Security Bulletin: NVIDIA Triton Inference Server - April 2026

Updated 04/13/2026 05:45 PM

NVIDIA has released a software update for NVIDIA® Triton Inference Server.

To protect your system, clone or update this software to Triton Server r26.02 or later from the NVIDIA Triton Inference Server GitHub repo.

Go to NVIDIA Product Security.

Details

The following table summarizes the potential vulnerabilities that this security update addresses and their impact. Descriptions use CWE™, and base scores and vectors use CVSS v3.1 standards.

CVE ID	Description	Vector	CVSS Score	Severity	CWE	Impacts
CVE-2026-24146	NVIDIA Triton Inference Server contains a vulnerability where insufficient input validation and a large number of outputs could cause a server crash. A successful exploit of this vulnerability might lead to denial of service.	AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H	7.5	High	CWE-789	Denial of service
CVE-2026-24173	NVIDIA Triton Inference Server contains a vulnerability where an attacker could cause a server crash by sending a malformed request to the server. A successful exploit of this vulnerability might lead to denial of service.	AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H	7.5	High	CWE-190	Denial of service
CVE-2026-24174	NVIDIA Triton Inference Server contains a vulnerability where an attacker could cause a server crash by sending a malformed request to the server. A successful exploit of this vulnerability might lead to denial of service.	AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H	7.5	High	CWE-681	Denial of service
CVE-2026-24175	NVIDIA Triton Inference Server contains a vulnerability where an attacker could cause a server crash by sending a malformed request header to the server. A successful exploit of this vulnerability might lead to denial of service.	AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H	7.5	High	CWE-248	Denial of service
CVE-2026-24147	NVIDIA Triton Inference Server contains a vulnerability in triton server where an attacker may cause an information disclosure by uploading a model configuration. A successful exploit of this vulnerability may lead to information disclosure or denial of service.	AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:N/A:L	4.8	Medium	CWE-22	Denial of service, information disclosure

The NVIDIA risk assessment is based on an average of risk across a diverse set of installed systems and may not represent the true risk to your local installation. NVIDIA recommends evaluating the risk to your specific configuration.

SECURITY UPDATES

The following table lists the NVIDIA products affected, versions affected, and the version that includes this security update.

CVE IDs Addressed	Affected Products	Platform or OS	Affected Versions	Updated
CVE-2026-24146 CVE-2026-24173	Triton Inference Server	All	All versions prior to r26.02	r26.02

CVE IDs Addressed	Affected Products	Platform or OS	Affected Versions	Updated Version
CVE-2026-24174 CVE-2026-24175 CVE-2026-24147				

MITIGATIONS

Refer to Security Updates for the updated versions to install.

ACKNOWLEDGEMENTS

NVIDIA thanks the following for reporting these issues:
CVE-2026-24146: Sarvesh Patil
CVE-2026-24173: Jaeyoung Lee
CVE-2026-24174: Mahammad Huseynkhanli
CVE-2026-24175: SeaWind (ZSEC Red Team, Zalo)
CVE-2026-24147: Tian Yu from ADLab of VenusTech

GET THE MOST UP-TO-DATE PRODUCT SECURITY INFORMATION

Visit the NVIDIA Product Security page to:

- Subscribe to security bulletin notifications
- See the current list of NVIDIA security bulletins
- Report a potential security issue in any NVIDIA supported product
- Learn more about the vulnerability management process followed by the NVIDIA Product Security Incident Response Team (PSIRT)

REVISION HISTORY

Revision	Date	Description
1.0	April 07, 2026	Initial release

SUPPORT

If you have any questions about this security bulletin, contact NVIDIA Support.