مجلس الأمن السيبراني

CYBER SECURITY COUNCIL

United Arab Emirates

Security Updates - NVIDIA

Tracking #:432318290

Date:22-01-2026

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 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 has released security updates to address multiple vulnerabilities in its products.

TECHNICAL DETAILS:

NVIDIA has released security updates addressing multiple high- and medium-severity vulnerabilities affecting NVIDIA CUDA Toolkit and NVIDIA Merlin (Transformers4Rec). Exploitation of these vulnerabilities could allow attackers to achieve arbitrary code execution, privilege escalation, data tampering, denial of service, and information disclosure.

Vulnerability Details
NVIDIA CUDA Toolkit

- **CVE-2025-33228 – High Severity (CVSS 7.3)**
  A command injection vulnerability in NVIDIA Nsight Systems exists within the gfx_hotspot recipe. When the script is manually invoked with a malicious input, an attacker could execute arbitrary OS commands, leading to code execution, privilege escalation, data tampering, denial of service, and information disclosure.
- **CVE-2025-33229 – High Severity (CVSS 7.3)**
  NVIDIA Nsight Visual Studio Edition for Windows contains a vulnerability in the Nsight Monitor component that allows execution of arbitrary code with the same privileges as the monitor application. Successful exploitation may result in privilege escalation, data tampering, denial of service, and information disclosure.
- **CVE-2025-33230 – High Severity (CVSS 7.3)**
  A command injection vulnerability exists in the NVIDIA Nsight Systems Linux .run installer. By supplying a malicious installation path, an attacker could execute arbitrary commands, potentially leading to elevated privileges and system compromise.
- **CVE-2025-33231 – Medium Severity (CVSS 6.7)**
  NVIDIA Nsight Systems for Windows contains an insecure DLL search path vulnerability. An attacker could exploit this weakness to load a malicious DLL, resulting in code execution, privilege escalation, data tampering, denial of service, and information disclosure.

NVIDIA Merlin (Transformers4Rec)

- **CVE-2025-33233 – High Severity (CVSS 7.8)**
  NVIDIA Merlin Transformers4Rec contains a code injection vulnerability that could allow an attacker to execute arbitrary code. A successful exploit may lead to privilege escalation, data tampering, and information disclosure.

Affected Products
NVIDIA CUDA Toolkit

- **Platforms:** Windows, Linux
- **Affected Versions:** All versions up to **CUDA Toolkit 13.1**

NVIDIA Merlin (Transformers4Rec)

- **Platform:** Linux
- **Affected Versions:** All versions that do **not** include commit 27ddd49

Fixed Versions

- **NVIDIA CUDA Toolkit: 13.1 or later**
- **NVIDIA Merlin (Transformers4Rec):** Any code branch that includes commit 27ddd49

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/5755
- https://nvidia.custhelp.com/app/answers/detail/a_id/5761