

**Date:** 4/9/2014

Arista 7000 Series Products and Arista EOS Not Vulnerable to OpenSSL CVE-2014-0160

On April 7<sup>th</sup>, the OpenSSL Project issued a security advisory for a TLS heartbeat read overrun vulnerability. This vulnerability allows attackers to access the memory of web servers and potentially access confidential data.

A number of customers have contacted Arista Networks, understandably worried that their Arista products are susceptible to the SSL vulnerability. We can confirm that Arista EOS and Arista 7000 Series products are not vulnerable.

This exploit was introduced with the implementation of RFC 6520 on more recent versions of OpenSSL. The affected versions of OpenSSL are as follows:

OpenSSL 1.0.1 through 1.0.1f (inclusive) are vulnerable

OpenSSL 1.0.1g is NOT vulnerable

OpenSSL 1.0.0 branch is NOT vulnerable

OpenSSL 1.0.0e is NOT vulnerable

OpenSSL 0.9.8 branch is NOT vulnerable

Arista EOS do not include vulnerable versions of OpenSSL and are therefore NOT impacted by this vulnerability.

## References:

For more information about the vulnerability, please visit:

<http://heartbleed.com/>

## Verification:

Verification of the OpenSSL version running in EOS:

```
switch# show version detail |grep -i openssl  
openssl 1.0.0e.Ar 1709429.4134F.1
```

## Alternative command

```
switch#bash rpm -qi openssl  
Name: openssl  
Relocations: (not relocatable)  
Version: 1.0.0e.Ar
```

Vendor: (none)  
Release: 1709429.4134F.1  
Build Date: Tue Mar 18 20:52:37 2014  
Install Date: Fri Mar 21 13:13:16 2014  
Build Host: [dhcp-2006-102.sjc.arista.com](http://dhcp-2006-102.sjc.arista.com)  
Group: System Environment/Libraries  
Source RPM: openssl-1.0.0e.Ar-1709429.4134F.1.src.rpm  
Size : 3591792  
License: OpenSSL  
Signature: (none)  
URL : <http://www.openssl.org/>  
Summary : A general purpose cryptography library with TLS implementation

## Description :

The OpenSSL toolkit provides support for secure communications between machines. OpenSSL includes a certificate management tool and shared libraries which provide various cryptographic algorithms and protocols.  
switch#

## 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](mailto:support@arista.com)

By telephone: 408-547-5502

866-476-0000