



INTEL-SA-00233

THE LATEST SECURITY INFORMATION ON INTEL[®] PRODUCTS.

[Report a Vulnerability](#) [Product Support](#)

MICROARCHITECTURAL DATA SAMPLING ADVISORY



Intel ID:	INTEL-SA-00233
Advisory Category:	Hardware
Impact of vulnerability:	Information Disclosure
Severity rating:	MEDIUM
Original release:	05/14/2019
Last revised:	06/17/2019

Summary:

A potential security vulnerability in CPUs may allow information disclosure. Intel is releasing Microcode Updates (MCU) updates to mitigate this potential vulnerability.

Vulnerability Details:

CVEID: CVE-2018-12126

Microarchitectural Store Buffer Data Sampling (MSBDS): Store buffers on some microprocessors utilizing speculative execution may allow an authenticated user to potentially enable information disclosure via a side channel with local access.

CVSS Base Score: 6.5 Medium

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

CVEID: CVE-2018-12127




Microarchitectural Load Port Data Sampling (MLPDS): Load ports on some microprocessors utilizing speculative execution may allow an authenticated user to potentially enable information disclosure via a side channel with local access.

CVSS Base Score: 6.5 Medium

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



CVEID: CVE-2018-12130

USA (English)   

Microarchitectural Fill Buffer Data Sampling (MFBDS): Fill buffers on some microprocessors utilizing speculative execution may allow an authenticated user to potentially enable information disclosure via a side channel with local access.

CVSS Base Score: 6.5 Medium

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

CVEID: CVE-2019-11091

Microarchitectural Data Sampling Uncacheable Memory (MDSUM): Uncacheable memory on some microprocessors utilizing speculative execution may allow an authenticated user to potentially enable information disclosure via a side channel with local access.

CVSS Base Score: 3.8 Low

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

Affected Products:

A list of impacted products can be found here.

Recommendation:

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.

Status of available microcode can be found here.

Public Github: <https://github.com/intel/Intel-Linux-Processor-Microcode-Data-Files>

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

In addition, for Intel® SGX, Intel will perform a TCB Recovery operation to enable parties utilizing SGX to determine whether the microcode version related to this Intel SGX (English) has been applied on the platform the SGX attestation request originated from. Intel plans to update the Intel SGX Attestation Service (IAS) Dev environment on June 14th, 2019 and the IAS Production environment on July 12th, 2019, to return "GROUP_OUT_OF_DATE" response for affected platforms without the BIOS applied microcode update, and "CONFIGURATION_NEEDED" response for affected platforms that applied the microcode update through BIOS but with Intel® Hyper-Threading technology enabled.

Acknowledgements:

Microarchitectural Store Buffer Data Sampling (MSBDS) - CVE-2018-12126: This vulnerability was found internally by Intel employees. Intel would like to thank Ke Sun, Henrique Kawakami, Kekai Hu and Rodrigo Branco. It was independently reported by Lei Shi - Qihoo - 360 CERT and by Marina Minkin¹, Daniel Moghimi², Moritz Lipp³, Michael Schwarz³, Jo Van Bulck⁴, Daniel Genkin¹, Daniel Gruss³, Berk Sunar², Frank Piessens⁴, Yuval Yarom⁵ (¹University of Michigan, ²Worcester Polytechnic Institute, ³Graz University of Technology, ⁴imec-DistriNet, KU Leuven, ⁵University of Adelaide).

Microarchitectural Load Port Data Sampling (MLPDS) - CVE-2018-12127: This vulnerability was found internally by Intel employees and Microsoft. Intel would like to thank Brandon Falk – Microsoft Windows Platform Security Team, Ke Sun, Henrique Kawakami, Kekai Hu, and Rodrigo Branco - Intel. It was independently reported by Matt Miller – Microsoft, and by Stephan van Schaik, Alyssa Milburn, Sebastian Österlund, Pietro Frigo, Kaveh Razavi, Herbert Bos, and Cristiano Giuffrida - VUSec group at VU Amsterdam.

Microarchitectural Fill Buffer Data Sampling (MFBDS) - CVE-2018-12130: This vulnerability was found internally by Intel employees. Intel would like to thank Ke Sun, Henrique Kawakami, Kekai Hu and Rodrigo Branco. It was independently reported by Giorgi Maisuradze – Microsoft Research, and by Dan Horea Lutas, and Andrei Lutas - Bitdefender, and by Volodymyr Pikhur, and by Stephan van Schaik, Alyssa Milburn, Sebastian Österlund, Pietro Frigo, Kaveh Razavi, Herbert Bos, and Cristiano Giuffrida - VUSec group at VU Amsterdam, and by Moritz Lipp, Michael Schwarz, and Daniel Gruss - Graz University of Technology.

Microarchitectural Data Sampling Uncacheable Memory (MDSUM) – CVE-2019-11091: This vulnerability was found internally by Intel employees. Intel would like to thank Ke Sun, Henrique Kawakami, Kekai Hu and Rodrigo Branco. It was independently found by Volodymyr Pikhur, and by Moritz Lipp, Michael Schwarz, Daniel Gruss - Graz University of Technology, and by Stephan van Schaik, Alyssa Milburn, Sebastian Österlund, Pietro Frigo, Kaveh Razavi, Herbert Bos, and Cristiano Giuffrida - VUSec group at VU Amsterdam.

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	05/14/2019	Initial Release
1.1	06/17/2019	SGX update

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.

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.




Copyright © Intel Corporation 2019

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

USA (English)   

- › 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 security issues.


e-mail address should only be used for reporting

If you...

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

Please visit [Support & Downloads](#).

Company Information

 Commitment

USA (English)   

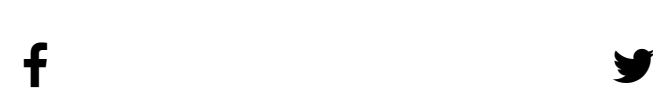
Communities

Investor Relations

Contact Us

Newsroom

Jobs



© Intel Corporation

Terms of Use

*Trademarks

Privacy

Cookies

Supply Chain Transparency

Site Map