The latest security information on Intel® products.

2019.2 IPU – Intel® TXT Advisory

Intel ID:	INTEL-SA-00164
Advisory Category:	Firmware
Impact of vulnerability:	Information Disclosure
Severity rating:	MEDIUM

Intel ID:	INTEL-SA-00164
Original release:	11/12/2019
Last revised:	11/21/2019

Summary:

A potential security vulnerability in Intel® Trusted Execution Technology (TXT) with Intel® Processor Graphics may allow information disclosure. Intel is releasing firmware updates to mitigate this potential vulnerability.

Vulnerability Details:

CVEID: CVE-2019-0184

Description: Insufficient access control in protected memory subsystem for Intel(R) TXT for 6th, 7th, 8th and 9th Generation Intel(R) Core(TM) Processor Families; Intel(R) Xeon(R) Processor E3-1500 v5 and v6 Families; Intel(R) Xeon(R) E-2100 and E-2200 Processor Families with Intel(R) Processor Graphics and Intel(R) TXT may allow a privileged user to potentially enable information disclosure via local access.

CVSS Base Score: 6.0 Medium

CVSS Vector: CVSS:3.0/AV:L/AC:L/PR:H/UI:N/S:C/C:H/I:N/A:N

Affected Products:

Product Collection	Product Names	Vertical Segment	CPUID	Platform ID
8th Generation Intel® Core™ Processor Family	Intel® Core™ Processori7-8700B, i7-8850H Intel® Core™ Processori5-8400H, i5-8500B	Mobile	906EA	22
9th Generation Intel® Core™ Processor Family	Intel® Core™ Processor i9-9880H Intel® Core™ Processor i7-9850H Intel® Core™ Processor i5-9400H	Mobile	906ED	22
8th Generation Intel® Core™ Processor Family	Intel® Core™ Processori7-8700, i7-8700K, i7-8700T, i7-8086K Intel® Core™ Processor i5-8500, i5-8500T, i5-8600, i5-8600K, i5-8600T,	Desktop	906EA	22
Intel® Xeon® Processor E Family	Intel® Xeon® Processor E-2224G, E-2244G, E-2274G, E-2226G, E-2246G, E-2276G, E-2276M, E-2286G, E-2286M, E-2278G, E-2288G, E-2186G, E-2176G, E-2174G, E-2146G, E-2144G E-2136, E-2134, E-2126G, E-2124, E-2124G	Server	906EA	22
9th Generation Intel® Core™ Processor Family	Intel® Core™ Processor i9-9900K Intel® Core™ Processor i7-9700K	Desktop	906EC	22

9th Generation Intel® Core™ Processor Family	Intel® Core™ Processor i9-9900, i9-9900T Intel® Core™ Processor i7-9700, i7-9700T	Desktop	906ED	22
	Intel® Core™ Processor i5-9500, i5-9500T, i5-9600, i5-9600T, i5-9600K		906EA	
8th Generation Intel® Core™ Processor Family	Intel® Core™ Processor i7-8500Y, i7-8510Y Intel® Core™ Processor i5-8200Y, i5-8210Y, i5-8310Y	Mobile	806EC	10
8th Generation Intel® Core™ Processor Family	Intel® Core™ Processor i7-8706G Intel® Core™ Processor i5-8305G	Mobile	906E9	2A
7th Generation Intel® Core™ Processor Family	Intel® Core™ Processori7-7820HQ, i7-7920HQ Intel® Core™ Processor i5-7440HQ	Mobile	906E9	2A
8th Generation Intel® Core™ Processor Family	Intel® Core™ Processor i7-8650U Intel® Core™ Processor i5-8350U	Mobile	806EA	C0
7th Generation Intel® Core™ Processor Family	Intel® Core™ Processor i7-7700, i7-7700T Intel® Core™ Processori5-7500, i5-7500T, i5-7600, i5-7600T	Desktop	906E9	2A
7th Generation Intel® Core™ Processor Family	Intel® Core™ Processor i7-7820EQ Intel® Core™ Processori5-7440EQ, i5-7442EQ	Embedded	906E9	2A
7th Generation Intel® Core™ Processor Family	Intel® Core™ Processor i7-7600U Intel® Core™ Processor i5-7300U	Mobile	806E9	C0
7th Generation Intel® Core™ Processor Family	Intel® Core™ Processor i7-7660U, Intel® Core™ Processor i5-7360U	Mobile	806E9	C0
Intel® Xeon® Processor E3 v6 Family	Intel® Xeon® Processor v6 E3-1220, E3-1225, E3-1230, E3-1240, E3-1245, E3-1270, E3-1275, E3-1280, E3-1501L, E3-1501M, E3-1505L, E3-1505M, E3-1535M	Server	906E9	2A
7th Generation Intel® Core™ Processor Family	Intel® Core™ Processor i7-7Y75 Intel® Core™ Processor i5-7Y57	Mobile	806E9	C0
6th Generation Intel® Core™ Processor Family	Intel® Core™ Processor, i7-6820HQ, i7-6920HQ, Intel® Core™ Processor i5-6440HQ	Mobile	506E3	36
6th Generation Intel® Core™ Processor Family	Intel® Core™ Processor i7-6700, i7-6700T, i7-6785R Intel® Core™ Processor i5-6500, i5-6500T, i5-6600, i5-6600T, i5-6585R, i5-6685R	Desktop	506E3	36

6th Generation Intel® Core™ Processors	Intel® Core™ Processor i7-i7-6600U Intel® Core™ Processor i5-i5-6300U, i5-6310U	Mobile	406E3	C0
6th Generation Intel® Core™ Processor Family	Intel® Core™ Processor I7-6650U, I7-6660U Intel® Core™ Processor I5-6360U	Mobile	406E3	C0
Intel® Xeon® Processor E3 v5 Family	Intel® Xeon® Processor v5 E3-1220, E3-1225, E3-1230, E3-1235L, E3-1240, E3-1240L, E3-1245, E3-1260L, E3-1270, E3-1275, E3-1280, E3-1505M, E3-1515M, E3-1535M, E3-1545M, E3-1558L, E3-1565L, E3-1575M, E3-1578L, E3-1585, E3-1585L	Server	506E3	36
6th Generation Intel® Core™ Processor Family	Intel® Core™ Processor m7-6Y75 Intel® Core™ Processor m5-6Y57	Mobile	406E3	C0
6th Generation Intel® Core™ Processor Family	Intel® Core™ Processor i7-6700TE, i7-6820EQ, i7-6822EQ Intel® Core™ Processor i5-6440EQ, i5-6442EQ, i5-6500TE	Embedded	506E3	36
8th Generation Intel® Core™ Processor Family	Intel® Core™ Processor I7-8665U Intel® Core™ Processor I5-8365U	Mobile	806EC	C0

Recommendations:

Intel recommends that users of Intel® TXT update to the latest version provided by the system manufacturer that addresses these issues.

Acknowledgements:

This issue was found internally by Intel. Intel would like to thank Artem Shishkin, Bill Wager, Edgar Barbosa, Gabriel Negreira Barbosa, Gustavo de Castro Scotti, Jeffrey S Frizzell, Kekai Hu, Rodrigo Axel Monroy, Willem Pinckaers and Rodrigo Rubira Branco (BSDaemon).

Intel, and nearly the entire technology industry, follows a disclosure practice called Coordinated Disclosure, under which a cybersecurity vulnerability is generally publicly disclosed only after mitigations are available.

Revision History

Revision	Date	Description
1.0	11/12/2019	Initial Release
1.1	11/21/2019	Updated Acknowledgements
1.2	02/03/2020	Updated Acknowledgements

Legal Notices and Disclaimers

Intel provides these materials as-is, with no express or implied warranties.

All products, dates, and figures specified are preliminary based on current expectations, and are subject to change without notice.

Intel, processors, chipsets, and desktop boards may contain design defects or errors known as errata, which may cause the product to deviate from published specifications. Current characterized errata are available on request.

Intel technologies' features and benefits depend on system configuration and may require enabled hardware, software or service activation. Performance varies depending on system configuration. No product or component can be absolutely secure. Check with your system manufacturer or retailer or learn more at https://intel.com .

Some results have been estimated or simulated using internal Intel analysis or architecture simulation or modeling, and provided to you for informational purposes. Any differences in your system hardware, software or configuration may affect your actual performance.

Intel and the Intel logo are trademarks of Intel Corporation in the United States and other countries.

*Other names and brands may be claimed as the property of others.

Report a Vulnerability

If you have information about a security issue or vulnerability with an **Intel branded product or technology**, please send an e-mail to secure@intel.com . Encrypt sensitive information using our PGP public key .

Please provide as much information as possible, including:

- The products and versions affected
- Detailed description of the vulnerability
- Information on known exploits

A member of the Intel Product Security Team will review your e-mail and contact you to collaborate on resolving the issue. For more information on how Intel works to resolve security issues, see:

- Vulnerability handling guidelines

For issues related to Intel's external web presence (Intel.com and related subdomains), please contact Intel's External Security Research team.

Need product support?

If you...

- Have questions about the security features of an Intel product
- Require technical support
- Want product updates or patches

Please visit Support & Downloads .