Array Networks Security Advisory for TLS 1.x Padding Vulnerability (POODLE)

Advisory Date: December 12, 2014

Vulnerability Overview

Certain Array hardware and software SSL components, when using TLS 1.x before TLS 1.2, should be enhanced to check CBC padding bytes when terminating connections, without doing so make it easier for man-in-the-middle attackers to obtain clear-text data via a padding-Oracle attack, a variant of the CVE-2014-3566 vulnerability (POODLE).

Impact

Attackers may be able to decrypt sensitive data on secure connections.

Status

SSL connections based on hardware SSL and software SSL are affected.

The SSL feature of the APV/TMX/AG/SPX product is affected while WebUI, XML-RPC and SOAP are not affected.

No feature of the WAN optimization (aCelera) product is affected.

Product	Affected Versions	Affected Features/Modules
APV(x600)	All ArrayOS APV 8.5.1.x All ArrayOS APV 8.5.x earlier than 8.5.0.40 All ArrayOS APV 8.4.x	SSL (including soft SSL from APV 8.3.2)
TMX/APV(x200)	All ArrayOS TM 6.5.x	SSL
AG	All ArrayOS AG 9.x	SSL (including soft SSL from AG 9.2)
SPX	All ArrayOS SPX 8.x	SSL

Mitigation

If no ArrayOS version containing the solution is available for upgrade, you are recommended to use RC4 ciphers temporarily. Please refer to the "**ssl settings ciphersuite**" command in the ArrayOS CLI Handbook.

Array Networks Solution

For APV/TMX/AG/SPX, new ArrayOS versions have been released or will be released to address this vulnerability.

- **Available ArrayOS APV/TM Versions**

The solution has been available in or will be available from the following ArrayOS APV/TM versions:

- APV 8.5.1: A new ArrayOS APV 8.5.1.x version will be released on January 30, 2015.
- APV 8.5: ArrayOS APV 8.5.0.40 eliminating this vulnerability has been released on December 5, 2014.
- APV 8.4: A new ArrayOS APV 8.4.0.x version will be released on December 19, 2014.
- TM 6.5.2: A new ArrayOS TM 6.5.2.x version will be released on February 27, 2015.

- **Available ArrayOS AG/SPX Versions**

The solution has been available in or will be available from the following ArrayOS AG/SPX versions:

- AG 9.3: A new ArrayOS AG 9.3.0.x version will be released on January 15, 2015.
- SPX 8.6.4.2: A new ArrayOS SPX 8.4.6.2.x version will be released on December 31, 2014.