The latest security information on Intel® products.

2019.2 IPU – Intel® Processor Security Advisory

Intel ID:	INTEL-SA-00240
Advisory Category:	Hardware
Impact of vulnerability:	Escalation of Privilege
Severity rating:	HIGH
Original release:	11/12/2019

Intel ID:	INTEL-SA-00240
Last revised:	07/30/2020

Summary:

Potential security vulnerabilities in System Management Mode (SMM) and Intel® Trusted Execution Technology (TXT) for some Intel® Core™ Processors and Intel® Xeon® Processors may allow escalation of privilege, denial of service or information disclosure. Intel is releasing firmware updates to mitigate these potential vulnerabilities.

Vulnerability Details:

CVEID: CVE-2019-0152

Description: Insufficient memory protection in System Management Mode (SMM) and Intel(R) TXT for certain Intel(R) Xeon(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access.

CVSS Base Score: 8.2 High

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

CVEID: CVE-2019-0151

Description: Insufficient memory protection in Intel(R) TXT for certain Intel(R) Core Processors and Intel(R) Xeon(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access.

CVSS Base Score: 7.5 High

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

Affected Products:

For CVE-2019-0152

Server:

- Intel® Xeon® Scalable Processor
- 2nd Generation Intel® Xeon® Scalable Processor
- Intel® Xeon® Processor D (2100, 3100)
- Intel® Xeon® Processor W (2100, 3100)

For CVE-2019-0151

Client:

- 4th generation Intel® Core™ Processors
- 5th generation Intel® Core™ Processors
- 6th generation Intel® Core™ Processors
- 7th generation Intel® Core™ Processors
- 8th generation Intel® Core™ Processors

*For Intel® Core™ Processors CVE-2019-0151 only impacts Intel® vPro™ Eligible Processors.

Server:

- Intel® Xeon® Processor E3 v2 Family
- Intel® Xeon® Processor E3 v3 Family
- Intel® Xeon® Processor E3 v4 Family
- Intel® Xeon® Processor E3 v5 Family

- Intel® Xeon® Processor E3 v6 Family
- Intel® Xeon® Processor E5 v2 Family
- Intel® Xeon® Processor E5 v3 Family
- Intel® Xeon® Processor E5 v4 Family
- Intel® Xeon® Processor E7 v2 Family
- Intel® Xeon® Processor E7 v3 Family
- Intel® Xeon® Processor E7 v4 Family
- Intel® Xeon® Scalable Processor
- 2nd Generation Intel® Xeon® Scalable Processor
- Intel® Xeon® Processor D (1500, 2100)
- Intel® Xeon® Processor E (2100, 2200)
- Intel® Xeon® Processor W (2100, 3100)

Recommendations:

Intel recommends that users of Intel server products listed above update to the latest firmware version provided by the system manufacturer that addresses these issues.

For client platforms listed above updated SINIT modules are available at https://www.intel.com/content/www/us/en/design/resource-design-center.html

Acknowledgements:

This was found internally by Intel. Intel would like to credit Joe Cihula, Gabriel Negreira Barbosa and Rodrigo Rubira Branco (BSDaemon) for CVE--2019-0151. As well as Gabriel Negreira Barbosa and Rodrigo Rubira Branco (BSDaemon) for CVE-2019-0152.

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	02/10/2020	Updated Acknowledgements
1.2	7/30/2020	Updated dowload link.

Legal Notices and Disclaimers

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.

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 .