مجلس الأمن السيبراني

CYBER SECURITY COUNCIL

United Arab Emirates

Security Updates - NVIDIA

Tracking #:432318090

Date:03-12-2025

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 to address multiple high-severity vulnerabilities impacting NVIDIA TAO and NVIDIA Triton Inference Server products. These vulnerabilities could allow attackers to perform actions such as privilege escalation, data tampering, information disclosure, or denial of service.

Vulnerability Details

1. **CVE-2025-33208 – NVIDIA TAO**
    - **CVSS Base Score:** 8.8
    - **Severity:** High
    - **Description:** NVIDIA TAO contains an uncontrolled search path vulnerability that may allow an attacker to load malicious resources.
    - **Impact:** Escalation of privileges, information disclosure, data tampering, denial of service
2. **CVE-2025-33211 – NVIDIA Triton Server for Linux**
    - **CVSS Base Score:** 7.5
    - **Severity:** High
    - **Description:** NVIDIA Triton Server contains an improper validation vulnerability related to input quantity, potentially allowing denial of service.
    - **Impact:** Denial of service
3. **CVE-2025-33201 – NVIDIA Triton Inference Server**
    - **CVSS Base Score:** 7.5
    - **Severity:** High
    - **Description:** An improper check for exceptional conditions may allow an attacker to trigger denial of service by submitting extremely large payloads.
    - **Impact:** Denial of service

Affected Products	Platform or OS	Affected Versions	Fixed Versions
NVIDIA TAO	Ubuntu LTS	6.25.7	6.25.9
Triton Inference Server	Linux	All versions prior to r25.10	r25.10

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/5730
- https://nvidia.custhelp.com/app/answers/detail/a_id/5734