch(config)#ntp authentication-key 3333 sha1 cleartext
Resolution	Bug 155381 tracks this vulnerability for EOS.A software fix will be available in upcoming versions for the currently active EOS software trains.

CVE-2016-1547 (Validate crypto-NAKs, AKA: nak-dos):

Software versions	All EOS releases shipped prior to the date of this release are affected. The list of affected releases is documented in Table-2.
Status	Vulnerable
Details	This vulnerability can allow an off-path attacker cause a preemptable client association to be demobilized by sending a crypto NAK packet to a victim client with a spoofed source address of an existing associated peer. This is true even if authentication is enabled.
Resolution	Bug 155375 tracks this vulnerability for EOS.

CVE-2016-1550 (Improve NTP security against buffer comparison timing attacks, authdecrypt-timing, AKA: authdecrypt-timing):

Software versions	All EOS releases shipped prior to the date of this release are affected. The list of affected releases is documented in Table-2.
Status	Vulnerable
Details	With this vulnerability there is a possibility for a local or LAN-based attacker to send a packet with an authentication payload and indirectly observe how much of the digest has matched.

Resolution	Bug 155376 tracks this vulnerability for EOS.

AFFECTED EOS RELEASES:

Table-2: Affected EOS releases

4.15	4.14	4.13	Older release trains
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-750	4.14.0F 4.14.1F 4.14.2F 4.14.3F 4.14.3.1F 4.14.4F 4.14.4.1F 4.14.4.2F 4.14.5F • 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	4.13.1.1F 4.13.2.1F 4.13.3.1F* 4.13.4.1F 4.13.5F 4.13.5.1F 4.13.6F 4.13.7M 4.13.7.2M 4.13.7.3M 4.13.8M 4.13.9M 4.13.9.1M 4.13.10M 4.13.11M 4.13.12M 4.13.13M 4.13.14M	All releases in 4.12 All releases in 4.11 All releases in 4.10 All releases in 4.9 All releases in 4.8 All releases in 4.7 All releases in 4.6 All releases in 4.5 All release trains older than 4.5

0R 4.15.6M	4.14.9.1M 4.14.10M 4.14.10.1M 4.14.11M 4.14.12M	4.13.15M	
* First EOS release to support CloudVision eXchange			

Vulnerability report for CloudVision Portal (CVP)

CloudVision Portal running NTP as a client **is affected** by the following vulnerabilities:

- **CVE-2016-1548** (Interleave-pivot)
- **CVE-2015-8138** (Zero Origin Timestamp Bypass, AKA: Additional KoD Checks)

Affected releases: 2015.1.0, 2015.1.1, 2015.1.2, 2016.1.0

Mitigation: There is no mitigation available.

Resolution: Bugs 155917 and 155918 tracks this vulnerability in CloudVision Portal and will be fixed in release 2016.1.1.

References:

For more information on these vulnerabilities please visit:

http://support.ntp.org/bin/view/Main/SecurityNotice#Recent_Vulnerabilities

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