Array Networks Security Advisory:
OpenSSL Vulnerability CVE-2016-2108

Advisory Date: May 17, 2016

The purpose of this Array Networks Security Advisory is to advise customers that AG, APV and SPX products of Array Networks are not exposed to the OpenSSL vulnerability CVE-2016-2108 since we have the proprietary SSL implementation for processing SSL and TLS service traffic.

Overview

Unlike HW and SW vendors who have integrated OpenSSL into their core product and service offerings, AG, APV and SPX products of Array Networks are not exposed to the OpenSSL vulnerability CVE-2016-2108 since we use a proprietary SSL stack to process SSL and TLS service traffic.

Reference: CVE-2016-2108 https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-2108

Details

If an application deserializes untrusted ASN.1 structures containing an ANY field, and later reserializes them, an attacker may be able to trigger an out-of-bounds write. This has been shown to cause memory corruption that is potentially exploitable with some malloc implementations. This vulnerability affected versions of OpenSSL prior to April 2015.

AG, APV and SPX products of Array Networks use proprietary SSL stack to process SSL and TLS service traffic. Besides, the OpenSSL version used on these products is higher than the vulnerable one. Therefore, neither service traffic nor management traffic on AG, APV and SPX products is vulnerable to CVE-2016-2108.

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