مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Security Updates - NVIDIA

Tracking #:432317565

Date:05-08-2025

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed that NVIDIA has released security updates to address multiple vulnerabilities in its Triton Inference Server.

TECHNICAL DETAILS:

NVIDIA has addressed multiple vulnerabilities in its Triton Inference Server. These flaws could allow attackers to execute arbitrary code, cause denial of service, perform data tampering, and trigger information disclosure, posing a serious threat to system integrity and confidentiality.

Vulnerability Details (including but not limited to):

CVE ID	Description	Base Score	Severity	Impacts
CVE-2025-23310	NVIDIA Triton Inference Server for Windows and Linux contains a vulnerability where an attacker could cause stack buffer overflow by specially crafted inputs.	9.8	Critical	Code execution, denial of service, information disclosure, data tampering
CVE-2025-23311	NVIDIA Triton Inference Server contains a vulnerability where an attacker could cause a stack overflow through specially crafted HTTP requests.	9.8	Critical	Code execution, denial of service, information disclosure, data tampering
CVE-2025-23317	NVIDIA Triton Inference Server contains a vulnerability in the HTTP server, where an attacker could start a reverse shell by sending a specially crafted HTTP request.	9.1	Critical	Code execution, denial of service, data tampering, information disclosure

Affected/Fixed Versions: Refer Security Bulletin: NVIDIA Triton Inference Server - August 2025

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/5687