مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

# Security Updates - NVIDIA TensorRT LLM

Tracking #:432317147

Date:30-04-2025



TLP: WHITE

## EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed that NVIDIA has released a security update for its TensorRT-LLM Framework addressing a high-severity vulnerability (CVE-2025-23245) in the Python executor component.

## TECHNICAL DETAILS:

NVIDIA has released a security update for its TensorRT-LLM Framework addressing a high-severity vulnerability (CVE-2025-23245) in the Python executor component.

**Vulnerability Details:**

- CVE ID-CVE-2025-23245
- Description-Insecure deserialization in Python executor used for socket-based IPC. Allows local attackers to execute arbitrary code, leak sensitive data, or tamper with system state.
- Severity-High
- CVSS v3.1-8.8 (AV:L/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H)
- CWE-CWE-502: Deserialization of Untrusted Data
- Impact-Code Execution, Information Disclosure, Data Tampering
- Affected Versions-All TensorRT-LLM versions prior to 0.18.2
- Fixed Version-0.18.2

## RECOMMENDATIONS:

The UAE Cyber Security Council recommends to upgrade TensorRT-LLM to the fixed or latest versions at the earliest.

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/5648