A10 Products Not Vulnerable to OpenSSL CVE-2014-0160 (Heartbleed)

Posted on April 9, 2014

On April 7th, the OpenSSL Project issued a security advisory (http://www.openssl.org/news/secadv_20140407.txt) 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 A10, understandably worried that their A10 products are susceptible to the SSL vulnerability. **We can confirm that A10 Thunder Series and AX 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 0.9.8 branch is NOT vulnerable

A10 Thunder, AX, ID, and EX Series hardware appliances and vThunder virtual appliances (including AWS AMI versions) do not include vulnerable versions of OpenSSL and are therefore **NOT** impacted by this vulnerability.

For more information about the vulnerability, please visit:

http://heartbleed.com/