



Technical Bulletin

Bulletin No.: ALT20260810005

Date Issued: 2026-08-10

NVIDIA Multi-Instance GPU (MIG) Security Announcement (CVE-2026-24197)

Overview:

NVIDIA released a security announcement in May 2026 regarding a security vulnerability in **Multi-Instance GPU (MIG)** partition management in the **NVIDIA Linux GPU Display Driver**.

The vulnerability is related to the insecure default initialization of **memory subsystem routing resources** during MIG partition reconfiguration, which may lead to data corruption or GPU hang, further causing a denial-of-service (DoS).

This issue affects systems using the **NVIDIA Linux GPU Display Driver** and **NVIDIA vGPU Software / Virtual GPU Manager**, particularly Linux environments with **MIG enabled**.

Potential Impact:

The vulnerability may result in:

- Data corruption
- GPU hang
- Denial-of-Service (DoS)

Resolution:

NVIDIA has provided patch information in the security announcement and recommends that users update to the patched driver version listed in the announcement **as soon as possible**.

Required Action:

For systems with **MIG enabled**, users are recommended to perform the following actions:

1. Update the **NVIDIA Linux GPU Display Driver** or **NVIDIA vGPU Software / Virtual GPU Manager** to the patched driver version listed in the official NVIDIA security announcement.
2. Restrict **MIG management privileges** to system administrators to prevent unauthorized users from performing reconfiguration operations.
3. After updating, verify the currently loaded driver version using:

nvidia-smi

Compare the loaded driver version with the version listed in the official NVIDIA security announcement.

References

NVIDIA GPU Display Drivers Security Bulletin – May 2026

Bulletin ID: 5821

CVE: CVE-2026-24197

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

Support

If you require assistance with the driver update or have questions regarding this security announcement, please contact:

Altos Technical Support

AltosCare.Taiwan@altoscomputing.com