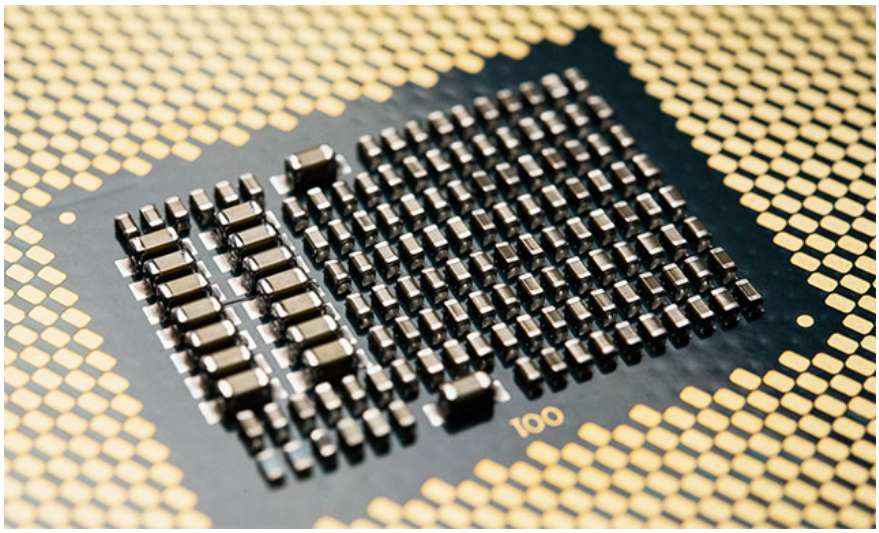
Intel has overcome serious vulnerabilities in graphics drivers for Windows

Intel recently announced that it has successfully overcome 20 security vulnerabilities in Intel Graphics Driver for Windows.

Intel recently announced that it has successfully overcome 20 security vulnerabilities in Intel Graphics Driver for Windows, resulting in escalation of system privileges, denial of service or Disclosure of information if exploited by an attacker with access to the targeted system.

According to QSR security recommendations released two days ago, Intel has released several updates for Windows graphics drivers, designed to minimize the many vulnerabilities found by security researchers from Genuine and worldwide.



1. Intel CVAT, a handy open source data annotation toolkit

Of the 20 vulnerabilities found on Intel Graphics Driver for Windows, two were rated to contain extremely high levels of risk with CVSS Base Scores of 7.3 and 8.2, allowing attackers to execute local code. optionally after escalating possession of privileges on the victim's system.

An attacker requires local access to exploit the Intel Graphics Driver vulnerability

To be more precise, security issues, even if strictly monitored, such as CVE-2018-12214 and CVE-2018-12216, can still lead to local user privileges after a set error. Remember the potential as well as the lack of input authentication of the Kernel Mode (Kernel Mode Drive) driver.

The remaining 18 vulnerabilities are all considered low and medium security risks, and have been patched by Intel. More specifically, all of these vulnerabilities can be exploited through local attack vectors with complexity in the way deployments are not so significant, and also without the need for human interaction. use. Of course, among them, there are still some flaws that need user interaction: CVE-2018- 18090 and CVE-2018-18091, they need this factor to activate the DoS status.

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-2018-12216

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

1. Intel and Qualcomm show off the hardware prototype that allows the integration of 5G into computers

As detailed in the security recommendation, "Intel recommends Intel Graphics Driver for Windows users to update to version 10.18.x.5059 (also called 15.33.x.5059), 10.18.x. 5057 (also called 15.36.x.5057), 20.19.x.5063 (also called 15.40.x.5063) 21.20.x.5064 (also called 15.45.x.5064) and 24.20.100.6373 or more ".

The product is affected

Versions affected by vulnerabilities include Intel Graphics Driver for Windows before versions 10.18.x.5059 (also called 15.33.x.5059), 10.18.x.5057 (also called 15.36.x.5057).), 20.19.x.5063 (also called 15.40.x.5063) 21.20. x.5064 (also called 15.45.x.5064) and 24.20.100.6373.

All Intel Graphics Driver for Windows security updates are available for download from the Intel Drivers & Software Download Center page.

1. Intel officially introduced the Ice 10nm CPU, promising to be available on PCs shipped later this year

In addition, Intel also said it discovered two high-risk vulnerabilities (CVE-2019-0135 and CVE-2019-0121) on the Intel Matrix Storage Manager and the management. Intel Accelerated Storage Manager (Intel Accelerated Storage Manager) in RSTe software can allow escalation to possess system privileges.

In addition, two other medium severity software bugs (CVE-2019-0122 and CVE-2019-0129) were also found, affecting Intel software protection extension tool (Intel Software Guard Extensions - SGX) SDK and Intel USB 3.0 Creator Utility, which can in turn lead to denial of service, theft of information and system privileges.

You finished reading the article "**Intel has overcome serious vulnerabilities in graphics drivers for Windows** " edited by the **TipsMake** team. We hope this article has provided you with many useful tech tips and tricks. You can search for similar articles on tips and guides. Thank you for reading and for following us regularly.

© 2019 TipsMake.com