مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Security Updates-NVIDIA GPU Display Drivers and vGPU Software

Tracking #:432318994

Date:19-05-2026

THE INFORMATION CONTAINED WITHIN IS THE PROPERTY OF THE CYBER SECURITY COUNCIL OF THE UNITED ARAB EMIRATES GOVERNMENT AND IS TO BE USED EXCLUSIVELY FOR INTELLGIENCE PURPOSES. IT MAY NOT BE USED IN ANY LEGAL OR PUBLIC MATTER WITHOUT THE EXPLICIT APPROVAL OF THE CYBER SECURITY COUNCIL

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed NVIDIA Product Security has released security updates addressing multiple high and medium-severity vulnerabilities affecting NVIDIA GPU Display Drivers, vGPU Software, and Cloud Gaming components across Windows and Linux platforms.

TECHNICAL DETAILS:

NVIDIA Product Security has released security updates addressing multiple high and medium-severity vulnerabilities affecting NVIDIA GPU Display Drivers, vGPU Software, and Cloud Gaming components across Windows and Linux platforms.
The vulnerabilities impact a broad range of NVIDIA products, including GeForce, NVIDIA RTX, Quadro, NVS, Tesla, and enterprise virtualization environments.

High Severity Vulnerability Details:

- CVE-2026-24187 | CVSS 8.8 | High
  Use-after-free vulnerability in Linux Display Driver allowing possible privilege escalation and code execution.
- CVE-2026-24190 | CVSS 7.8 | High
  Improper GPU resource access in Windows/Linux kernel mode layer leading to code execution and data tampering.
- CVE-2026-24191 | CVSS 7.8 | High
  TOCTOU race condition vulnerability in Windows Display Driver enabling privilege escalation and code execution.
- CVE-2026-24192 | CVSS 7.8 | High
  Heap buffer overflow in Linux Display Driver caused by incorrect numeric conversion.
- CVE-2026-24193 | CVSS 7.8 | High
  Out-of-bounds write vulnerability in Windows/Linux drivers that may allow code execution.
- CVE-2026-24194 | CVSS 7.1 | High
  Improper input validation flaw in Linux UVM component causing denial of service.
- CVE-2026-24195 | CVSS 7.1 | High
  Input validation issue in Linux UVM component leading to denial of service.
- CVE-2026-24196 | CVSS 7.1 | High
  Out-of-bounds read vulnerability in Linux Display Driver causing information disclosure.
- CVE-2026-24200 | CVSS 7.0 | High
  Use-after-free vulnerability in vGPU Manager potentially enabling code execution.

Affected Products

The vulnerabilities affect multiple NVIDIA software branches and platforms, including:

- NVIDIA GPU Display Driver for Windows
- NVIDIA GPU Display Driver for Linux
- NVIDIA vGPU Software
- NVIDIA Cloud Gaming Software
- Virtual GPU Manager Components

Affected hardware families include:

- NVIDIA GeForce GPUs
- NVIDIA RTX Series
- Quadro

- NVS
- Tesla GPUs

Affected driver branches include:

- R595
- R590
- R580
- R570
- R535

Affected virtualization platforms include:

- VMware vSphere
- XenServer
- Red Hat Enterprise Linux KVM
- Ubuntu KVM
- Azure Local
- Windows Server

RECOMMENDATIONS:

Immediate Actions

- Update all affected NVIDIA GPU Display Drivers immediately
- Apply latest vGPU Manager and guest driver patches

Kindly circulate this information to your subsidiaries and partners as well as share with us any relevant information and findings.

The UAE Cyber Security Council extends its appreciation for the continued collaboration.

REFERENCES:

- https://nvidia.custhelp.com/app/answers/detail/a_id/5821