Array Networks Security Advisory: OpenSSL SSL/TLS MitM Vulnerability CVE-2014-0224

Advisory Date: July 4, 2014

Vulnerability Overview

An attacker using a carefully crafted handshake can force the use of weak keying material in OpenSSL SSL/TLS clients and servers. This can be exploited by a Man-in-the-Middle (MitM) attack where the attacker can decrypt and modify traffic from the attacked client and server.

The attack can only be performed between a vulnerable client *and* server. OpenSSL clients are vulnerable in all versions of OpenSSL. Servers are only known to be vulnerable in OpenSSL 1.0.1 and 1.0.2-beta1.

Impact

Clients running affected OpenSSL versions are vulnerable to a man-in-the-middle attack when connecting to a server running OpenSSL 1.0.1 or 1.0.2. In this case, an attacker can exploit this vulnerability to decrypt and modify traffic between the client and the server.

Array WebUI, XMLRPC, and SOAP API are using the HTTPS server running the affected OpenSSL versions and therefore are affected by this vulnerability. Array WAN SSL acceleration are using the affected OpenSSL versions and therefore are affected by this vulnerability. For information about affected features and affected versions, please refer to the table in the Status section.

APV/TMX HTTPS-, TCPS- and FTPS-type virtual services and AG/SPX virtual site are using Array's proprietary SSL stack and are not affected by this vulnerability.

Status

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

Product	Affected Versions	Affected Features/Modules
APV	All ArrayOS APV 8.x	WebUI, XMLRPC and SOAP API
TMX	All ArrayOS TM 6.x	WebUI and XMLRPC
AG	All ArrayOS AG 9.x	WebUI and XMLRPC
SPX	All ArrayOS SPX 8.x	WebUI and XMLRPC
WAN	aCelera 4.2.3 and earlier	WAN SSL acceleration

Mitigation

To eliminate this vulnerability on the affected versions, administrators are recommended to take the following measures:

- Disable WebUI, XMLRPC and SOAP API, and use SSH instead to perform configuration tasks.
- Limit access to WebUI, XMLRPC and SOAP API only from trusted networks.

Array Networks Solution

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

- APV 8.4: ArrayOS APV 8.4.0.64 has been released on June 27, 2014
- APV 8.5: A new ArrayOS APV 8.5 version will be released in the end of July 2014.
- TM 6.5.2: A new ArrayOS TM 6.5.2 version will be released in the end of July 2014.

For AG, ArrayOS AG 9.3.0.91 without the known OpenSSL vulnerability has been released on June 30, 2014.

For SPX, a new ArrayOS SPX 8.4.6.2 version without the known OpenSSL vulnerability will be released in the middle of August 2014.

For WAN, ArrayOS aCelera 4.2.4 has been released to address this vulnerability on June 17, 2014.

After the ArrayOS version without this known OpenSSL vulnerability is available, you are recommended to upgrade the system.