مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Multiple Vulnerabilities in NVIDIA NemoClaw

Tracking #:432318888

Date:04-05-2026

TLP: WHITE

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed that NVIDIA has released security updates for NVIDIA NemoClaw to address multiple vulnerabilities that could allow information disclosure through prompt injection and server-side request forgery (SSRF).

TECHNICAL DETAILS:

Vulnerability Details

- **CVE-2026-24222**
  - **Severity:** High | **CVSS:** 8.6
    NVIDIA NemoClaw contains an improper access control vulnerability in the sandbox environment initialization component. A remote attacker can send prompt-injected content that causes the agent to read and exfiltrate host environment variables that were not properly restricted during sandbox creation, resulting in information disclosure.
- **CVE-2026-24231**
  - **Severity:** Medium | **CVSS:** 5.9
    NVIDIA NemoClaw contains a server-side request forgery (SSRF) vulnerability in the validateEndpointUrl() component. An attacker can supply a crafted endpoint URL targeting the 0.0.0.0/8 address range through a blueprint configuration file or CLI flag, potentially leading to unauthorized information disclosure.

Affected Products

- NVIDIA NemoClaw (All Platforms / Operating Systems)
  - All versions prior to v0.0.18
  - All versions prior to v0.0.13

Fixed Versions

- v0.0.18 or later
- v0.0.13 or later

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/5837