مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

# Security Updates-NVIDIA

Tracking #:432316873

Date:17-02-2025



TLP: WHITE

## EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed NVIDIA has released security updates to address a high severity vulnerability in NVIDIA Container Toolkit.

## TECHNICAL DETAILS:

NVIDIA has released security updates to address a high severity vulnerability in NVIDIA Container Toolkit.

**Vulnerability Details:**

1. **CVE-2025-23359- 8.3** High
    - NVIDIA Container Toolkit for Linux contains a Time-of-Check Time-of-Use (TOCTOU) vulnerability when used with default configuration, where a crafted container image could gain access to the host file system.
    - A successful exploit of this vulnerability might lead to code execution, denial of service, escalation of privileges, information disclosure, and data tampering.
    - **Affected Versions:**
        - NVIDIA Container Toolkit-Linux-All versions up to and including 1.17.3
        - NVIDIA GPU Operator-Linux-All versions up to and including 24.9.1
    - **Fixed Versions:**
        - NVIDIA Container Toolkit- 1.17.4
        - NVIDIA GPU Operator 24.9.2

## RECOMMENDATIONS:

The UAE Cyber Security Council recommends to update 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/5616