The latest security information on Intel® products.

2019.2 IPU – Intel® Processor Graphics SMM Advisory

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

Intel ID:	INTEL-SA-00254
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:

- 6th Generation Intel® Core™ Processors
- 7th Generation Intel® Core™ Processors
- 8th Generation Intel® Core™ Processors
- 9th 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

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 .