Date: January 9th 2015

Revision	Date	Changes
1.0	January 9th 2015	Initial release

Arista 7000 Series Products and Arista EOS are not vulnerable to NTP CVE-2014-9293, CVE-2014-9294, CVE-2014-9295, and CVE-2014-9296.

In December 2014, the Network Time Foundation issued a series of security advisories detailing vulnerabilities in ntpd, their network time synchronization daemon. EOS uses this daemon for time synchronization, and a number of customers have contacted Arista Networks to ask whether their switches are affected. EOS is not exposed to these vulnerabilities, provided that users configure NTP through Arista's CLI rather than directly configuring ntpd, and that they do not use the ntp-keygen program to generate MD5 authentication keys.

CVE-2014-9293 (Weak default key in config_auth()): Not vulnerable.

CVE-2014-9294 (Non-cryptographic random number generator with weak seed used by ntp-keygen to generate symmetric keys): Not vulnerable unless configured to use MD5 authentication for NTP and the MD5 key is generated manually with the ntp-keygen program. Arista EOS does not provide any mechanism for generating the key for NTP authentication. The ntp-key program can only be executed from the bash shell. If a user has generated a key using ntp-keygen from the bash shell the resulting key would be weak in MD5 authentication.

CVE-2014-9295 (Buffer overflows in crypto_recv(), ctl_putdata(), and configure()): Not vulnerable.

CVE-2014-9296 (Missing return on error in receive()): Not vulnerable.

References:
For more information on vulnerability please visit:
http://support.ntp.org/bin/view/Main/SecurityNotice
https://rhn.redhat.com/errata/RHSA-2014-2024.html

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