USA (English)

INTEL-SA-00238

THE LATEST SECURITY INFORMATION ON INTEL® PRODUCTS.

Report a Vulnerability Product Support

MICROPROCESSOR MEMORY MAPPING ADVISORY

Intel ID:	**INTEL-SA-00238**
Advisory Category:	Hardware
Impact of vulnerability:	Information Disclosure
Severity rating:	LOW
Original release:04	04/09/2019
Last revised:	04/09/2019

Summary:

A potential security vulnerability in some microprocessors may allow information disclosure.

Vulnerability Details:

CVEID: CVE-2019-0162

Description: Memory access in virtual memory mapping for some microprocessors may allow an authenticated user to potentially enable information disclosure via 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:

Some Microprocessors with Virtual Memory Mapping.

Recommendations:

Intel recommends that users follow existing best practices to mitigate exploitation of this vulnerability. More information on these practices can be found here:

Security Best Practices For Side Channel Resistance:

https://software.intel.com/security-software-guidance/insights/security-best-practices-side-channel-resistance

Guidelines For Mitigating Timing Side Channels Against Cryptographic Implementations:

https://software.intel.com/security-software-guidance/insights/guidelines-mitigating-timing-side-channels-against-cryptographic-implementations

Additional information regarding Spoiler:

https://software.intel.com/security-software-guidance/insights/more-information-spoiler

Acknowledgements:

Intel would like to thank Saad Islam, Ahmad Moghimi, Berk Gulmezoglu, and Berk Sunar of Worcester Polytechnic Institute and Ida Bruhns, Moritz Krebbel, and Thomas Eisenbarth from University of Lübeck for reporting this issue.

This issue was found internally by Intel employees. Intel would like to thank Ke Sun, Henrique Kawakami, Kekai Hu and Rodrigo Branco.

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	04/09/2019	Initial Release

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.

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
- Require technical support
- Want product updates or patches

Please visit Support & Downloads .

Company Information

Our Commitment

Communities

Investor Relations

Contact Us

Newsroom

Jobs