



مجلس الأمن السيبراني
CYBER SECURITY COUNCIL



Security Updates - NVIDIA

Tracking #:432318838

Date:24-04-2026

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 INTELLIGENCE PURPOSES. IT MAY NOT BE USED IN ANY LEGAL OR PUBLIC MATTER WITHOUT THE EXPLICIT APPROVAL OF THE CYBER SECURITY COUNCIL

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed that NVIDIA has released security updates to address multiple vulnerabilities in CUDA-Q and KAI Scheduler. These vulnerabilities could allow attackers to perform denial-of-service (DoS) attacks, access sensitive information, or manipulate data.

TECHNICAL DETAILS:

Vulnerability Details

High Severity Vulnerabilities

- **CVE-2026-24189 – Out-of-Bounds Read in NVIDIA CUDA-Q**
A vulnerability exists in a CUDA-Q endpoint where an unauthenticated attacker can trigger an out-of-bounds read via a specially crafted request. Successful exploitation may result in denial of service and potential information disclosure.
- **CVE-2026-24177 – Unauthorized API Access in NVIDIA KAI Scheduler**
Improper access control in KAI Scheduler allows attackers to access API endpoints without proper authorization, potentially leading to exposure of sensitive information.

Medium Severity Vulnerabilities

- **CVE-2026-24176 – Improper Authorization in NVIDIA KAI Scheduler**
This vulnerability allows improper authorization through cross-namespace pod references, which may enable attackers to tamper with data.

Affected Products

- **NVIDIA CUDA-Q**
 - Affected Versions: All versions prior to **0.14.0**
 - Platform: All
- **NVIDIA KAI Scheduler**
 - Affected Versions: All versions prior to **0.13.0**
 - Platform: Linux

Fixed Versions

- **CUDA-Q:** Upgrade to **version 0.14.0 or later**
- **KAI Scheduler:** Upgrade to **version 0.13.0 or later**

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/5820
- https://nvidia.custhelp.com/app/answers/detail/a_id/5818