10 years CERT-EU

Security Advisory 2024-104

Critical Vulnerability in NVIDIA Container Toolkit

September 27, 2024 — v1.0

TLP:CLEAR

History:

- *27/09/2024 — v1.0 – Initial publication*

Summary

On September 26, 2024, a security advisory was issued regarding a critical vulnerability, **CCVE-2024-0132**, affecting NVIDIA Container Toolkit. NVIDIA Container Toolkit is providing containerised AI applications with access to GPU resources. This vulnerability impacts any AI application that is running the vulnerable container toolkit to enable GPU support.

This vulnerability could allow a rogue user or software to escape their containers and ultimately take complete control of the underlying host [1].

Technical details

The vulnerability **CCVE-2024-0132** has a CVSS score of 9.0 out of 10. It is a Time-of-Check/Time-of-Use (TOC/TOU) vulnerability, a type of race condition.

A successful exploit of this vulnerability may lead to code execution, denial of service, escalation of privileges, information disclosure, and data tampering [2].

Affected products

- NVIDIA Container Toolkit: All versions up to and including v1.16.1
- NVIDIA GPU Operator: All versions up to and including 24.6.1

Recommendations

CERT-EU strongly recommends affected organisations to upgrade to the latest version of Container Toolkit (v1.16.2) and NVIDIA GPU Operator (v24.6.2)[1].

References

[1] https://nvidia.custhelp.com/app/answers/detail/a_id/5582

[2] https://www.wiz.io/blog/wiz-research-critical-nvidia-ai-vulnerability