Array Networks Security Advisory: Intel Firmware Vulnerabilities (CVE-2017-5705, CVE-2017-5706, CVE-2017-5707, CVE-2017-5708, CVE-2017-5709, CVE-2017-5710, CVE-2017-5711 and CVE-2017-5712)

Advisory Date: March 5, 2018

Overview

Researchers disclosed security vulnerabilities found in certain versions of Intel Management Engine (ME), Intel Trusted Execution Engine (TXE), and Intel Server Platform Services (SPS) firmwares. These security vulnerabilities are identified as CVE-2017-5705, CVE-2017-5706, CVE-2017-5707, CVE-2017-5708, CVE-2017-5709, CVE-2017-5710, CVE-2017-5711 and CVE-2017-5712, or called INTEL-SA-00086 by Intel itself.

Reference:

CVE-2017-5705 http://cve.mitre.org/cgi-bin/cvekey.cgi?keyword=CVE-2017-5705

CVE-2017-5706 http://cve.mitre.org/cgi-bin/cvekey.cgi?keyword=CVE-2017-5706

CVE-2017-5707 http://cve.mitre.org/cgi-bin/cvekey.cgi?keyword=CVE-2017-5707

CVE-2017-5708 http://cve.mitre.org/cgi-bin/cvekey.cgi?keyword=CVE-2017-5708

CVE-2017-5709 http://cve.mitre.org/cgi-bin/cvekey.cgi?keyword=CVE-2017-5709

CVE-2017-5710 http://cve.mitre.org/cgi-bin/cvekey.cgi?keyword=CVE-2017-5710

CVE-2017-5711 http://cve.mitre.org/cgi-bin/cvekey.cgi?keyword=CVE-2017-5711

CVE-2017-5712 http://cve.mitre.org/cgi-bin/cvekey.cgi?keyword=CVE-2017-5712

INTEL-SA-00086 https://security-center.intel.com/advisory.aspx?intelid=INTEL-SA-00086&languageid=en-fr

Impact

An attacker could gain unauthorized access to platform, Intel ME feature, and 3rd party secrets protected by Intel ME, SPS or TXE firmware.

Array Networks has thoroughly reviewed all the product lines and found that only the affected Intel SPS firmware version was installed on the following product models:

- APV 1600 v5
- APV 2600 v5

- APV 3600 v5
- APV 3650 v5
- AVX 3600 v5

Since Flash Descriptor write protections have been enabled on above-mentioned product models, to exploit vulnerabilities CVE-2017-5706 and CVE-2017-5709 that exist on the Intel SPS firmware of these models, an attacker needs physical access by manually opening the chassis of Array Networks products, and then updates the platform with a malicious firmware image through a flash programmer physically connected to the platform's flash memory.

Therefore, as long as Array Networks products are physically secured, they are NOT affected by all these vulnerabilities. Array Networks highly recommend you to physically secure your systems.

Status

Array Networks will work on a solution to update the firmware remotely to resolve these security vulnerabilities and follow up the updates of these security vulnerabilities.