The latest security information on Intel® products.

2019.2 IPU – Intel® SGX with Intel® Processor Graphics Update Advisory

Intel ID:	INTEL-SA-00219
Advisory Category:	Firmware, Software
Impact of vulnerability:	Information Disclosure
Severity rating:	MEDIUM

Intel ID:	**INTEL-SA-00219**
Original release:	11/12/2019
Last revised:	11/20/2019

Summary:

A potential security vulnerability in Intel® Software Guard Extensions (SGX) enabled processors with Intel® Processor Graphics may allow information disclosure. Intel is releasing software and firmware updates to mitigate this potential vulnerability.

Vulnerability Details:

CVEID: CVE-2019-0117

Description: Insufficient access control in protected memory subsystem for Intel(R) SGX for 6th, 7th, 8th, 9th Generation Intel(R) Core(TM) Processor Families; Intel(R) Xeon(R) Processor E3-1500 v5, v6 Families; Intel(R) Xeon(R) E-2100 & E-2200 Processor Families with Intel(R) Processor Graphics may allow a privileged user to potentially enable information disclosure via local access.

CVSS Base Score: 6.0 Medium

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

Affected Products:

- 6th Generation Intel® Core™ processors
- 7th Generation Intel® Core™ processors
- 8th Generation Intel® Core™ processors
- 9th Generation Intel® Core™ processors
- Intel® Xeon® Processor E3 v5 Family
- Intel® Xeon® Processor E3 v6 Family
- Intel® Xeon® Processor E- 2100 Family
- Intel® Xeon® Processor E-2200 Family

Recommendations:

Intel recommends following the steps below to address these issues:

Impacted system users:

- Ensure the latest BIOS from your system provider and Intel SGX platform software (PSW) is installed.
- Disable integrated processor graphics where they are not used (usually server).
- Where integrated processor graphics are required, get updated SGX application(s) from your SGX application provider(s).

Application Providers:

- Organize the code/data within enclave memory to avoid putting sensitive materials in DWORD0 and DWORD1 of cache line. The effectiveness of this mitigation is dependent on the ability for the software to avoid the affected memory region. To assist the enclave application providers to modify their code, Intel is releasing SGX SDK update (Windows* version 2.5.101.3, Linux version 2.7.101.3) with new memory allocation APIs to avoid the affected memory region. More details about the APIs can be found here

  .
- Increase the Security Version Number (ISVSVN) of the enclave application to reflect that these modifications have been put in place.

- For existing solutions which utilize Remote Attestation (IAS), please refer to Intel® SGX Attestation Technical Details to determine whether you may need to implement changes to your SGX application for SGX attestation service.

The status of available microcode can be found here

.

Windows* developers can find latest SGX SDK at https://registrationcenter.intel.com/en/forms/?productid=2614

Linux developers can find latest SGX SDK at https://01.org/intel-software-guard-extensions/downloads

Acknowledgements:

This issue was found internally by Intel. Intel would like to thank Artem Shishkin, Edgar Barbosa, Gabriel Negreira Barbosa, Gustavo de Castro Scotti, Jeffrey S Frizzell, Kekai Hu, Rodrigo Axel Monroy, Willem Pinckaers
, and Rodrigo Rubira Branco (BSDaemon).

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	11/12/2019	Initial Release
1.1	11/20/2019	Updated acknowledgements
1.2	02/03/2020	Updated acknowledgements

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 product or component 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 Product Support

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?

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

intel