Array Networks Security Advisory: OpenSSL Vulnerability CVE-2016-2107

Advisory Date: May 17, 2016

Overview

The AES-NI implementation in OpenSSL before 1.0.1t and 1.0.2 before 1.0.2h does not consider memory allocation during a certain padding check, which allows remote attackers to obtain sensitive cleartext information via a padding oracle attack when the connection uses an AES CBC cipher and the server supports AES-NI. This vulnerability is known as CVE-2016-2107.

Reference: CVE-2016-2107 https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-2107

Impact

AG, APV and SPX products of Array Networks use proprietary SSL stack to process SSL and TLS service traffic. Therefore, service traffic on these products is not affected by this vulnerability.

This vulnerability affects only management traffic on AG 1000/1100/1150/1200 and APV 10600/10650/11600/3600/3650/1600 v5/2600 v5/3600 v5. For details of affected versions and affected features, please refer to the “Status” section.

On other AG and APV models (except those listed above) and SPX products, neither service traffic nor management traffic is affected by this vulnerability.

Workaround

None.

Status

This table lists the affected products, software versions, and features. You can use this table to check whether your Array products are affected by this vulnerability.

Product	Affected Versions	Affected Features/Modules
APV 10600/10650/11600/3600/3650/1600 v5/2600 v5/3600 v5	All	WebUI, XML-RPC, SOAP API, RESTful API
AG 1000/1100/1150/1200	All	WebUI, XML-RPC

Solution

For APV and AG products, new ArrayOS versions will be released to address this vulnerability.

➢ ArrayOS APV Versions

The solution will be available from the following ArrayOS APV versions:

- Next ArrayOS APV 8.4.0.x release
- Next ArrayOS APV 8.5.0.x release
- Next ArrayOS APV 8.6.0.x release

➢ ArrayOS AG Versions

The solution will be available from the following ArrayOS AG versions:

- Next ArrayOS AG 9.3.0.x release (will be released around the end of August 2016)
- Next ArrayOS AG 9.4.0.x release (will be released around the end of June 2016)