مجلس الأمن السيبراني

CYBER SECURITY COUNCIL

United Arab Emirates

Security Updates - NVIDIA

Tracking #:432317491

Date:16-07-2025

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 INTELLGIENCE 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 released security updates addressing several vulnerabilities, including one critical flaw. The vulnerabilities could allow attackers to execute arbitrary code, escalate privileges, or cause denial of service, potentially compromising system integrity and data security.

TECHNICAL DETAILS:

The vulnerabilities allow attackers to execute arbitrary code, escalate privileges, or cause denial of service by exploiting flaws in NVIDIA's software components. Successful exploitation may require specific configurations, such as enabling the VGT+ feature in certain network environments. These issues pose significant risks to system integrity, especially in high-performance computing or enterprise setups.

Vulnerability Details:

CVE ID	Description	Base Score	Severity	Impacts
CVE-2025-23266	NVIDIA Container Toolkit for all platforms contains a vulnerability in some hooks used to initialize the container, where an attacker could execute arbitrary code with elevated permissions. A successful exploit of this vulnerability might lead to escalation of privileges, data tampering, information disclosure, and denial of service.	9.0	Critical	Escalation of privileges, data tampering, information disclosure, denial of service
CVE-2025-23263	NVIDIA DOCA-Host and Mellanox OFED contain a vulnerability in the VGT+ feature, where an attacker on a VM might cause escalation of privileges and denial of service on the VLAN.	7.6	High	Escalation of privileges, denial of service
CVE-2025-23267	NVIDIA Container Toolkit for all platforms contains a vulnerability in the update-ldcache hook, where an attacker could cause a link following by using a specially crafted container image. A successful exploit of this vulnerability	8.5	High	Data tampering, denial of service

CVE ID	Description	Base Score	Severity	Impacts
	might lead to data tampering and denial of service.			
CVE-2025-23263	NVIDIA DOCA-Host and Mellanox OFED contain a vulnerability in the VGT+ feature, where an attacker on a VM might cause escalation of privileges and denial of service on the VLAN.	7.6	High	Escalation of privileges, denial of service
CVE-2025-23270	NVIDIA Jetson Linux contains a vulnerability in UEFI Management mode, where an unprivileged local attacker may cause exposure of sensitive information via a side channel vulnerability. A successful exploit of this vulnerability might lead to code execution, data tampering, denial of service, and information disclosure	7.1	High	Code execution, data tampering, denial of service, information disclosure
CVE-2025-23269	NVIDIA Jetson Linux contains a vulnerability in the kernel where an attacker may cause an exposure of sensitive information due to a shared microarchitectural predictor state that influences transient execution. A successful exploit of this vulnerability may lead to information disclosure.	4.7	Medium	Information disclosure

Affected/Fixed Versions:

CVE IDs Addressed	Affected Products	Platform or OS	Affected Versions	Updated Version
CVE-2025-23263	NVIDIA DOCA-Host	Linux	All versions prior to 2.5.3-0.1.2	2.5.3-0.1.2
			All versions prior to 2.9.2-0.1.6	2.9.2-0.1.6

CVE IDs Addressed	Affected Products	Platform or OS	Affected Versions	Updated Version
			All versions prior to 3.0.0-058001	3.0.0-058001
CVE-2025-23263	Mellanox OFED	Linux	All versions prior to 5.8-6.0.5.0	5.8-6.0.5.0
			All versions prior to 23.10-4.1.1.0	23.10-4.1.1.0
			All versions prior to 24.10-2.1.9.0	24.10-2.1.9.0
CVE-2025-23266	NVIDIA Container Toolkit	All	All versions up to and including 1.17.7 (CDI mode only for versions prior to 1.17.5)	1.17.8
CVE-2025-23267	NVIDIA GPU Operator	Linux	All versions up to and including 25.3.0 (CDI mode only for versions prior to 25.3.0)	25.3.1
CVE-2025-23269 CVE-2025-23270	NVIDIA Jetson Orin Series	Jetson Linux	All versions prior to JP5.x: 35.6.2 All versions prior to JP6.x: 36.4.4	35.6.2 36.4.4
	NVIDIA Xavier Series	Jetson Linux	All versions prior to JP5.x: 35.6.2	35.6.2
CVE-2025-23270	IGX Orin	IGX OS	All versions prior to IGX 1.1.2	IGX 1.1.2

NOTE: Refer to NVIDIA security bulletins for mitigation steps for each vulnerability.

RECOMMENDATIONS:

The UAE Cyber Security Council recommends applying the latest updates released by NVIDIA at the earliest.

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/5654
- https://nvidia.custhelp.com/app/answers/detail/a_id/5659
- https://nvidia.custhelp.com/app/answers/detail/a_id/5662