



مجلس الأمن السيبراني
CYBER SECURITY COUNCIL



Security Updates - NVIDIA
Tracking #:432317141
Date:28-04-2025

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 INTELLIGENCE 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 that NVIDIA has released security updates to address multiple vulnerabilities in its products.

TECHNICAL DETAILS:

NVIDIA has released security updates addressing multiple critical vulnerabilities affecting NVIDIA GPU Display Drivers and vGPU software for Linux and Windows platforms. These vulnerabilities may allow local attackers to escalate privileges, execute arbitrary code, cause denial of service, or access sensitive resources.

Vulnerability Details:

1. CVE-2025-23244 (High Severity, CVSS 7.8)

- **Description:** Local attackers can escalate privileges, execute code, cause denial of service, disclose information, or tamper with data via a flaw in the Linux GPU Display Driver.
- **Impact:** Code execution, privilege escalation, denial of service, information disclosure, data tampering

2. CVE-2025-23245 (Medium Severity, CVSS 5.5)

- **Description:** vGPU Manager allows a guest to access global resources, potentially causing denial of service.
- **Impact:** Denial of service

3. CVE-2025-23246 (Medium Severity, CVSS 5.5)

- **Description:** vGPU Manager allows a guest to consume uncontrolled resources, potentially causing denial of service.
- **Impact:** Denial of service

Affected Products:

- **NVIDIA GPU Display Driver (Linux):**
GeForce, RTX, Quadro, NVS, Tesla (Driver branches: R535, R550, R570, R575)
- **NVIDIA vGPU Software (Windows & Linux):**
Virtual GPU Manager (Citrix Hypervisor, VMware vSphere, RHEL KVM, Ubuntu, Microsoft Azure Local, Windows Server)
- **NVIDIA Cloud Gaming (Linux):**
Guest driver and Virtual GPU Manager

Note: Refer to the NVIDIA Security Bulletin for affected versions, fixed versions, and more information.

RECOMMENDATIONS:

The UAE Cyber Security Council recommends updating the affected versions to the fixed or latest versions released by NVIDIA.

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/5630