مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Security Updates - NVIDIA

Tracking #:432317645

Date:27-08-2025

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 to address multiple vulnerabilities in its NeMo Curator and NeMo Framework products across all platforms (Windows, Linux, macOS). Successful exploitation of these vulnerabilities could allow code execution, privilege escalation, information disclosure, and data tampering.

Vulnerabilities Details

1. CVE-2025-23307 – NVIDIA NeMo Curator

- CVSS Base Score: 7.8 (High)
- Description: A vulnerability exists in NeMo Curator where a malicious file created by an attacker could allow code injection.
- Impact: Code execution, privilege escalation, information disclosure, data tampering.
- Affected Products: NVIDIA NeMo Curator (Windows, Linux, macOS)
- Affected Versions: All versions prior to Curator 25.07
- Fixed Version: Curator 25.07

2. CVE-2025-23312, CVE-2025-23313, CVE-2025-23314, CVE-2025-23315 – NVIDIA NeMo Framework

- CVSS Base Score: 7.8 (High)
- Description: Multiple vulnerabilities in NeMo Framework components (retrieval services, NLP, export and deploy) allow attackers to inject malicious code via crafted data.
- Impact: Code execution, privilege escalation, information disclosure, data tampering.
- Affected Products: NVIDIA NeMo Framework (Windows, Linux, macOS)
- Affected Versions: All versions prior to 2.4.0
- Fixed Version: 2.4.0

RECOMMENDATIONS:

The UAE Cyber Security Council recommends applying the fixed or latest updates released by the 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/5690
- https://nvidia.custhelp.com/app/answers/detail/a_id/5689