INTEL-SA-00115

THE LATEST SECURITY INFORMATION ON INTEL® PRODUCTS.

Report a Vulnerability Product Support

Q2 2018 SPECULATIVE EXECUTION SIDE CHANNEL UPDATE

Intel ID:	**INTEL-SA-00115**
Product family:	Multiple
Impact of vulnerability:	Information Disclosure
Severity rating:	Moderate
Original release:	05/21/2018
Last revised:	07/22/2019

Summary:

Security researchers identified two software analysis methods that, if used for malicious purposes, have the potential to improperly gather sensitive data from multiple types of computing devices with different vendors' processors and operating systems.

Intel is committed to product and customer security and to coordinated disclosure. We worked closely with other technology companies and several operating system and system software vendors, developing an industry-wide approach to mitigate these issues promptly.

For facts about these new methods, technical resources, and steps you can take to help protect your systems and information please visit: https://www.intel.com/securityfirst

.

Description:

CVE-2018-3639 – Speculative Store Bypass (SSB) – also known as Variant 4

- Systems with microprocessors utilizing speculative execution and speculative execution of memory reads before the addresses of all prior memory writes are known may allow unauthorized disclosure of information to an attacker with local user access via a side-channel analysis.
- 4.3 Medium CVSS:3.0/AV:L/AC:L/PR:N/UI:N/S:C/C:L/I:N/A:N

CVE-2018-3640 – Rogue System Register Read (RSRE) – also known as Variant 3a

Systems with microprocessors utilizing speculative execution and that perform speculative reads of system registers may allow unauthorized disclosure of system parameters to an attacker with local user access via a side-channel analysis.

- 4.3 Medium CVSS:3.0/AV:L/AC:L/PR:N/UI:N/S:C/C:L/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® Atom™ Processor C Series (C3308, C3338, C3508, C3538, C3558, C3708, C3750, C3758, C3808, C3830, C3850, C3858, C3950, C3955, C3958)
Intel® Atom™ Processor E Series
Intel® Atom™ Processor A Series
Intel® Atom™ Processor X Series (x5-E3930, x5-E3940, x7-E3950)
Intel® Atom™ Processor T Series (T5500, T5700)
Intel® Atom™ Processor Z Series
Intel® Celeron® Processor J Series (J3355, J3455, J4005, J4105)
Intel® Celeron® Processor N Series (N3450)
Intel® Pentium® Processor J Series (J4205)
Intel® Pentium® Processor N Series (N4000, N4100, N4200)
Intel® Pentium® Processor Silver Series (J5005, N5000)

Please check with your system vendor or equipment manufacturer for more information regarding updates for your system. For non-Intel based systems please contact your system manufacturer or microprocessor vendor.

Recommendations:

Most leading browser providers have recently deployed mitigations in their Managed Runtimes – mitigations that substantially increase the difficulty of exploiting side channels in a modern web browser. These techniques would likewise increase the difficulty of exploiting a side channel in a browser based on SSB.

Intel has released Beta microcode updates to operating system vendors, equipment manufacturers, and other ecosystem partners adding support for *Speculative Store Bypass Disable (SSBD)*. SSBD provides additional protection by providing a means for system software to completely inhibit a Speculative Store Bypass from occurring if desired. This is documented in whitepapers located at Intel's Software Side-Channel Security site . Most major operating system and hypervisors will add support for Speculative Store Bypass Disable (SSBD) starting as early as May 21, 2018.

The microcode updates will also address Rogue System Register Read (RSRR) – CVE-2018-3640 by ensuring that RDMSR instructions will not speculatively return data under certain conditions. This is documented in whitepapers located at Intel's Software Side-Channel Security site . No operating system or hypervisor changes are required to support the RDMSR change.

A listing of microcode updates that have been production qualified can be found here and will be updated as necessary. It is expected that remaining microcode updates, currently in beta, will be production qualified in the coming weeks. Intel recommends end users and systems administrators check with their OEM and system software vendors and apply any available updates as soon as practical.

Acknowledgements:

Intel would like to acknowledge and thank Jann Horn of Google Project Zero (GPZ) and Ken Johnson of the Microsoft Security Response Center (MSRC) for independently reporting CVE-2018-3639.

Intel would like to acknowledge and thank Zdenek Sojka, Rudolf Marek and Alex Zuepke from SYSGO AG (https://sysgo.com) for reporting CVE-2018-3640. Intel would also like to acknowledge and thank Innokentiy Sennovskiy from BiZone LLC (bi.zone).

Intel would like to thank Kekai Hu, Ke Sun, Henrique Kawakami and Rodrigo Branco for CVE-2018-3639 and CVE-2018-3640.

Revision History

Revision	Date	Description
1.0	May 21, 2018	Initial Release
1.1	June 21, 2018	Updated Recommendations
1.2	July 22, 2019	Updated Acknowledgements

CVE Name: CVE-2018-3639, CVE-2018-3640

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 computer system 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?

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

Please visit Support & Downloads .