Array Networks Security Advisory:
OpenSSL Heartbleed Vulnerability

Revision 1.0

Last Updated: April 9th, 2014

The purpose of this Array Networks Security Advisory is to advise customers that Array Networks products are not exposed to the OpenSSL Heartbleed vulnerability since we have a proprietary SSL implementation for processing SSL, TLS and DTLS service traffic.

Overview

Unlike HW and SW vendors who have integrated OpenSSL into their core product and service offerings, Array Networks products are not exposed to the OpenSSL Heartbleed vulnerability since we use a proprietary SSL stack to process SSL, TLS and DTLS service traffic.

Reference: CVE-2014-0160 https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-0160

Details

The TLS and DTLS implementations in OpenSSL 1.0.1, before 1.0.1g, do not properly handle Heartbeat Extension packets which allow remote attackers to obtain sensitive information from process memory via crafted packets that trigger a buffer over-read, as demonstrated by reading private keys, related to d1_both.c and t1_lib.c, aka the Heartbleed bug.

Array products, including APV, vAPV, AG, vxAG, and EOS products (TMX, SPX), uses Array's proprietary SSL stack to process all SSL, TLS and DTLS service traffic. Therefore, service traffic on Array products is not affected by this OpenSSL Heartbleed vulnerability.

In addition, Array products only have limited usage of OpenSSL for WebUI and SSH management. The versions of OpenSSL used by Array products are not affected by the OpenSSL Heartbleed vulnerability so management traffic on Array products is not affected by the vulnerability either.

Should you have any questions, please contact one of our customer service representatives at support@arraynetworks.com or Array Networks TAC telephone.