

INTEL HEREBY CONFIRMS THAT THERE IS A BACKDOOR IN ITS CHIPS

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

Intel ID:	INTEL-SA-00086
Product family:	Various
Impact of vulnerability:	Elevation of Privilege
Severity rating:	Important
Original release:	Nov 20, 2017
Last revised:	Nov 22, 2017

Summary:

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

As a result, Intel has identified security vulnerabilities that could potentially place impacted platforms at risk.

Description:

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.

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

Based on the items identified through the comprehensive security review, an attacker could gain unauthorized access to platform, Intel® ME feature, and 3rd party secrets protected by the Intel® Management Engine (ME), Intel® Server Platform Service (SPS), or Intel® Trusted Execution Engine (TXE).

This includes scenarios where a successful attacker could:

- 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.
- For more information, please see this Intel [Support article](#)

If the INTEL-SA-00086 Detection Tool reported your system being vulnerable, please check with your system manufacturer for updated firmware. Links to system manufacturer pages concerning this issue can be found at <http://www.intel.com/sa-00086-support>.

If you need further assistance, contact [Customer Support](#) to submit an online service request.

Recommendations:

The following CVE IDs are covered in this security advisory:

Intel® Manageability Engine Firmware 11.0.x.x/11.5.x.x/11.6.x.x/11.7.x.x/11.10.x.x/11.20.x.x

CVE ID	CVE Title	CVSSv3 Vectors	
CVE-2017-5705	Multiple buffer overflows in kernel in Intel Manageability Engine Firmware 11.0/11.5/11.6/11.7/11.10/11.20 allow attacker with local access to the system to execute arbitrary code.	8.2 High AV:L/AC:L/PR:H/UI:N/S:C/C:H/I:H/A:H	Intel Manageability Engine Firmware 8.x/9.x/10.x* <i>*The two CVE IDs above were also resolved in earlier generations of corporate versions of Intel ME, where Intel® Active Management Technology shares the same code base.</i>
CVE-2017-5708	Multiple privilege escalations in kernel in Intel Manageability Engine Firmware 11.0/11.5/11.6/11.7/11.10/11.20 allow unauthorized process to access privileged content via unspecified vector.	7.5 High AV:L/AC:H/PR:L/UI:N/S:C/C:H/I:H/A:N	
CVE-2017-5711	Multiple buffer overflows in Active Management Technology (AMT) in Intel Manageability Engine Firmware 8.x/9.x/10.x/11.0/11.5/11.6/11.7/11.10/11.20 allow attacker with local access to the system to execute arbitrary code with AMT execution privilege.	6.7 Moderate AV:L/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H	
CVE-2017-5712	Buffer overflow in Active Management Technology (AMT) in Intel Manageability Engine Firmware 8.x/9.x/10.x/11.0/11.5/11.6/11.7/11.10/11.20 allows attacker with remote Admin access to the system to execute arbitrary code with AMT execution privilege.	7.2 High AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H	
CVE ID	CVE Title	CVSSv3 Vectors	Server Platform
CVE-	Multiple buffer overflows in Active	6.7 Moderate	

2017-5711*	Management Technology (AMT) in Intel Manageability Engine Firmware 8.x/9.x/10.x/11.0/11.5/11.6/11.7/11.10/11.20 allow attacker with local access to the system to execute arbitrary code with AMT execution privilege.	AV:L/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H	Service 4.0.x.x Intel Trusted Execution Engine 3.0.x.x
CVE-2017-5712*	Buffer overflow in Active Management Technology (AMT) in Intel Manageability Engine Firmware 8.x/9.x/10.x/11.0/11.5/11.6/11.7/11.10/11.20 allows attacker with remote Admin access to the system to execute arbitrary code with AMT execution privilege.	7.2 High AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H	Intel has released a downloadable detection tool

CVE ID	CVE Title	CVSSv3 Vectors	
CVE-2017-5706	Multiple buffer overflows in kernel in Intel Server Platform Services Firmware 4.0 allow attacker with local access to the system to execute arbitrary code.	CVSS 8.2 High AV:L/AC:L/PR:H/UI:N/S:C/C:H/I:H/A:H	located at http://www.intel.com/support/00086-00086-support , which will analyze your system for the vulnerabilities identified in this security advisory.
CVE-2017-5709	Multiple privilege escalations in kernel in Intel Server Platform Services Firmware 4.0 allows unauthorized process to access privileged content via unspecified vector.	CVSS 7.5 High AV:L/AC:H/PR:L/UI:N/S:C/C:H/I:H/A:N	Intel highly recommends that all customers install the updated firmware and Intel® Capability License Service on impacted
CVE ID	CVE Title	CVSSv3 Vectors	
CVE-2017-5707	Multiple buffer overflows in kernel in Intel Trusted Execution Engine Firmware 3.0 allow attacker with local access to the system to execute arbitrary code.	CVSS 8.2 High AV:L/AC:L/PR:H/UI:N/S:C/C:H/I:H/A:H	
CVE-2017-5710	Multiple privilege escalations in kernel in Intel Trusted Execution Engine Firmware 3.0 allows unauthorized process to access privileged content via unspecified vector.	CVSS 7.5 High AV:L/AC:H/PR:L/UI:N/S:C/C:H/I:H/A:N	

platforms.

Associated CPU Generation	Resolved Firmware version
6th Generation Intel® Core™ Processor Family	Recommended: Intel® ME 11.8.50.3425 or higher Minimum: Intel® ME 11.8.50.3399
6th Gen X-Series Intel® Core™ Processor	Recommended: Intel® ME 11.11.50.1422 or higher Minimum: Intel® ME 11.11.50.1402
7th Generation Intel® Core™ Processor Family	Recommended: Intel® ME 11.8.50.3425 or higher Minimum: Intel® ME 11.8.50.3399

7 th Gen X-Series Intel® Core™ Processor	Recommended: Intel® ME 11.11.50.1422 or higher Minimum: Intel® ME 11.11.50.1402
8th Generation Intel® Core™ Processor Family	Recommended: Intel® ME 11.8.50.3425 or higher Minimum: Intel® ME 11.8.50.3399
Intel® Xeon® Processor E3-1200 v5 Product Family	Recommended: Intel® ME 11.8.50.3425 or higher Minimum: Intel® ME 11.8.50.3399 Intel® SPS 4.1.4.054
Intel® Xeon® Processor E3-1200 v6 Product Family	Recommended: Intel® ME 11.8.50.3425 or higher Minimum: Intel® ME 11.8.50.3399 Intel® SPS 4.1.4.054
Intel® Xeon® Processor Scalable Family	Intel SPS 4.0.04.288 Recommended: Intel® ME 11.21.50.1424 or higher Minimum: Intel® ME 11.21.50.1400
Intel® Xeon® Processor W Family	Recommended: Intel® ME 11.11.50.1422 or higher Minimum: Intel® ME 11.11.50.1402
Intel® Atom® C3000 Processor Family	Intel® SPS 4.0.04.139
Apollo Lake Intel® Atom Processor E3900 series	Intel® TXE Firmware 3.1.50.2222– Production version release
Apollo Lake Intel® Pentium™	Intel® TXE Firmware 3.1.50.2222– Production version release
Celeron™ N series Processors	Intel® TXE Firmware 3.1.50.2222– Production version release
Celeron™ J series Processors	Intel® TXE Firmware 3.1.50.2222– Production version release

Acknowledgements:

External Security Researchers and Intel Validation.

Intel would like to thank Mark Ermolov and Maxim Goryachy from Positive Technologies Research for working collaboratively with Intel on a coordinated disclosure and providing the initial finding for CVE-2017-5705, CVE-2017-5706 and CVE-2017-5707.

Related Information:

<http://www.intel.com/sa-00086-support>

Revision history:

Revision	Date	Description
1.0	20-November-2017	Initial Release

1.1	21-November-2017	Updated Recommended and minimum versions
1.2	22-November-2017	Updated links to online support page

Disclaimer:

INFORMATION IN THIS DOCUMENT IS PROVIDED "AS IS" IN CONNECTION WITH INTEL® PRODUCTS. YOUR USE OF THE INFORMATION IN THE DOCUMENT OR MATERIALS LINKED FROM THE DOCUMENT IS AT YOUR OWN RISK. INTEL RESERVES THE RIGHT TO CHANGE OR UPDATE THIS DOCUMENT AT ANY TIME. EXCEPT AS PROVIDED IN INTEL'S TERMS AND CONDITIONS OF SALE FOR SUCH PRODUCTS, INTEL ASSUMES NO LIABILITY WHATSOEVER, AND INTEL DISCLAIMS ANY EXPRESS OR IMPLIED WARRANTY, RELATING TO SALE AND/OR USE OF INTEL PRODUCTS INCLUDING LIABILITY OR WARRANTIES RELATING TO FITNESS FOR A PARTICULAR PURPOSE, MERCHANTABILITY, OR INFRINGEMENT OF ANY PATENT, COPYRIGHT OR OTHER INTELLECTUAL PROPERTY RIGHT. NO LICENSE, EXPRESS OR IMPLIED, BY ESTOPPEL OR OTHERWISE, TO ANY INTELLECTUAL PROPERTY RIGHTS IS GRANTED BY THIS DOCUMENT.