مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Security Updates - NVIDIA

Tracking #:432316757

Date:17-01-2025

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed that NVIDIA has released security updates to address multiple vulnerabilities in the NVIDIA Container Toolkit and NVIDIA GPU Operator.

TECHNICAL DETAILS:

Vulnerability Details:

- **CVE-2024-0135**
  - A high-severity improper isolation vulnerability that could lead to code execution, denial of service, escalation of privileges, information disclosure, and data tampering.
- **CVE-2024-0136**
  - A high-severity improper isolation vulnerability present in non-default configurations, potentially resulting in code execution, denial of service, escalation of privileges, information disclosure, and data tampering.
- **CVE-2024-0137**
  - A medium-severity improper isolation vulnerability in non-default configurations that could lead to denial of service and escalation of privileges

Affected Products	Platform or OS	Affected Versions	Fixed Version
NVIDIA Container Toolkit	Linux	All versions up to and including v1.17.0	v1.17.1
NVIDIA GPU Operator	Linux	All versions up to and including 24.9.0	24.9.1

Note: Refer to the NVIDIA Security Bulletin for additional mitigation details and further information.

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/5599