Security Bulletin: NVIDIA KAI Scheduler - April 2026

Updated 04/17/2026 01:29 PM

NVIDIA has released a software update for NVIDIA® KAI Scheduler.

To protect your system, clone or update this software to KAI Scheduler v0.13.0 or later from the KAI-Scheduler 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-2026-24177	NVIDIA KAI Scheduler contains a vulnerability where an attacker could access API endpoints without authorization. A successful exploit of this vulnerability might lead to information disclosure.	AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:N/A:N	7.7	High	CWE-306	Information disclosure
CVE-2026-24176	NVIDIA KAI Scheduler contains a vulnerability where an attacker could cause improper authorization through cross-namespace pod references. A successful exploit of this vulnerability might lead to data tampering.	AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:L/A:N	4.3	Medium	CWE-863	Data tampering

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 updated version that includes this security update.

CVE IDs Addressed	Affected Products	Platform or OS	Affected Versions	Updated Version
CVE-2026-24176 CVE-2026-24177	NVIDIA KAI Scheduler	Linux	All versions prior to 0.13.0	0.13.0

MITIGATIONS

Refer to Security Updates for the updated versions to install.

ACKNOWLEDGEMENTS

NVIDIA thanks the following for reporting these issues:
CVE-2026-24176: Ziyi Guo (Northwestern University)
CVE-2026-24177: Tianze Ding (Tencent Security Xuanwu Lab)

GET THE MOST UP-TO-DATE PRODUCT SECURITY INFORMATION

- See a list of all NVIDIA published security bulletins.
- Report a potential NVIDIA security vulnerability.
- Learn about the NVIDIA Product Security Incident Response Team (PSIRT) and its vulnerability management process.

REVISION HISTORY

Revision	Date	Description
1.0	April 21, 2026	Initial release

SUPPORT

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