Security Advisory 2022-083

Critical Vulnerabilities in NVIDIA GPU Display Driver

December 1, 2022 — v1.0

TLP:CLEAR

History:

- *01/12/2022 — v1.0 – Initial publication*

Summary

On November 28, NVIDIA released a software security update for its GPU display driver for Windows, containing a fix for a high-severity flaw that threat actors can exploit to perform, among other things, code execution and privilege escalation [1].

Technical Details

The most critical vulnerabilities are:

- **CVE-2022-34669** (CVSS v3.1: 8.8) – Locally exploited user mode flaw in the Windows GPU driver allowing an unprivileged regular user to access or modify files critical to the application, potentially leading to code execution, privilege escalation, information disclosure, data tampering, and denial of service;
- **CVE-2022-34671** (CVSS v3.1: 8.5) – Remotely exploited user mode flaw in the Windows GPU driver allowing an unprivileged regular user to cause an out-of-bounds write, potentially leading to code execution, privilege escalation, information disclosure, data tampering, and denial of service.

Affected Products

NVIDIA announced in its Security Bulletin [2] all affected driver versions.

Recommendations

CERT-EU recommends to check NVIDIA's Security Bulletin and apply the released security updates [2].

References

[1] https://www.bleepingcomputer.com/news/security/nvidia-releases-gpu-driver-update-to-fix-29-security-flaws/

[2] https://nvidia.custhelp.com/app/answers/detail/a_id/5415