مجلس الأمن السيبراني
CYBER SECURITY COUNCIL

United Arab Emirates

Security Updates - NVIDIA

Tracking #:432318417

Date:18-02-2026

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 INTELLGIENCE PURPOSES. IT MAY NOT BE USED IN ANY LEGAL OR PUBLIC MATTER WITHOUT THE EXPLICIT APPROVAL OF THE CYBER SECURITY COUNCIL

TLP: WHITE

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 for the NeMo Framework and Megatron Bridge. These updates address multiple high-severity vulnerabilities that could allow remote code execution, code injection, privilege escalation, information disclosure, denial of service, and data tampering.

Vulnerability Details
NeMo Framework

- **CVE-2025-33245:** Malicious data could trigger remote code execution, privilege escalation, information disclosure, and data tampering. (CWE-502)
- **CVE-2025-33236:** Attacker-crafted data could cause code injection leading to code execution, privilege escalation, information disclosure, and data tampering. (CWE-94)
- **CVE-2025-33241 & CVE-2025-33243:** Malicious files or distributed environment attacks can lead to remote code execution with full system impact. (CWE-502)
- **CVE-2025-33246 & CVE-2025-33249:** Command injection vulnerabilities in ASR Evaluator and voice preprocessing scripts could allow code execution, privilege escalation, data tampering, and information disclosure. (CWE-77)
- **CVE-2025-33250, CVE-2025-33251, CVE-2025-33252, CVE-2025-33253:** Remote code execution vulnerabilities triggered by malicious files or user interaction may result in code execution, denial of service, information disclosure, and data tampering. (CWE-94 / CWE-502)

Affected Product: NVIDIA NeMo Framework (all platforms)
Fixed Version: 2.6.1 or later

Megatron Bridge

- **CVE-2025-33239:** Malicious input in the data merging tutorial could cause code injection, potentially leading to code execution, privilege escalation, information disclosure, and data tampering. (CWE-94)
- **CVE-2025-33240:** Malicious input in the data shuffling tutorial could cause code injection with the same impacts. (CWE-94)

Affected Product: NVIDIA Megatron Bridge (all platforms)
Fixed Version: 0.2.2 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/5762
- https://nvidia.custhelp.com/app/answers/detail/a_id/5781