Array Networks Security Advisory for SSL Timing Attack

Advisory Date: August 15, 2014
Revision: 1.1

Vulnerability Overview

When Array Networks APV/AG SSL stack decrypts PKCS#1 V1.5 data and finds a bad packet at different offsets, the time taken to process each bad packet varies significantly from the time taken to process good packets. This can lead to the famous Bleichenbacher attack on RSA-based cipher suites.

An attacker can exploit this timing difference to decrypt a recorded Client Key Exchange message to get the PreMaster Secret.

While theoretically possible, it is quite difficult to exploit. It is a timing attack and you should need to create a large number of connections and measure the differences in timing.

In addition, the timing difference can vary on a live system due to workload as well as Internet delay; therefore, it is not likely for the attacker to get accurate measurement of the timing difference.

Impact

SSL decryption based on the hardware SSL and soft SSL is affected by this vulnerability.

The SSL feature of the APV/TMX/AG/SPX is affected while no feature of WAN is affected.

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(x600)	All ArrayOS APV 8.x	SSL (including soft SSL from APV 8.3.2)
TMX/APV(x200)	All ArrayOS TM 6.x	SSL
AG	All ArrayOS AG 9.x	SSL (including soft SSL from AG 9.2)
SPX	All ArrayOS SPX 8.x	SSL

Mitigation

None.

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/TMX Versions**

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

- APV 8.5: ArrayOS APV 8.5.0.28 has been released on July 18, 2014.
- APV 8.4: ArrayOS APV 8.4.0.68 has been released on July 31, 2014.
- APV 8.3: ArrayOS APV 8.3.0.62 has been released in August 15, 2014.
- TM 6.5.2: ArrayOS TM 6.5.2.63 has been released on August 13, 2014.

➢ **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: ArrayOS AG 9.3.0.110 has been released on July 31, 2014.
- SPX 8.6.4.2: ArrayOS SPX 8.4.6.2.105 has been released on August 15, 2014.