INTEL-SA-00161

THE LATEST SECURITY INFORMATION ON INTEL® PRODUCTS.

Q3 2018 SPECULATIVE EXECUTION SIDE CHANNEL UPDATE

USA (English)

Intel ID:	**INTEL-SA-00161**
Product family:	Multiple
Impact of vulnerability:	Information Disclosure
Severity rating:	*See Security Advisory text*
Original release:	08/14/2018
Last revised:	07/24/2019

Summary:

Security researchers have identified a speculative execution side-channel method called L1 Terminal Fault (L1TF). This method impacts select microprocessor products supporting Intel® Software Guard Extensions (Intel® SGX). Further investigation by Intel has identified two related applications of L1TF with the potential to impact additional microprocessors, operating systems, system management mode, and virtualization software. If used for malicious purposes, this class of vulnerability has the potential to improperly infer data values from multiple types of computing devices.

Intel is committed to product and customer security and to coordinated disclosure. We worked closely with other technology companies, operating system, and hypervisor software vendors, developing an industry-wide approach to mitigate these issues promptly and constructively. For facts about these new exploits, technical resources, and steps you can take to help protect systems and information please visit: https://www.intel.com/securityfirst

.

Description:

CVE-2018-3615 - L1 Terminal Fault: SGX

- Systems with microprocessors utilizing speculative execution and Intel® software guard extensions (Intel® SGX) may allow unauthorized disclosure of information residing in the L1 data cache from an enclave to an attacker with local user access via a side-channel analysis.

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

USA (English)

CVE-2018-3620 - L1 Terminal Fault: OS/SMM

- Systems with microprocessors utilizing speculative execution and address translations may allow unauthorized disclosure of information residing in the L1 data cache to an attacker with local user access via a terminal page fault and a side-channel analysis.
- 6.5 Medium CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:C/C:H/I:N/A:N

CVE-2018-3646 - L1 Terminal Fault: VMM

- Systems with microprocessors utilizing speculative execution and address translations may allow unauthorized disclosure of information residing in the L1 data cache to an attacker with local user access with guest OS privilege via a terminal page fault and a side-channel analysis.
- 6.5 Medium CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:C/C:H/I:N/A:N

Affected products:

The following Intel-based platforms are potentially impacted by these issues. Intel may modify this list at a later time.

Intel® Core™ i3 processor (45nm and 32nm)
Intel® Core™ i5 processor (45nm and 32nm)
Intel® Core™ i7 processor (45nm and 32nm)
Intel® Core™ M processor family (45nm and 32nm)
2nd generation Intel® Core™ processors
3rd generation Intel® Core™ processors
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 ***
Intel® Core™ X-series Processor Family for Intel® X99 platforms
Intel® Core™ X-series Processor Family for Intel® X299 platforms
Intel® Xeon® processor 3400 series
Intel® Xeon® processor 3600 series
Intel® Xeon® processor 5500 series
Intel® Xeon® processor 5600 series
Intel® Xeon® processor 6500 series
Intel® Xeon® processor 7500 series
Intel® Xeon® Processor E3 Family
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 Family
Intel® Xeon® Processor E5 v2 Family
Intel® Xeon® Processor E5 v3 Family
Intel® Xeon® Processor E5 v4 Family
Intel® Xeon® Processor E7 Family
Intel® Xeon® Processor E7 v2 Family
Intel® Xeon® Processor E7 v3 Family
Intel® Xeon® Processor E7 v4 Family
Intel® Xeon® Processor Scalable Family
Intel® Xeon® Processor D (1500, 2100)

** indicates Intel microprocessors affected by CVE-2018-3615 - L1 Terminal Fault: SGX

Please check with your system manufacturer for more information regarding updates for your system.

USA (English)

Recommendations:

Intel has worked with operating system vendors, equipment manufacturers, and other ecosystem partners to develop platform firmware and software updates that can help protect systems from these methods.

This includes the release of updated Intel microprocessor microcode to our customers and partners. This microcode was previously released as part of INTEL-SA-00115 .

Status of available microcode can be found here .

End users and systems administrators should check with their system manufacturers and system software vendors and apply any available updates as soon as practical.

Acknowledgements:

Intel would like to thank Raoul Strackx[1],Jo Van Bulck[1], Marina Minkin[2], Ofir Weisse[3], Daniel Genkin[3], Baris Kasikci[3], Frank Piessens[1], Mark Silberstein[2], Thomas F. Wenisch[3], and Yuval Yarom[4] for reporting this issue and working with us on coordinated disclosure of CVE-2018-3615 (www.foreshadowattack.com)

[1]*imec-DistriNet, KU Leuven,* [2]*Technion,* [3]*University of Michigan,* [4]*University of Adelaide and Data61*

Intel would like to thank employees Rodrigo Branco, Henrique Kawakami, Ke Sun, and Kekai Hu for discovery of CVE-2018-3615, CVE-2018-3620 and CVE-2018-3646.

Intel would like to acknowledge Lei Shi, Qihoo360 CERT for his independent work on CVE-2018-3620.

Revision History

Revision	Date	Description
1.0	08/14/2018	Initial Release

Revision	Date	Description
1.1	08/23/2018	Correct CVSS entries
1.2	09/11/2018	Updated Acknowledgements
1.3	07/24/2019	Updated Acknowledgements

CVE Name: CVE-2018-3615, CVE-2018-3620, CVE-2018-3646

Legal Notices and Disclaimers

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 USA (English) 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?

The secure@intel.com e-mail address should only be used for reporting security issues.

If you...

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

Please visit Support & Downloads .