Array Networks Security Advisory:
OpenSSL Alternative Chains Certificate Forgery Vulnerability
CVE-2015-1793

Advisory Date: July 10, 2015

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

Overview

Unlike hardware and software vendors who have integrated OpenSSL into their core product and service offerings, Array Networks products are not exposed to the OpenSSL Alternative Chains Certificate Forgery vulnerability because we use a proprietary SSL stack to process SSL, TLS and DTLS service traffic.

Reference: CVE-2015-1793 https://www.openssl.org/news/secadv_20150709.txt

Details

During certificate verification, OpenSSL (starting from version 1.0.1n and 1.0.2b) will attempt to find an alternative certificate chain if the first attempt to build such a chain fails. An error in the implementation of this logic can mean that an attacker could cause certain checks on untrusted certificates to be bypassed, such as the CA flag, enabling them to use a valid leaf certificate to act as a CA and “issue” an invalid certificate. This vulnerability will impact any application that verifies certificates including SSL/TLS/DTLS clients and SSL/TLS/DTLS servers using client authentication.

Array products, including APV, vAPV, AG, vxAG, TMX, SPX and WAN, 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 the OpenSSL Alternative Chains Certificate Forgery vulnerability.

Array products only have 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 Alternative Chains Certificate Forgery vulnerability so management traffic on Array products is also not affected by this vulnerability.

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