مجلس الأمن السيبراني

CYBER SECURITY COUNCIL

United Arab Emirates

Security Updates - NVIDIA

Tracking #:432318073

Date:26-11-2025

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

TECHNICAL DETAILS:

NVIDIA has released security updates for DGX Spark, NeMo Framework, and NeMo Agent Toolkit, addressing multiple vulnerabilities that could allow attackers to execute code, escalate privileges, tamper with data, cause denial of service, or access sensitive information.

Vulnerability Details:
Critical-Severity Vulnerability

- **CVE-2025-33187 (DGX Spark):** A vulnerability in NVIDIA DGX Spark GB10 SROOT allows privileged users to access protected SoC areas, potentially leading to code execution, data disclosure or tampering, DoS, and privilege escalation.

High-Severity Vulnerabilities

- **CVE-2025-33188 (DGX Spark):** Hardware resource tampering; may lead to information disclosure, data tampering, denial of service.
- **CVE-2025-33189 (DGX Spark):** SROOT firmware out-of-bound write; may lead to code execution, data tampering, denial of service, information disclosure, escalation of privileges.
- **CVE-2025-33204 (NeMo Framework):** NLP/LLM code injection; may lead to code execution, escalation of privileges, information disclosure, data tampering.
- **CVE-2025-33205 (NeMo Framework):** Predefined variable exploitation; may lead to code execution.
- **CVE-2025-33203 (NeMo Agent Toolkit):** SSRF in chat API endpoint; may lead to information disclosure, denial of service.

Medium-Severity Vulnerabilities

- **CVE-2025-33190 (DGX Spark):** SROOT firmware out-of-bound write; may lead to code execution, data tampering, denial of service, escalation of privileges.
- **CVE-2025-33191 (DGX Spark):** OSROOT firmware invalid memory read; may lead to denial of service.
- **CVE-2025-33192 (DGX Spark):** SROOT arbitrary memory read; may lead to code execution, information disclosure, denial of service.
- **CVE-2025-33193 (DGX Spark):** SROOT improper integrity validation; may lead to code execution, information disclosure, denial of service.
- **CVE-2025-33194 (DGX Spark):** SROOT improper input processing; may lead to information disclosure, denial of service.
- **CVE-2025-33195 (DGX Spark):** SROOT unexpected memory buffer operations; may lead to data tampering, denial of service, escalation of privileges.
- **CVE-2025-33196 (DGX Spark):** SROOT resource reuse; may lead to information disclosure.
- **CVE-2025-33197 (DGX Spark):** SROOT NULL pointer dereference; may lead to code execution, denial of service.

Low-Severity Vulnerabilities

- **CVE-2025-33198 (DGX Spark):** SROOT resource reuse; may lead to information disclosure.
- **CVE-2025-33199 (DGX Spark):** SROOT incorrect control flow; may lead to data tampering.
- **CVE-2025-33200 (DGX Spark):** SROOT resource reuse; may lead to information disclosure.

Affected Products and Fixed Versions

- **DGX Spark:** All versions prior to OTA0 → Update to OTA0
- **NeMo Framework:** All versions prior to 2.5.1 → Update to 2.5.1
- **NeMo Agent Toolkit:** All versions prior to 1.3.0 → Update to 1.3.0

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/5720
- https://nvidia.custhelp.com/app/answers/detail/a_id/5729
- https://nvidia.custhelp.com/app/answers/detail/a_id/5726