مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

# Multiple Vulnerabilities in NVIDIA NVTabular

Tracking #:432319069

Date:05-06-2026



**TLP: WHITE**

## EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed high-severity vulnerabilities in NVIDIA NVTabular. These vulnerabilities could enable authenticated local attackers to execute arbitrary code, manipulate data, disclose sensitive information, or trigger denial-of-service conditions.

## TECHNICAL DETAILS:

**Vulnerability Details**

- **CVE-2026-24237**
  - **Severity:** High | **CVSS:** 7.8
  - A vulnerability in NVIDIA NVTabular exists due to improper deserialization of untrusted data. A successful attacker could exploit this flaw to execute arbitrary code, tamper with data, access sensitive information, or cause denial of service.
- **CVE-2026-24221**
  - **Severity:** High | **CVSS:** 7.8
  - NVIDIA NVTabular contains an improper deserialization vulnerability that may allow attackers with local access and low privileges to execute malicious code, alter data, disclose sensitive information, or disrupt system availability.

**Affected Products and Versions**

- NVIDIA NVTabular | Platform / OS: All
- All versions from 0.0 to 5dd11f4

**Fixed Versions**

- 08e0633 or later

## RECOMMENDATIONS:

The UAE Cyber Security Council recommends applying the mitigation or workaround provided 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/5851