Intel Management Engine Critical Firmware Update (Intel SA-00086)

Intel Management Engine (Intel ME 11.0.0-11.7.0), Intel Trusted Execution Engine (Intel TXE 3.0), and Intel Server Platform Services (Intel SPS 4.0) vulnerability (Intel-SA-00086)

Summary

On November 20th 2017, Intel published a security advisory regarding a firmware vulnerability in certain systems that utilize 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.

Threat level

High – Potential for:

- Impersonate the ME/SPS/TXE, thereby impacting local security feature attestation validity.
- Load and execute arbitrary code outside the visibility of the user and operating system.
- Cause a system crash or system instability.
- Attackers could utilize older vulnerabilities to gain access remotely (for example SA-00075).

Note: Based on information at time of writing, most of the vulnerabilities require local access.

Affected Products

- 6th, 7th & 8th Generation Intel® Core™ Processor Family
- Intel® Xeon® Processor E3-1200 v5 & v6 Product Family
- Intel® Xeon® Processor Scalable Family
- Intel® Xeon® Processor W Family
- Intel® Atom® C3000 Processor Family
- Apollo Lake Intel® Atom Processor E3900 series
- Apollo Lake Intel® Pentium™
- Celeron™ N and J series Processors

Recommendations

Our customer's security is paramount, to that end Stone are working with key vendors to provide firmware updates which close this vulnerability as quickly as possible. Those updates will be able available to download from this article as soon as they are made available to us

We recommend that customers ensure physical access is only granted to authorised individuals where possible and that all other possible steps have been taken to implement security policy.

We also highly recommend that all customers ensure they have applied firmware patches for Intel SA-00075 AMT security vulnerability (1st May 2017), to any vulnerable systems within their estates. Further information can be found here.

Actions:

Intel has released a discovery tool which will analyse your systems for the vulnerability, please follow the steps below and take appropriate action.

1. Determine if you have affected systems based on the list of affected products above.
2. Utilize the Intel-SA-00086 Detection Tool to assess if your system has the impacted firmware.
3. Stone highly recommends updating the firmware of affected systems as soon it becomes available. Please review the Downloads section of this article for firmware update availability.

Downloads

StonePC Lite / Tower / Pro / AIO

Product code	Motherboard model	Firmware download
BOAMOT-480	B150M-A	ME FW 11.8 corporate
BOAMOT-481	H110M-A-DP	ME FW 11.8 consumer
BOAMOT-482	Q170M-C	ME FW 11.8 corporate
BOAMOT-483 / BOAMOT-490	H110T	ME FW 11.8 consumer
BOAMOT-484	Q170T	ME FW 11.8 corporate
BOAMOT-485	B150M-A-M.2	ME FW 11.8 corporate
BOAMOT-488	PRIME B250M-A	ME FW 11.8 consumer
BOAMOT-489	PRIME Q270M-C	ME FW 11.8 corporate

StonePC Mini

Product code	Motherboard model	Firmware download
PCMSYS-100 / PCMSYS-102	H110D4-P1	BIOS 0403

StonePC Micro

Product code	Motherboard model	Firmware download
INTNUC-10015	NUC6i3SYB	BIOS SY0063
INTNUC-10016	NUC6i5SYB	BIOS SY0063
INTNUC-10017	NUC6I7KYB	TBD
INTNUC-10018	NUC7i3BNB	BIOS BN0057
INTNUC-10019	NUC7i5BNB	BIOS BN0057
INTNUC-10020	NUC7i7BNB	BIOS BN0057
INTNUC-10021	NUC6CAYH	BIOS AY0042

StoneBook Mini / Lite / Pro

Product code	Motherboard model	Firmware download
NOTCHA-276 / NOTCHA-280	N240JU	Awaiting release
NOTCHA-277 / NOTCHA-278 / NOTCHA-286 / NOTCHA-287 / NOTCHA-292	N250JU	Awaiting release
NOTCHA-279 / NOTCHA-281	W515LU	Awaiting release
NOTCHA-284 / NOTCHA-290	W515PU	Awaiting release
NOTCHA-283 / NOTCHA-285	N751BU	Awaiting release
NOTCHA-288 / NOTCHA-289	N240BU	Awaiting release

Applies to:

- Stone desktop, notebook and NUC products.

Note: For branded products supplied through Stone (Toshiba, Acer, Lenovo), please visit those manufacturers support pages directly.

29/11/2017