Array Networks Security Advisory:
OpenSSL ClientHello Sigalgs DoS Vulnerability

Advisory Date: March 23, 2015

The purpose of this Array Networks Security Advisory is to advise customers that Array Networks products are not exposed to the OpenSSL ClientHello Sigalgs DoS vulnerability because we use 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 ClientHello Sigalgs DoS vulnerability because we use a proprietary SSL stack to process SSL, TLS and DTLS service traffic.

Reference: CVE-2015-0291 https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-0291

Details

If a client connects to an OpenSSL 1.0.2 server and renegotiates with an invalid signature algorithms extension, a denial of service (NULL pointer dereference) will occur. This vulnerability can be exploited in a DoS attack against the server.

Array products, including APV, vAPV, AG, vxAG, TMX and SPX, use 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 ClientHello Sigalgs DoS vulnerability.

In addition, Array products have only a limited usage of OpenSSL for WebUI, XML-RPC and SOAP API management. The versions of OpenSSL used by Array products are not affected by the OpenSSL ClientHello Sigalgs DoS 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.