

مجلس الأمن السيبراني
CYBER SECURITY COUNCIL



Security Updates - NVIDIA

Tracking #:432317667

Date:03-09-2025

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 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 its products.

TECHNICAL DETAILS:

NVIDIA has released security updates addressing multiple vulnerabilities in NVIDIA BlueField, ConnectX, DOCA, Mellanox DPDK, Cumulus Linux, and NVOS. Successful exploitation of these vulnerabilities may result in escalation of privileges, information disclosure, denial of service (DoS), or data tampering.

High-Severity Vulnerabilities:

- **CVE-2025-23256**
NVIDIA BlueField contains a vulnerability in the management interface, where an attacker with local access could cause incorrect authorization to modify configuration.
- **CVE-2025-23257**
NVIDIA DOCA (collectx-clxapidev Debian package) contains a privilege escalation vulnerability.
- **CVE-2025-23258**
NVIDIA DOCA (collectx-dpeserver Debian package for arm64) contains a privilege escalation vulnerability.

Medium-Severity Vulnerabilities:

- **CVE-2025-23259**
NVIDIA Mellanox DPDK contains a vulnerability in Poll Mode Driver (PMD), where an attacker on a VM might cause information disclosure and denial of service.
- **CVE-2025-23262**
NVIDIA ConnectX contains a vulnerability in the management interface that could allow unauthorized configuration modification.
- **CVE-2025-23261**
NVIDIA Cumulus Linux and NVOS products contain a vulnerability where hashed user passwords are not properly suppressed in log files.

Affected Products and Fixed Versions:

- **NVIDIA DOCA**
 - collectx-clxapidev: Fixed in 2.9.3, 3.0.0
 - collectx-dpeserver (arm64): Fixed in 2.5.4, 2.9.3, 3.0.0
- **NVIDIA BlueField**
 - GA: Fixed in 45.1020
 - LTS22: Fixed in 35.4554
 - LTS23: Fixed in 39.5050
 - LTS24: Fixed in 43.3608
- **NVIDIA ConnectX**
 - GA: Fixed in 45.1020
 - LTS22: Fixed in 35.4554
 - LTS23: Fixed in 39.5050
 - LTS24: Fixed in 43.3608
 - ConnectX-4: Fix pending (12.28.4704, to be published by end of September)

- ConnectX-4 LX: Fix pending (14.32.1908, to be published by end of September)
- **Mellanox DPDK**
 - Fixed in 22.11_2504.1.0, 22.11_2410.4.0 LTS, 22.11_2310.6.0 LTS, 20.11.7.9.0, 25.07, 24.11.3 LTS, 23.11.5 LTS, 22.11.10 LTS
- **NVOS / Cumulus Linux**
 - NVOS: Fixed in 25.02.42xx, 25.02.4xxx
 - Cumulus Linux: Fixed in 5.13, 5.11.0.0026, 5.11.1.1009, 5.9.2.0020, 5.9.0.0032

RECOMMENDATIONS:

The UAE Cyber Security Council recommends applying the fixed or latest updates released by the 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/5655