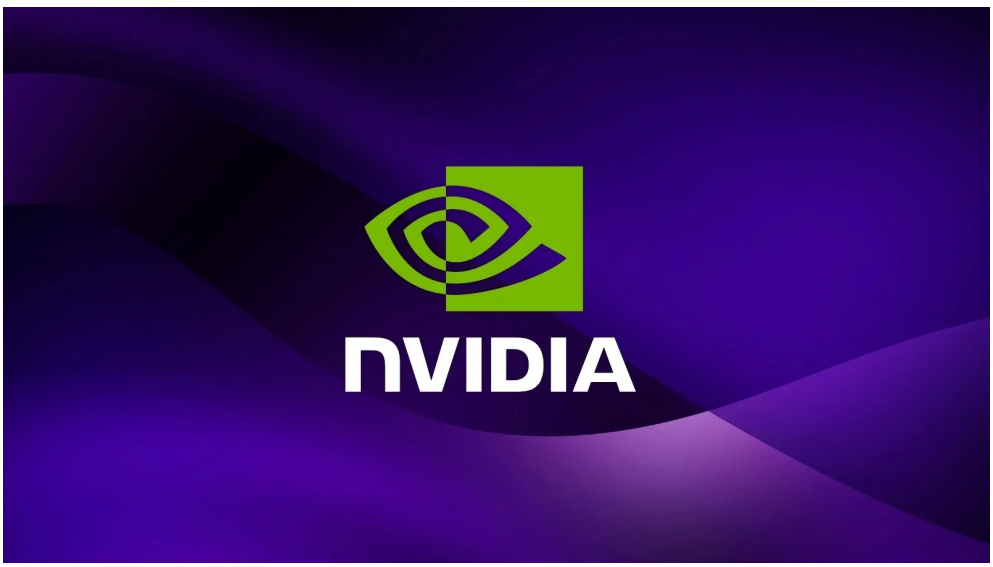
NVIDIA fixes ten vulnerabilities in Windows GPU display drivers

By **Bill Toulas (https://www.bleepingcomputer.com/author/bill-toulas/)**

May 17, 2022 03:12 PM **0**



NVIDIA has released a security update for a wide range of graphics card models, addressing four high-severity and six medium-severity vulnerabilities in its GPU drivers.

The security update fixes vulnerabilities that can lead to denial of service, information disclosure, elevation of privileges, code execution, etc.

The updates have been made available for Tesla, RTX/Quadro, NVS, Studio, and GeForce software products, covering driver branches R450, R470, and R510.

Driver Branch	CVE IDs Addressed
R510	CVE-2022-28181, CVE-2022-28182, CVE-2022-28183, CVE-2022-28184, CVE-2022-28185, CVE-2022-28186, CVE-2022-28187, CVE-2022-28188, CVE-2022-28189, CVE-2022-28190
R470	CVE-2022-28181, CVE-2022-28182, CVE-2022-28183, CVE-2022-28184, CVE-2022-28185, CVE-2022-28186, CVE-2022-28188, CVE-2022-28189
R450	CVE-2022-28181, CVE-2022-28182, CVE-2022-28185, CVE-2022-28186, CVE-2022-28188, CVE-2022-28189

CVEs fixed for each driver branch *(NVIDIA)*

Interestingly, apart from the current and recent product lines that are actively supported, NVIDIA's latest release also covers GTX 600 and GTX 700 Kepler-series cards, whose support ended in October 2021.

The GPU maker previously promised (https://nvidia.custhelp.com/app/answers/detail/a_id/5202) to continue providing critical security updates for these products until September 2024, and this driver update honors that promise.

The four high-severity flaws fixed this month are:

- **CVE-2022-28181** (CVSS v3 score: 8.5) - Out-of-bounds write in the kernel mode layer caused by a specially crafted shader sent over the network, potentially leading to code execution, denial of service, escalation of privileges, information disclosure, and data tampering.
- **CVE-2022-28182** (CVSS v3 score: 8.5) – Flaw in DirectX11 user mode driver allowing an unauthorized attacker to send a specially crafted shared over the network and cause denial of service, escalation of privileges, information disclosure, and data tampering.
- **CVE-2022-28183** (CVSS v3 score: 7.7) - Vulnerability in the kernel mode layer, where an unprivileged regular user can cause an out-of-bounds read, which may lead to denial of service and information disclosure.
- **CVE-2022-28184** (CVSS v3 score: 7.1) - Vulnerability in the kernel mode layer (nvlddmkm.sys) handler for DxgkDdiEscape, where a regular

> unprivileged user can access administrator-privileged registers, which may lead to denial of service, information disclosure, and data tampering.

These vulnerabilities require low privileges and no user interaction, so they could be incorporated into malware, allowing attackers to execute commands with higher privileges.

The first two are exploitable over the network, while the other two are exploited with local access, which could still be helpful for a malware infecting a system with low privileges.

Cisco Talos, which discovered CVE-2022-28181 and CVE-2022-28182, has also published a post today (https://blog.talosintelligence.com/2022/05/vuln-spotlight-nvidia-driver-memory.html) detailing how they triggered the memory corruption flaws by supplying a malformed compute shader.

As threat actors can use a malicious shader in the browser by WebAssembly and WebGL, Talos warns that threat actors may be able to trigger this remotely.

> "A specially-crafted executable/shader file can lead to memory corruption. This vulnerability potentially could be triggered from guest machines running virtualization environments (i.e. VMware, qemu, VirtualBox etc.) in order to perform guest-to-host escape. Theoretically this vulnerability could be also triggered from web browser using webGL and webassembly," explains Talos (https://talosintelligence.com/vulnerability_reports/TALOS-2021-1435) regarding CVE-2022-28181.

For more details on all of the fixes and every software and hardware product covered this month, check out NVIDIA's security bulletin (https://nvidia.custhelp.com/app/answers/detail/a_id/5353).

All users are advised to apply the released security updates as soon as possible. Users can download the latest driver for their GPU model from NVIDIA’s download central (https://www.nvidia.com/Download/index.aspx) section, where they can select the specific product and OS they are using.

The updates can also be applied through NVIDIA's GeForce Experience suite.

However, if you don't specifically need the software to save gaming profiles or use its streaming features, we recommend against using it as it introduces unnecessary security risks and the use of resources.

Related Articles:

NVIDIA has open-sourced its Linux GPU kernel drivers (https://www.bleepingcomputer.com/news/linux/nvidia-has-open-sourced-its-linux-gpu-kernel-drivers/)

Google fixes actively exploited Android kernel vulnerability (https://www.bleepingcomputer.com/news/security/google-fixes-actively-exploited-android-kernel-vulnerability/)

Public interest in Log4Shell fades but attack surface remains (https://www.bleepingcomputer.com/news/security/public-interest-in-log4shell-fades-but-attack-surface-remains/)

CISA adds 7 vulnerabilities to list of bugs exploited in attacks (https://www.bleepingcomputer.com/news/security/cisa-adds-7-vulnerabilities-to-list-of-bugs-exploited-in-attacks/)

Lenovo UEFI firmware driver bugs affect over 100 laptop models (https://www.bleepingcomputer.com/news/security/lenovo-uefi-firmware-driver-bugs-affect-over-100-laptop-models/)

DRIVER (HTTPS://WWW.BLEEPINGCOMPUTER.COM/TAG/DRIVER/)

GPU (HTTPS://WWW.BLEEPINGCOMPUTER.COM/TAG/GPU/)

NVIDIA (HTTPS://WWW.BLEEPINGCOMPUTER.COM/TAG/NVIDIA/)

SECURITY (HTTPS://WWW.BLEEPINGCOMPUTER.COM/TAG/SECURITY/)

VULNERABILITY (HTTPS://WWW.BLEEPINGCOMPUTER.COM/TAG/VULNERABILITY/)

WINDOWS (HTTPS://WWW.BLEEPINGCOMPUTER.COM/TAG/WINDOWS/)