Array Networks Security Advisory:
OpenSSL Vulnerability CVE-2016-0800 (DROWN)

Advisory Date: March 7, 2016

The purpose of this Array Networks Security Advisory is to advise customers that Array Networks application delivery controllers and secure access gateways (SSL VPNs) are not exposed to the OpenSSL DROWN vulnerability due to Array's proprietary SSL implementation for processing SSL and TLS service traffic.

Overview

Unlike hardware and software vendors who have integrated OpenSSL into their core product and service offerings, APV Series, TMX Series, AG Series, and SPX Series products of Array Networks are not exposed to the OpenSSL DROWN vulnerability because Array uses a proprietary SSL stack to process SSL and TLS service traffic.

Reference: CVE-2016-0800 https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-0800

Details

A cross-protocol attack was discovered that could lead to decryption of TLS sessions by using a server supporting SSLv2 and EXPORT cipher suites as a Bleichenbacher RSA padding oracle. Note that traffic between clients and non-vulnerable servers can be decrypted provided another server supporting SSLv2 and EXPORT ciphers (even with a different protocol such as SMTP, IMAP or POP) shares the RSA keys of the non-vulnerable server.

Array Networks products with ArrayOS TMX 6.5.2.x, ArrayOS APV 8.4.x.x, 8.5.x.x or 8.6.x.x, AG9.4.x.x/9.3.x.x/9.2.x.x versions or SPX 8.4.6.2.x, use a proprietary SSL stack to process SSL and TLS service traffic. In addition, Array's proprietary SSL stack disallows the use of the weak SSLv2 protocol. Therefore, service traffic on Array Networks products is not affected by this OpenSSL DROWN vulnerability.

On Array Networks ADC and SSL VPN products, the OpenSSL version used for WebUI, XML-RPC and SOAP API management also disallows the use of SSLv2. Therefore, 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 (1-877-99-ARRAY).