INTEL-SA-00189

THE LATEST SECURITY INFORMATION ON INTEL® PRODUCTS.

INTEL® GRAPHICS DRIVER FOR WINDOWS* 2018.4 QSR ADVISORY

USA (English)

Intel ID:	INTEL-SA-00189
Advisory Category:	Software
Impact of vulnerability:	Escalation of Privilege, Denial of Service, Information Disclosure
Severity rating:	HIGH
Original release:	03/12/2019
Last revised:	03/20/2019

Summary:

Multiple potential security vulnerabilities in Intel® Graphics Driver for Windows* may allow escalation of privileges, denial of service or information disclosure. Intel is releasing Intel® Graphics Driver for Windows* updates to mitigate these potential vulnerabilities.

Vulnerability Details:

CVEID: CVE-2018-12209

Description: Insufficient access control in User Mode Driver in Intel(R) Graphics Driver for Windows* before versions 10.18.x.5059 (aka 15.33.x.5059), 10.18.x.5057 (aka 15.36.x.5057), 20.19.x.5063 (aka 15.40.x.5063) 21.20.x.5064 (aka 15.45.x.5064) and 24.20.100.6373 potentially enables an unprivileged user to read device configuration information via local access.

CVSS Base Score: 3.3 Low

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

CVEID: CVE-2018-12210

Description: Multiple pointer dereferences in User Mode Driver in Intel(R) Graphics Driver for Windows* before versions 10.18.x.5059 (aka 15.33.x.5059), 10.18.x.5057 (aka 15.36.x.5057), 20.19.x.5063 (aka 15.40.x.5063) 21.20.x.5064 (aka 15.45.x.5064) and 24.20.100.6373 potentially enables an unprivileged user to cause a denial of service via local access.

CVSS Base Score: 6.5 Medium

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

CVEID: CVE-2018-12211

Description: Insufficient input validation in User Mode Driver in Intel(R) Graphics Driver for Windows* before versions 10.18.x.5059 (aka 15.33.x.5059), 10.18.x.5057 (aka 15.36.x.5057), 20.19.x.5063 (aka 15.40.x.5063) 21.20.x.5064 (aka 15.45.x.5064) and 24.20.100.6373 potentially enables an unprivileged user to cause a denial of service via local access.

CVSS Base Score: 6.5 Medium

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

CVEID: CVE-2018-12212

Description: Buffer overflow in User Mode Driver in Intel(R) Graphics Driver for Windows* before versions 10.18.x.5059 (aka 15.33.x.5059), 10.18.x.5057 (aka 15.36.x.5057), 20.19.x.5063 (aka 15.40.x.5063) 21.20.x.5064 (aka 15.45.x.5064) and 24.20.100.6373 potentially enables an unprivileged user to cause a denial of service via local access.

CVSS Base Score: 6.5 Medium

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

CVEID: CVE-2018-12213

Description: Potential memory corruption in Kernel Mode Driver in Intel(R) Graphics Driver for Windows* before versions 10.18.x.5059 (aka 15.33.x.5059), 10.18.x.5057 (aka 15.36.x.5057), 20.19.x.5063 (aka 15.40.x.5063) 21.20.x.5064 (aka 15.45.x.5064) and 24.20.100.6373 potentially enables an unprivileged user to cause a denial of service 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:N/I:N/A:H

CVEID: CVE-2018-12214

Description: Potential memory corruption in Kernel Mode Driver in Intel(R) Graphics Driver for Windows* before versions 10.18.x.5059 (aka 15.33.x.5059), 10.18.x.5057 (aka 15.36.x.5057), 20.19.x.5063 (aka 15.40.x.5063) 21.20.x.5064 (aka 15.45.x.5064) and 24.20.100.6373 potentially enables a privileged user to execute arbitrary code via local access.

CVSS Base Score: 7.3 High

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

CVEID: CVE-2018-12215

Description: Insufficient input validation in Kernel Mode Driver in Intel(R) Graphics Driver for Windows* before versions 10.18.x.5059 (aka 15.33.x.5059), 10.18.x.5057 (aka 15.36.x.5057), 20.19.x.5063 (aka 15.40.x.5063) 21.20.x.5064 (aka 15.45.x.5064) and 24.20.100.6373 potentially enables a privileged user to cause a denial of service via local access.

CVSS Base Score: 3.2 Low

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

CVEID: CVE-2018-12216

Description: Insufficient input validation in Kernel Mode Driver in Intel(R) Graphics Driver for Windows* before versions 10.18.x.5059 (aka 15.33.x.5059), 10.18.x.5057 (aka 15.36.x.5057), 20.19.x.5063 (aka 15.40.x.5063) 21.20.x.5064 (aka 15.45.x.5064) and 24.20.100.6373 potentially enables a privileged user to execute arbitrary code via local access via local access.

CVSS Base Score: 8.2 High

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

CVEID: CVE-2018-12217

Description: Insufficient access control in Kernel Mode Driver in Intel(R) Graphics Driver for Windows* before versions 10.18.x.5059 (aka 15.33.x.5059), 10.18.x.5057 (aka 15.36.x.5057), 20.19.x.5063 (aka 15.40.x.5063) 21.20.x.5064 (aka 15.45.x.5064) and 24.20.100.6373 potentially enables a privileged user to read device configuration information via local access.

CVSS Base Score: 2.3 Low

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

CVEID: CVE-2018-12218

Description: Unhandled exception in User Mode Driver in Intel(R) Graphics Driver for Windows* before versions 10.18.x.5059 (aka 15.33.x.5059), 10.18.x.5057 (aka 15.36.x.5057), 20.19.x.5063 (aka 15.40.x.5063) 21.20.x.5064 (aka 15.45.x.5064) and 24.20.100.6373 potentially enables an unprivileged user to cause a memory leak via local access.

CVSS Base Score: 3.3 Low

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

CVEID: CVE-2018-12219

Description: Insufficient input validation in Kernel Mode Driver in Intel(R) Graphics Driver for Windows* before versions 10.18.x.5059 (aka 15.33.x.5059), 10.18.x.5057 (aka 15.36.x.5057), 20.19.x.5063 (aka 15.40.x.5063) 21.20.x.5064 (aka 15.45.x.5064) and 24.20.100.6373 potentially enables an unprivileged user to read memory via local access via local access.

CVSS Base Score: 5.5 Medium

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

CVEID: CVE-2018-12220

Description: Logic bug in Kernel Mode Driver in Intel(R) Graphics Driver for Windows* before versions before versions 10.18.x.5059 (aka 15.33.x.5059), 10.18.x.5057 (aka 15.36.x.5057), 20.19.x.5063 (aka 15.40.x.5063) 21.20.x.5064 (aka 15.45.x.5064) and 24.20.100.6373 potentially enables a privileged user to execute arbitrary code via local access.

CVSS Base Score: 3.9 Low

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

CVEID: CVE-2018-12221

Description: Insufficient input validation in Kernel Mode Driver in Intel(R) Graphics Driver for Windows* before versions 10.18.x.5059 (aka 15.33.x.5059), 10.18.x.5057 (aka 15.36.x.5057), 20.19.x.5063 (aka 15.40.x.5063) 21.20.x.5064 (aka 15.45.x.5064) and 24.20.100.6373 potentially enables an unprivileged user to cause an integer overflow via local access.

CVSS Base Score: 3.3 Low

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

CVEID: CVE-2018-12222

Description: Insufficient input validation in Kernel Mode Driver in Intel(R) Graphics Driver for Windows* before versions 10.18.x.5059 (aka 15.33.x.5059), 10.18.x.5057 (aka 15.36.x.5057), 20.19.x.5063 (aka 15.40.x.5063) 21.20.x.5064 (aka 15.45.x.5064) and 24.20.100.6373 potentially enables an unprivileged user to cause an out of bound memory read via local access.

CVSS Base Score: 3.3 Low

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

CVEID: CVE-2018-12223

Description: Insufficient access control in User Mode Driver in Intel(R) Graphics Driver for Windows* before versions 10.18.x.5059 (aka 15.33.x.5059), 10.18.x.5057 (aka 15.36.x.5057), 20.19.x.5063 (aka 15.40.x.5063) 21.20.x.5064 (aka 15.45.x.5064) and 24.20.100.6373 potentially enables an unprivileged user to escape from a virtual machine guest-to-host via local access.

CVSS Base Score: 5.3 Medium

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

CVEID: CVE-2018-12224

Description: Buffer leakage in igdkm64.sys in Intel(R) Graphics Driver for Windows* before versions 10.18.x.5059 (aka 15.33.x.5059), 10.18.x.5057 (aka 15.36.x.5057), 20.19.x.5063 (aka 15.40.x.5063) 21.20.x.5064 (aka 15.45.x.5064) and 24.20.100.6373 may allow an authenticated user to potentially enable information disclosure via local access.

CVSS Base Score: 3.3 Low

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

CVEID: CVE-2018-18089

Description: Multiple out of bounds read in igdkm64.sys in Intel(R) Graphics Driver for Windows* before versions 10.18.x.5059 (aka 15.33.x.5059), 10.18.x.5057 (aka 15.36.x.5057), 20.19.x.5063 (aka 15.40.x.5063) 21.20.x.5064 (aka 15.45.x.5064) and 24.20.100.6373 may allow an authenticated user to potentially enable information disclosure via local access.

CVSS Base Score: 3.8 Low

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

CVEID: CVE-2018-18090

Description: Out of bounds read in igdkm64.sys in Intel(R) Graphics Driver for Windows* before versions 10.18.x.5059 (aka 15.33.x.5059), 10.18.x.5057 (aka 15.36.x.5057), 20.19.x.5063 (aka 15.40.x.5063) 21.20.x.5064 (aka 15.45.x.5064) and 24.20.100.6373 may allow an authenticated user to potentially enable denial of service via local access.

CVSS Base Score: 3.2 Low

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

CVEID: CVE-2018-18091

Description: Use after free in Kernel Mode Driver in Intel(R) Graphics Driver for Windows* before versions 10.18.x.5059 (aka 15.33.x.5059), 10.18.x.5057 (aka 15.36.x.5057), 20.19.x.5063 (aka 15.40.x.5063) 21.20.x.5064 (aka 15.45.x.5064) and 24.20.100.6373 may allow an unprivileged user to potentially enable a denial of service via local access.

CVSS Base Score: 5.9

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

Affected Products:

Intel® Graphics Driver for Windows* before versions 10.18.x.5059 (aka 15.33.x.5059), 10.18.x.5057 (aka 15.36.x.5057), 20.19.x.5063 (aka 15.40.x.5063) 21.20.x.5064 (aka 15.45.x.5064) and 24.20.100.6373

Recommendations:

Intel recommends that users of Intel® Graphics Driver for Windows* update to versions 10.18.x.5059 (aka 15.33.x.5059), 10.18.x.5057 (aka 15.36.x.5057), 20.19.x.5063 (aka 15.40.x.5063) 21.20.x.5064 (aka 15.45.x.5064) and 24.20.100.6373 or later.

Updates are available for download at this location:
https://downloadcenter.intel.com/product/80939/Graphics-Drivers

Acknowledgements:

Intel would like to thank @j00sean (CVE-2018-18091) for reporting this issue and working with us on coordinated disclosure.

CVE-2018-12218, CVE-2018-12219, CVE-2018-12220, CVE-2018-12221, CVE-2018-12222, CVE-2018-12223, CVE-2018-12224, CVE-2018-18089 and CVE-2018-18090 were found externally by an Intel partner.

The remaining issues were found internally by Intel employees. Intel we 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 deployed.

Revision History

Revision	Date	Description
1.0	03/12/2019	Initial Release
1.1	03/20/2019	Acknowledgement Correction

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.

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 .

USA (English)

Company Information

Our Commitment

Communities

Investor Relations

Contact Us

Newsroom

Jobs

Terms of Use

*Trademarks

Privacy

Cookies

Supply Chain Transparency

Site Map