Array Networks Security Advisory:
TLS Vulnerability CVE-2015-4000 (Logjam)

Advisory Date: May 28, 2015
Revision: 1.1

Vulnerability Overview

In TLS protocol 1.2 and earlier, when a DHE_EXPORT cipher suite is enabled on a server but not on a client, it does not properly convey a DHE_EXPORT choice, which potentially allows man-in-the-middle attackers to conduct cipher-downgrade attacks by rewriting a ClientHello with DHE replaced by DHE_EXPORT and then rewriting a ServerHello with DHE_EXPORT replaced by DHE. This vulnerability has been assigned CVE-2015-4000 and is referred to as "Logjam".

Impact

This vulnerability allows a man-in-the-middle attacker to downgrade vulnerable TLS connections to 512-bit export-grade cryptography. This allows the attacker to read and modify any data passed over the connection.

Status

- ***For the APV/TMX product, the HTTPS/TCPS/FTPS virtual services and WebUI are NOT affected***, but XML-RPC and SOAP API are affected.
- ***For the AG/SPX product, the virtual sites, WebUI and XML-RPC are NOT affected.***
- For the WAN product, the SSL optimization function and WebUI are affected.

Product	Affected Versions	Affected Features/Modules
APV	All ArrayOS APV 8.x	XML-RPC and SOAP API
TMX	All ArrayOS TM 6.5.2.x	XML-RPC
WAN	All ArrayOS aCelera 4.2.4.x - 5.0.0.x	SSL optimization and WebUI

Mitigation

- **ArrayOS APV/TMX Mitigation Measure**
  Please limit access to the system using XML-RPC or SOAP API for now.
- **ArrayOS WAN/aCelera Mitigation Measure**
  None.

Array Networks Solution

For APV Series and WAN (aCelera), new ArrayOS versions will be released to address this vulnerability. For TMX, new ArrayOS TM versions will not address this vulnerability.

- **Available ArrayOS APV Version**

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

  - APV 8.5.1: A new ArrayOS APV 8.5.1.x version will be released on about June 5, 2015.
  - APV 8.5: A new ArrayOS APV 8.5.0.x version will be released on May 29, 2015.
  - APV 8.4: A new ArrayOS APV 8.4.0.x version will be released on May 29, 2015.

- **Available ArrayOS WAN Version**

  The solution will be available in future ArrayOS aCelera 4.2.4.x and 5.0.0.x versions.