Severity

Medium

Analysis Summary

CVE-2022-28190; CVSS:5.5 NVIDIA GPU Display Driver for Windows is vulnerable to a denial of service, caused by improper input validation in the kernel mode layer (nvlddmkm.sys) handler for DxgkDdiEscape. By sending a specially-crafted request, a local authenticated attacker could exploit this vulnerability to cause a denial of service.

CVE-2022-28189 CVSS:5.5 NVIDIA GPU Display Driver for Windows is vulnerable to a denial of service, caused by a NULL pointer dereference in the kernel mode layer (nvlddmkm.sys) handler for DxgkDdiEscape. By sending a specially-crafted request, a local authenticated attacker could exploit this vulnerability to cause a denial of service.

CVE-2022-28188 CVSS:5.5 NVIDIA GPU Display Driver for Windows is vulnerable to a denial of service, caused by improper input validation in the kernel mode layer (nvlddmkm.sys) handler for DxgkDdiEscape. By sending a specially-crafted request, a local authenticated attacker could exploit this vulnerability to cause a denial of service.

CVE-2022-28187 CVSS:5.5 NVIDIA GPU Display Driver for Windows is vulnerable to a denial of service, caused by a flaw in the kernel mode layer (nvlddmkm.sys) handler for DxgkDdiEscape. By sending a specially-crafted request, a local authenticated attacker could exploit this vulnerability to cause a denial of service.

CVE-2022-28186 CVSS:5.5 NVIDIA GPU Display Driver for Windows is vulnerable to a denial of service, caused by a flaw in the kernel mode layer (nvlddmkm.sys) handler for DxgkDdiEscape. By sending a specially-crafted request, a local authenticated attacker could exploit this vulnerability to cause a denial of service.

CVE-2022-28185 CVSS:6.8 NVIDIA GPU Display Driver for Windows and Linux is vulnerable to a denial of service, caused by an out-of-bounds write in the ECC layer. By sending a specially-crafted request, a local attacker could exploit this vulnerability to cause denial of service and data tampering.

CVE-2022-28184 CVSS:7.8 NVIDIA GPU Display Driver for Windows and Linux is vulnerable to a denial of service, caused by a flaw in the kernel mode layer (nvlddmkm.sys) handler for DxgkDdiEscape. By sending a specially-crafted request, a local authenticated attacker could exploit this vulnerability to cause denial of service, information disclosure, and data tampering.

CVE-2022-28183 CVSS:7.7 NVIDIA GPU Display Driver for Windows and Linux is vulnerable to a denial of service, caused by an out-of-bounds read in the kernel mode layer. By sending a specially-crafted request, a local attacker could exploit this vulnerability to cause denial of service and information disclosure.

CVE-2022-28182 CVSS:8.5 NVIDIA GPU Display Driver for Windows could allow a remote authenticated attacker to gain elevated privileges on the system, caused by an out-of-bounds write in DirectX11 user mode driver (nvwgf2um/x.dll). By sending a specially-crafted shader, an attacker could exploit this vulnerability to cause denial of service, escalation of privileges, information disclosure, and data tampering.

CVE-2022-28181 CVSS:8.5 NVIDIA GPU Display Driver for Windows and Linux could allow a remote authenticated attacker to gain elevated privileges on the system, caused by an out-of-bounds write in DirectX11 user mode driver (nvwgf2um/x.dll). By sending a specially-crafted shader, an attacker could exploit this vulnerability to cause denial of service, escalation of privileges, information disclosure, and data tampering.

Impact

- Denial of Service
- Privilege Escalation

Indicators Of Compromise

CVE

- CVE-2022-28190

- CVE-2022-28189
- CVE-2022-28188
- CVE-2022-28187
- CVE-2022-28186
- CVE-2022-28185
- CVE-2022-28184
- CVE-2022-28183
- CVE-2022-28182
- CVE-2022-28181

Affected Vendors

- NVIDIA

Affected Products

- NVIDIA GPU Display Driver for Windows
- NVIDIA GPU Display Driver for Linux

Remediation

Refer to NVIDIA Security Advisory for patch, upgrade or suggested workaround information. NVIDIA Security Advisory