The latest security information on Intel® products.

Special Register Buffer Data Sampling Advisory

Intel ID:	INTEL-SA-00320
Advisory Category:	Hardware
Impact of vulnerability:	Information Disclosure
Severity rating:	MEDIUM
Original release:	06/09/2020
Last revised:	06/12/2020

Summary:

A potential security vulnerability in some Intel® Processors may allow information disclosure. Intel is releasing firmware updates to mitigate this potential vulnerability.

Vulnerability Details:

CVEID: CVE-2020-0543

Description: Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access.

CVSS Base Score: 6.5 Medium

CVSS Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:C/C:H/I:N/A:N

Affected Products:

A list of impacted products can be found here

.

Recommendations:

Intel recommends that users of affected Intel® Processors update to the latest version firmware provided by the system manufacturer that addresses this issue.

Intel has released microcode updates for the affected Intel® Processors that are currently supported on the public github repository. Please see details below on access to the microcode:

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

The microcode updates also provide an opt-out mechanism (RNGDS_MITG_DIS) to disable the mitigation for RDRAND and RDSEED instructions executed outside of Intel® Software Guard Extensions (Intel® SGX) enclaves. Please refer to technical details to find additional information on the opt-out mechanism here

.

Note that inside of an Intel SGX enclave, the mitigation is applied regardless of the value of RNGDS_MITG_DIS.

Additional technical details about SRBDS can be found here

.

To address this issue, an SGX TCB recovery will be required in Q3 2020. Refer to Intel® SGX Attestation Technical Details for more information on the SGX TCB recovery process.

Acknowledgements:

Intel would like to thank Alyssa Milburn, Hany Ragab, Kaveh Razavi, Herbert Bos, Cristiano Giuffrida from the VUSec group at VU Amsterdam for reporting this issue.

This issue was also identified by Intel employees. Intel would like to thank Rodrigo Branco (formerly Intel), Kekai Hu (formerly Intel), Gabriel Negreira Barbosa (Intel), and Ke Sun (Intel).

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	Date	Description
1.0	06/09/2020	Initial Release
1.1	06/12/2020	Updated Acknowledgements

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 . 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? Report a Vulnerability 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 .

Company Overview

Contact Intel

Newsroom

Investors

Careers

Corporate Responsibility

Diversity & Inclusion

Public Policy

Terms of Use

*Trademarks

Cookies

Privacy

Supply Chain Transparency

Site Map