



AUTORITETI KOMBËTAR PËR SIGURINË KIBERNETIKE

Përditësimet e Sigurisë - NVIDIA

Data: 18/02/2026
Version: 1.0

Përmbajtja

Përmbledhje Ekzekutive	2
Informacione Teknike	2
Rekomandime	3

Përmbledhje Ekzekutive

NVIDIA ka publikuar përditësime sigurie për të adresuar dobësi të shumta në produktin e saj.

Informacione Teknike

NVIDIA ka publikuar përditësime sigurie për NeMo Framework dhe Megatron Bridge. Këto përditësime adresojnë shumë dobësi me ashpërsi të lartë që mund të lejojnë ekzekutimin e kodit në distancë, injektimin e kodit, përshkallëzimin e privilegjeve, zbulimin e informacionit, mohimin e shërbimit dhe manipulimin e të dhënave.

Detajet e dobësive:

NeMo Framework

- CVE-2025-33245: Të dhënat keqdashëse mund të shkaktojnë ekzekutimin e kodit në distancë, përshkallëzimin e privilegjeve, zbulimin e informacionit dhe manipulimin e të dhënave. (CWE-502)
- CVE-2025-33236: Të dhënat e krijuara nga sulmuesi mund të shkaktojnë injektimin e kodit që çon në ekzekutimin e kodit, përshkallëzimin e privilegjeve, zbulimin e informacionit dhe manipulimin e të dhënave. (CWE-94)
- CVE-2025-33241 dhe CVE-2025-33243: Skedarët keqdashës ose sulmet në mjedisin e shpërndarë mund të çojnë në ekzekutimin e kodit në distancë me ndikim të plotë në sistem. (CWE-502)
- CVE-2025-33246 dhe CVE-2025-33249: Dobësitë e injektimit të komandës në ASR Evaluator dhe skriptet e përpunimit paraprak të zërit mund të lejojnë ekzekutimin e kodit, përshkallëzimin e privilegjeve, manipulimin e të dhënave dhe zbulimin e informacionit. (CWE-77)
- CVE-2025-33250, CVE-2025-33251, CVE-2025-33252, CVE-2025-33253: Dobësitë e ekzekutimit të kodit në distancë të shkaktuara nga skedarë keqdashës ose ndërveprimi i përdoruesit mund të rezultojnë në ekzekutimin e kodit, mohimin e shërbimit, zbulimin e informacionit dhe manipulimin e të dhënave. (CWE-94 / CWE 502)

Produkti i prekur: NVIDIA NeMo Framework (të gjitha platformat)

Versioni i rregulluar: 2.6.1 ose më i ri

Megatron Bridge

- CVE-2025-33239: Futja keqdashëse në tutorialin e bashkimit të të dhënave mund të shkaktojë injektimin e kodit, duke çuar potencialisht në ekzekutimin e kodit, përshkallëzimin e privilegjeve, zbulimin e informacionit dhe manipulimin e të dhënave. (CWE-94)
- CVE-2025-33240: Futja keqdashëse në tutorialin e përzierjes së të dhënave mund të shkaktojë injektimin e kodit me të njëjtat ndikime. (CWE-94)

Produkti i prekur: NVIDIA Megatron Bridge (të gjitha platformat)
Versioni i rregulluar: 0.2.2 ose më i ri

Rekomandime

AKSK rekomandon përditësimin e versioneve të prekura në versionet e rregulluara ose më të fundit të publikuar nga NVIDIA