



مجلس الأمن السيبراني
CYBER SECURITY COUNCIL



Security Updates-NVIDIA NeMo Framework
Tracking #:432319144
Date:16-06-2026

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

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed NVIDIA has released security updates for the NVIDIA NeMo Framework addressing three high-severity vulnerabilities.

TECHNICAL DETAILS:

NVIDIA has released security updates for the NVIDIA NeMo Framework addressing three high-severity vulnerabilities that could allow authenticated attackers to execute arbitrary code, escalate privileges, disclose sensitive information, and tamper with data.

Vulnerability Details:

1. CVE-2026-24155 — High — Code Injection
 - CVSS Score: 7.8
 - CVSS Vector: AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H
 - CWE: CWE-94 (Code Injection)
 - Description: NVIDIA NeMo Framework contains a code injection vulnerability.
 - An attacker with low privileges may inject and execute malicious code within the application context.
2. CVE-2026-24252 — High — OS Command Injection
 - CVSS Score: 7.8
 - CVSS Vector: AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H
 - CWE: CWE-78 (OS Command Injection)
 - Description: NVIDIA NeMo for Linux contains an operating system command injection vulnerability.
 - Improper handling of user-controlled input may allow execution of unintended operating system commands.
3. CVE-2026-24228 — High — Deserialization of Untrusted Data
 - CVSS Score: 7.8
 - CVSS Vector: AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H
 - CWE: CWE-502 (Deserialization of Untrusted Data)
 - Description: NVIDIA NeMo Framework for Linux improperly handles serialized data from untrusted sources.
 - Maliciously crafted serialized objects may trigger unintended code execution during deserialization.

Fixed Version:

- NVIDIA NeMo Framework 2.7.3 or later

RECOMMENDATIONS:

Immediate Actions:

- Upgrade NVIDIA NeMo Framework to fixed version or later.

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/5839