THE LATEST SECURITY INFORMATION ON INTEL® PRODUCTS.

2019.2 IPU – INTEL® GRAPHICS DRIVER FOR WINDOWS* AND LINUX ADVISORY

Intel ID:	**INTEL-SA-00242**
Advisory Category:	Software
Impact of vulnerability:	Escalation of Privilege, Denial of Service, Information Disclosure
Severity rating:	HIGH
Original release:	11/12/2019
Last revised:	11/12/2019

Summary:

Potential security vulnerabilities in Intel® Graphics Driver for Windows* and Linux may allow denial of service. Intel is releasing software updates to mitigate these potential vulnerabilities.

Vulnerability Details:

CVEID: CVE-2019-11112

Description: Memory corruption in Kernel Mode Driver in Intel(R) Graphics Driver before 26.20.100.6813 (DCH) or 26.20.100.6812 may allow an authenticated user to potentially enable escalation of privilege via local access.

CVSS Base Score: 8.8 High

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

CVEID: CVE-2019-0155

Description: Insufficient access control in a subsystem for Intel (R) processor graphics in 6th, 7th, 8th and 9th Generation Intel(R) Core(TM) Processor Families; Intel(R) Pentium(R) Processor J, N, Silver and Gold Series; Intel(R) Celeron(R) Processor J, N, G3900 and G4900 Series; Intel(R) Atom(R) Processor A and E3900 Series; Intel(R) Xeon(R) Processor E3-1500 v5 and v6, E-2100 and E-2200 Processor Families; Intel(R) Graphics Driver for Windows before 26.20.100.6813 (DCH) or

26.20.100.6812 and before 21.20.x.5077 (aka15.45.5077), i915 Linux Driver for Intel(R) Processor Graphics before versions 5.4-rc7, 5.3.11, 4.19.84, 4.14.154, 4.9.201, 4.4.201 may allow an authenticated user to potentially enable escalation of privilege via local access.

CVSS Base Score: 8.8 High

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

CVEID: CVE-2019-11111

Description: Pointer corruption in the Unified Shader Compiler in Intel(R) Graphics Drivers before 10.18.14.5074 (aka 15.36.x.5074) may allow an authenticated user to potentially enable escalation of privilege via local access.

CVSS Base Score: 7.3 High

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

CVEID: CVE-2019-14574

Description: Out of bounds read in a subsystem for Intel(R) Graphics Driver versions before 26.20.100.7209 may allow an authenticated user to potentially enable denial of service 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:N/I:N/A:H

CVEID: CVE-2019-14590

Description: Improper access control in the API for the Intel(R) Graphics Driver versions before 26.20.100.7209 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

CVEID: CVE-2019-14591

Description: Improper input validation in the API for Intel(R) Graphics Driver versions before 26.20.100.7209 may allow an authenticated user to potentially enable denial of service 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:N/I:N/A:H

CVEID: CVE-2019-11089

Description: Insufficient input validation in Kernel Mode module for Intel(R) Graphics Driver before version 25.20.100.6519 may allow an authenticated user to potentially enable denial of service via local access.

CVSS Base Score: 5.9 Medium

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

CVEID: CVE-2019-11113

Description: Buffer overflow in Kernel Mode module for Intel(R) Graphics Driver before version 25.20.100.6618 (DCH) or 21.20.x.5077 (aka15.45.5077) may allow a privileged user to potentially enable information disclosure via local access.

CVSS Base Score: 4.0 Medium

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

Affected Products:

6th, 7th, 8th, and 9th Gen Intel® Core™ processor family & 6th Gen Intel® Core™ processor family systems running Windows* 7 or Windows* 8.1 with Intel® Graphics Driver for Windows* before 26.20.100.6813 (DCH) or 26.20.100.6812 and before 21.20.x.5077 (aka15.45.5077).

4th Generation Intel® Core™/ Pentium®/ Xeon® (E3 v3 only) Processors systems running Windows* 7 or Windows* 8.1 with Intel® Graphics Driver for Windows* before versions 10.18.14.5074 (aka 15.36.x.5074).

Recommendations:

Intel recommends updating the Intel® Graphics Driver for Windows* and i915 Linux Driver to the latest version.

Windows* Driver updates are available for download at this location: https://downloadcenter.intel.com/product/80939/Graphics-Drivers

For i915 Linux Driver updates to mitigate CVE-2019-0155, contact your Linux OS Vendor.

Acknowledgements:

Intel would like to thank Piotr Bania of Cisco TALOS (CVE-2019-14574),

SSD Secure Disclosure / Ori Nimron / @orinimron123 (CVE-2019-11112) and Rancho Han of Tencent Security ZhanluLab (CVE-2019-11111) for reporting these issues and working with us on coordinated disclosure.

The additional issues were found internally by Intel employees. Intel would like to thank Artem Shishkin, Edgar Barbosa, Gabriel Barbosa, Gustavo Scotti, Kekai Hu, Rodrigo Axel Monroy, 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	11/12/2019	Initial Release
1.1	11/12/2019	Added Linux for CVE-2019-0155

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 .