



# nvmet: move async event work off nvmet-wq

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF !\[\]\(003082e50e3009141f59bd5df831749f\_img.jpg\)](#)

## Summary

<b>CVE</b>	CVE-2026-31557
<b>State</b>	PUBLISHED
<b>Assigner</b>	Linux
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2026-04-24 15:16:30 UTC
<b>Updated</b>	2026-04-27 20:14:08 UTC

**Description** In the Linux kernel, the following vulnerability has been resolved: nvmet: move async event work off nvmet-wq For target nv

## Risk And Classification

**Primary CVSS:** v3.1 7.5 HIGH from 416baaa9-dc9f-4396-8d5f-8c081fb06d67

**CVSS:** 3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H

**EPSS:** 0.000180000 probability, percentile 0.046080000 (date 2026-04-27)

**Problem Types:** NVD-CWE-noinfo

Version	Source	Type	Score	Severity	Vector
3.1	416baaa9-dc9f-4396-8d5f-8c081fb06d67	Secondary	7.5	HIGH	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H
3.1	CNA	DECLARED	7.5	HIGH	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H

## CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

None

User Interaction

None

Scope

Unchanged

Confidentiality

None

Integrity

None

None

Availability

High

CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Linux	Linux Kernel	All	All	All	All

Vendor Declared Affected Products

Source	Vendor	Product	Version
CNA	Linux	Linux	affected 8832cf922151e9dfa2821736beb0ae2dd3968b6e 49c7c50ee6325a084216e94395e067ecde8088fa gi
CNA	Linux	Linux	affected 8832cf922151e9dfa2821736beb0ae2dd3968b6e ca111c9d8d6c9d5735878d933a1716c4be86c2d1 g
CNA	Linux	Linux	affected 8832cf922151e9dfa2821736beb0ae2dd3968b6e 25ceffc1dabec3b93f458b437aae26f4da293f87 git
CNA	Linux	Linux	affected 8832cf922151e9dfa2821736beb0ae2dd3968b6e 2922e3507f6d5caa7f1d07f145e186fc6f317a4e git
CNA	Linux	Linux	affected d44ff3b100b94e9f23b1e8dbe688eee9bb867ac9 git
CNA	Linux	Linux	affected 84026f8c9357c62a9d3e4c554ffd10ccab813654 git
CNA	Linux	Linux	affected 5.18
CNA	Linux	Linux	unaffected 5.18 semver
CNA	Linux	Linux	unaffected 6.12.80 6.12.* semver
CNA	Linux	Linux	unaffected 6.18.21 6.18.* semver
CNA	Linux	Linux	unaffected 6.19.11 6.19.* semver
CNA	Linux	Linux	unaffected 7.0 * original_commit_for_fix

References

Reference	Source	Link	Tags
git.kernel.org/stable/c/49c7c50ee6325a084216e94395e067ecde8088fa	416baaa9-dc9f-4396-8d5f-8c081fb06d67	<a href="https://git.kernel.org">git.kernel.org</a>	Patch
git.kernel.org/stable/c/2922e3507f6d5caa7f1d07f145e186fc6f317a4e	416baaa9-dc9f-4396-8d5f-8c081fb06d67	<a href="https://git.kernel.org">git.kernel.org</a>	Patch
git.kernel.org/stable/c/ca111c9d8d6c9d5735878d933a1716c4be86c2d1	416baaa9-dc9f-4396-8d5f-8c081fb06d67	<a href="https://git.kernel.org">git.kernel.org</a>	Patch
git.kernel.org/stable/c/25ceffc1dabec3b93f458b437aae26f4da293f87	416baaa9-dc9f-4396-8d5f-8c081fb06d67	<a href="https://git.kernel.org">git.kernel.org</a>	Patch
CVE Program record	CVE.ORG	<a href="https://www.cve.org">www.cve.org</a>	canonic
NVD vulnerability detail	NVD	<a href="https://nvd.nist.gov">nvd.nist.gov</a>	canonic

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.

© [CVE.report](#) 2026 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

**Free CVE JSON API** [cve.report/api](#)

**CVE.report and Source URL Uptime Status** [status.cve.report](#)