مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Security Updates - NVIDIA

Tracking #:432317109

Date:23-04-2025

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed that NVIDIA has released a security update for its NeMo Framework to address three significant vulnerabilities. These vulnerabilities, if exploited, could lead to remote code execution, data tampering, and potential breaches of system integrity.

TECHNICAL DETAILS:

Vulnerabilities Details:

- **CVE-2025-23249:** A deserialization of untrusted data vulnerability could allow remote code execution. This issue may result in unauthorized code execution and data tampering.
- **CVE-2025-23250:** An improper limitation of pathname to a restricted directory could enable arbitrary file writing. This vulnerability may lead to unauthorized code execution and data tampering.
- **CVE-2025-23251:** An improper control of the generation of code could result in remote code execution. Successful exploitation may lead to unauthorized code execution and data tampering.

All three vulnerabilities are rated as "High" severity with a CVSS v3.1 base score of 7.6.

Affected Platforms:

- Windows, Linux, macOS

Affected Versions:

- NVIDIA NeMo Framework prior to 25.02

Fixed Versions:

- NVIDIA NeMo Framework version 25.02 or later

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/5641