

Silver Peak Security Advisory

Notification

Intel Q3'17 ME 11.x, SPS 4.0, and TXE 3.0 Security Review Cumulative Update, Escalation of Privilege

INTEL-SA-00086 published by Intel on November 20, 2017

Intel Manageability Engine (ME): CVE-2017-5705, CVE-2017-5708, CVE-2017-5711, CVE-2017-5712

Intel Server Platform Service (SPS): CVE-2017-5706, CVE-2017-5709

Intel Trusted Execution Engine (TXE): CVE-2017-5707, CVE-2017-5710

Summary:

In response to issues identified by external researchers, Intel has performed an in-depth comprehensive security review of its Intel® Management Engine (ME), Intel® Trusted Execution Engine (TXE), and Intel® Server Platform Services (SPS) with the objective of enhancing firmware resilience.

As a result, Intel has identified several security vulnerabilities that could potentially place impacted platforms at risk. Systems using ME Firmware versions 11.0/11.5/11.6/11.7/11.10/11.20, SPS Firmware version 4.0, and TXE version 3.0 are impacted.

We carefully reviewed all Silver Peak products. ME and TXE are not enabled in all Silver Peak platforms. SPS is enabled in one platform as determined by Intel's Detection Tool for INTEL-SA-00086 - <https://downloadcenter.intel.com/download/27150>. In order to exploit this vulnerability, an attacker needs physical access to the system's firmware flash to manually update the platform with a malicious firmware image. Since our systems are installed in controlled environments, the risk of an exploit is very low to none.

This vulnerability does not affect Silver Peak appliances including EdgeConnect and NX. It is not applicable to virtual appliances EdgeConnect-V, VX, and Silver Peak Unity Orchestrator/GMS.

Applicability to Silver Peak Products: Low to None

Recommended Action for Silver Peak Customers: None

Resolution: Not Applicable

Details:

The full details of the advisory are located at-

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

Advisory Revision History

Version	Date Updated	Changes
v1.0	November 22, 2017	Initial advisory
v2.0	December 1, 2017	More inputs on exploitability in paragraph 3 under summary

Thank you.

Security Incident Response Team

Silver Peak