مجلس الأمن السيبراني
CYBER SECURITY COUNCIL

United Arab Emirates

Security Bulletin – NVIDIA

Tracking #:432317411

Date:25-06-2025

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed that NVIDIA has released security update for NVIDIA Megatron LM to address multiple high-severity vulnerabilities. These vulnerabilities could enable attackers to execute arbitrary code, escalate privileges, access sensitive information, and tamper with data.

TECHNICAL DETAILS:

Vulnerability Details:

- **CVE-2025-23264, CVE-2025-23265**
  - **Base Score:** 7.8
  - **Severity:** High
  - **Description:** NVIDIA Megatron-LM for all platforms contains a vulnerability in a python component where an attacker may cause a code injection issue by providing a malicious file.
  - **Impact:** A successful exploit of this vulnerability may lead to Code Execution, Escalation of Privileges, Information Disclosure and Data Tampering.

Platform/OS:

- All platforms

Affected Versions:

- All versions prior to 0.12.0

Fixed Versions:

- 0.12.1

RECOMMENDATIONS:

The UAE Cyber Security Council recommends applying the security updates recently 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/5663