

The latest security information on Intel® products.

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

# 2019.2 IPU – Intel® Processor Graphics SMM Advisory

Intel ID:	INTEL-SA-00254
Advisory Category:	Hardware
Impact of vulnerability:	Information Disclosure

<b>Intel ID:</b>	<b>INTEL-SA-00254</b>
Severity rating:	MEDIUM
Original release:	11/12/2019
Last revised:	11/21/2019

## Summary:

A potential security vulnerability in System Management Mode (SMM) with Intel® Processor Graphics may allow information disclosure. Intel is releasing guidance to SMM developers to mitigate this potential vulnerability.

## Vulnerability Details:

CVEID: CVE-2019-0185

Description: Insufficient access control in protected memory subsystem for SMM for 6th, 7th, 8th and 9th Generation Intel(R) Core(TM) Processor families; Intel(R) Xeon(R) Processor E3-1500 v5 and v6 families; Intel(R) Xeon(R) E-2100 and 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:

- 6<sup>th</sup> Generation Intel® Core™ Processors
- 7<sup>th</sup> Generation Intel® Core™ Processors
- 8<sup>th</sup> Generation Intel® Core™ Processors
- 9<sup>th</sup> Generation Intel® Core™ Processors
- Intel® Xeon® Processor E3-1500 v5 and v6 Processors
- Intel® Xeon® E-2100 and E-2200 Processors

## Recommendations:

Intel recommends that users of the affected products update to the latest BIOS version provided by the system manufacturer that addresses this issue.

## Acknowledgements:

This issue was found internally by Intel. Intel would like to thank Artem Shishkin, Bill Wager, 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
----------	------	-------------

Revision	Date	Description
1.0	11/12/2019	Initial Release
1.1	11/21/2019	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.

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 2022

## 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](mailto: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](#)

[Diversity & Inclusion](#)

[Public Policy](#)



© Intel Corporation

[Terms of Use](#)

[\\*Trademarks](#)

[Cookies](#)

[Privacy](#)

[Supply Chain Transparency](#)

[Site Map](#)

Intel technologies may require enabled hardware, software or service activation. // No product or component can be absolutely secure. // Your costs and results may vary. // Performance varies by use, configuration and other factors. // See our complete legal [Notices and Disclaimers](#).

. // Intel is committed to respecting human rights and avoiding complicity in human rights abuses. See Intel's [Global Human Rights Principles](#). Intel's products and software are intended only to be used in applications that do not cause or contribute to a violation of an internationally recognized human right.

intel.