Array Networks Security Advisory: CVE-2015-4458 Vulnerability

Advisory Date: July 14, 2015

Revision: 1.1, September 30, 2016

Vulnerability Overview

The SSL hardware acceleration vendor Cavium reported that a microcode vulnerability had affected their CNlite Family Chips and Adapters with the microcode from CNLite-MC-SSLm-MAIN/PLUS-2.05 to 2.07 installed. As a result, SSL/TLS implementations using Cavium's affected CNlite Family Chips and Adapters do not check the Message Authentication Code, which could allow an unauthenticated, remote attacker to modify the contents of an encrypted TLS packet without detection of the modifications.

In addition, Array's software SSL module does not check the Message Authentication Code and therefore are affected by this vulnerability.

The hardware and software vulnerability is known as CVE-2015-4458.

Impact

This vulnerability allows a man-in-the-middle attacker to modify data without being detected.

Status

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

- **ArrayOS APV Series**

Array TMX, APV x200, and APV 3500 series application delivery controller products use the SSL hardware cards with affected microcode versions installed and therefore the HTTPS/TCPS/FTPS virtual services are affected on them.

vAPV uses the software SSL module, therefore the HTTPS/TCPS/FTPS virtual services are affected on them.

For APV x600 series with non-N3 SSL hardware card installed, when they use the software SSL module to implement ECC security, the HTTPS/TCPS/FTPS virtual services are affected on them.

- **ArrayOS AG Series**

AG 1000+ and above series secure access gateway products use unaffected SSL hardware cards and therefore are not affected.

vxAG, and AG 1000 with no SSL hardware card installed, use the software SSL module and therefore L3 VPN and Web Access are affected on them.

Product	Affected Versions	Affected Features/Modules
TMX APVx200 APV3500	ArrayOS TM 6.5.2.63, 6.5.2.71 and 6.5.2.72	HTTPS/TCPS/FTPS virtual services
vAPV APVx600 Series (with non-N3 SSL hardware card installed)	All ArrayOS APV versions earlier than 8.6.0.19	HTTPS/TCPS/FTPS virtual services
vxAG AG 1000	All ArrayOS AG 9.4.0.x versions All ArrayOS AG 9.3.0.x versions	L3 VPN and Web Access

Mitigation

None.

Array Networks Solution

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

➢ **Available ArrayOS TM/APV Version**

- TM 6.5.2: The solution was available in the ArrayOS TM 6.5.2.74 version released on July 13, 2015 to address this vulnerability.
- APV 8.6: The solution was available in the ArrayOS APV 8.6.0.19 version released on May 10, 2016 to address this vulnerability.
- APV 8.5: There is no plan to include the solution in an ArrayOS APV 8.5 release. It is recommended to upgrade to ArrayOS APV 8.6.0.19 or later.
- APV 8.4: There is no plan to include the solution in an ArrayOS APV 8.4 release. It is recommended to upgrade to ArrayOS APV 8.6.0.19 or later.

➢ **Available ArrayOS AG Version**

- AG 9.4: The solution will be available in the next ArrayOS AG 9.4 release.
- AG 9.3: The solution will be available in a future ArrayOS AG 9.3 release.