Array Networks Security Advisory:
OpenSSL Vulnerability CVE-2016-6304

Advisory Date: October 11, 2016

Overview

Multiple memory leaks in t1_lib.c in OpenSSL before 1.0.1u, 1.0.2 before 1.0.2i, and 1.1.0 before 1.1.0a allow remote attackers to cause a denial of service (memory consumption) via large OCSP Status Request extensions. This vulnerability is known as CVE-2016-6304.

Reference: CVE-2016-6304 https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-6304

Impact

AG, APV and SPX products of Array Networks use proprietary SSL stack to process SSL service traffic. Besides, they do not process OCSP Status Request extensions. Therefore, service traffic on these products is not affected by this vulnerability.

This vulnerability affects only management traffic on these products. For details of affected versions and affected features, please refer to the "Status" section.

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	ArrayOS APV 8.5 and later	WebUI, XML-RPC, SOAP API, RESTful API, SSH
AG	All	WebUI, XML-RPC, SSH

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:

- ArrayOS APV 8.5.0.x release (will be released on October 13, 2016)
- ArrayOS APV 8.6.0.x release (will be released on October 28, 2016)
- ArrayOS APV 8.6.1.x release (will be released on October 31, 2016)

➢ ArrayOS AG Versions

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

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