مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Critical Vulnerabilities in NVIDIA Triton Inference Server

Tracking #:432317715

Date:16-09-2025

TLP: WHITE

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed that NVIDIA has released security updates for the Triton Inference Server to address multiple critical and high-severity vulnerabilities impacting deployments on Windows and Linux platforms.

TECHNICAL DETAILS:

NVIDIA has released security updates for the Triton Inference Server to address multiple critical and high-severity vulnerabilities impacting deployments on Windows and Linux platforms. Exploitation of these flaws could enable threat actors to compromise AI inference workloads, steal or alter sensitive data, and disrupt machine learning services. Administrators are strongly advised to immediately upgrade to Triton Inference Server version 25.08 (or 25.07 for DALI backend) and review deployment security configurations.

CVE ID	CVSS v3.1 Score	Severity	Description	Impact
CVE-2025-23316	9.8	Critical	Python backend vulnerability where an attacker can manipulate the model name parameter in model control APIs.	Remote code execution, denial of service, information disclosure, data tampering
CVE-2025-23268	8.0	High	Improper input validation issue in the DALI backend.	Code execution
CVE-2025-23328	7.5	High	Out-of-bounds write triggered through specially crafted input.	Denial of service
CVE-2025-23329	7.5	High	Memory corruption by accessing shared memory region in Python backend.	Denial of service
CVE-2025-23336	4.4	Medium	Denial of service caused by loading a misconfigured model.	Denial of service

Affected Products & Fixed Versions:

Affected Product	Platform / Component	Affected Versions	Fixed Version
Triton Inference Server	Windows, Linux	All versions prior to 25.08	25.08
Triton Inference Server (DALI Backend)	DALI Backend	All versions prior to 25.07	25.07

RECOMMENDATIONS:

The UAE Cyber Security Council recommends to immediately upgrade Triton Inference Server to fixed version or latest version.

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/5691