



# nvme-pci: Fix slab-out-of-bounds in nvme\_dbbuf\_set

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF](#) 

## Summary

<b>CVE</b>	CVE-2026-43449
<b>State</b>	PUBLISHED
<b>Assigner</b>	Linux
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2026-05-08 15:16:57 UTC
<b>Updated</b>	2026-05-08 15:16:57 UTC

**Description** In the Linux kernel, the following vulnerability has been resolved: nvme-pci: Fix slab-out-of-bounds in nvme\_dbbuf\_set dev-

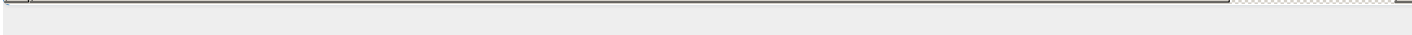
## Risk And Classification

**EPSS:** 0.000240000 probability, percentile 0.070400000 (date 2026-05-10)

## Vendor Declared Affected Products

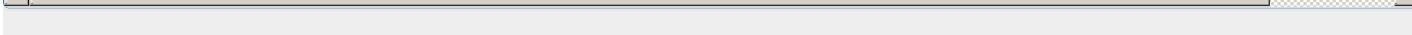
Source	Vendor	Product	Version
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	affected 0f0d2c876c96d4908a9ef40959a44bec21bdd6cf 2b9d605c3f0d3262142f196249cd3bd58c857c71 git
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	affected 0f0d2c876c96d4908a9ef40959a44bec21bdd6cf 86183d550559e45e07059bbdf17331fea469e38c git
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	affected 0f0d2c876c96d4908a9ef40959a44bec21bdd6cf d7990c936e25f484b61a5adeeadc1d290a9fd16e git
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	affected 0f0d2c876c96d4908a9ef40959a44bec21bdd6cf 83e6edd6358326c9c2de31a54bb4a1ec50703f1f git
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	affected 0f0d2c876c96d4908a9ef40959a44bec21bdd6cf 50bad78f03a02d3c0f228edf9912b494d3e7acb9 git
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	affected 0f0d2c876c96d4908a9ef40959a44bec21bdd6cf 328c551f0cc81ee776b186b86cc6e5253bb6fda7 git
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	affected 0f0d2c876c96d4908a9ef40959a44bec21bdd6cf 78279d2d74c58a0ed64e43cf601a02649771182e git
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	affected 0f0d2c876c96d4908a9ef40959a44bec21bdd6cf b4e78f1427c7d6859229ae9616df54e1fc05a516 git
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	affected 930bb3092fe606baa23d57ae59b70b291d67a8af git
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	affected fd1c1de8c4589fdd528733bfd01ed0c5f3f69204 git
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	affected 4940816604e3ce7e05e8df297773ee86c0476d48 git
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	affected 55a3b1ad694631cc2698b5500ac5865d7d0f064e git
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	affected 5.10
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	unaffected 5.10 semver
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	unaffected 5.10.253 5.10.* semver
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	unaffected 5.15.203 5.15.* semver
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	unaffected 6.1.167 6.1.* semver

CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	unaffected 6.6.130 6.6.* semver
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	unaffected 6.12.78 6.12.* semver
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	unaffected 6.18.19 6.18.* semver
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	unaffected 6.19.9 6.19.* semver
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	unaffected 7.0 * original_commit_for_fix



## References

Reference	Source	Link	Tags
<a href="https://git.kernel.org/stable/c/2b9d605c3f0d3262142f196249cd3bd58c857c71">git.kernel.org/stable/c/2b9d605c3f0d3262142f196249cd3bd58c857c71</a>	416baaa9-dc9f-4396-8d5f-8c081fb06d67	<a href="https://git.kernel.org">git.kernel.org</a>	
<a href="https://git.kernel.org/stable/c/b4e78f1427c7d6859229ae9616df54e1fc05a516">git.kernel.org/stable/c/b4e78f1427c7d6859229ae9616df54e1fc05a516</a>	416baaa9-dc9f-4396-8d5f-8c081fb06d67	<a href="https://git.kernel.org">git.kernel.org</a>	
<a href="https://git.kernel.org/stable/c/78279d2d74c58a0ed64e43cf601a02649771182e">git.kernel.org/stable/c/78279d2d74c58a0ed64e43cf601a02649771182e</a>	416baaa9-dc9f-4396-8d5f-8c081fb06d67	<a href="https://git.kernel.org">git.kernel.org</a>	
<a href="https://git.kernel.org/stable/c/328c551f0cc81ee776b186b86cc6e5253bb6fda7">git.kernel.org/stable/c/328c551f0cc81ee776b186b86cc6e5253bb6fda7</a>	416baaa9-dc9f-4396-8d5f-8c081fb06d67	<a href="https://git.kernel.org">git.kernel.org</a>	
<a href="https://git.kernel.org/stable/c/50bad78f03a02d3c0f228edf9912b494d3e7acb9">git.kernel.org/stable/c/50bad78f03a02d3c0f228edf9912b494d3e7acb9</a>	416baaa9-dc9f-4396-8d5f-8c081fb06d67	<a href="https://git.kernel.org">git.kernel.org</a>	
<a href="https://git.kernel.org/stable/c/d7990c936e25f484b61a5adeeadc1d290a9fd16e">git.kernel.org/stable/c/d7990c936e25f484b61a5adeeadc1d290a9fd16e</a>	416baaa9-dc9f-4396-8d5f-8c081fb06d67	<a href="https://git.kernel.org">git.kernel.org</a>	
<a href="https://git.kernel.org/stable/c/86183d550559e45e07059bbdf17331fea469e38c">git.kernel.org/stable/c/86183d550559e45e07059bbdf17331fea469e38c</a>	416baaa9-dc9f-4396-8d5f-8c081fb06d67	<a href="https://git.kernel.org">git.kernel.org</a>	
<a href="https://git.kernel.org/stable/c/83e6edd6358326c9c2de31a54bb4a1ec50703f1f">git.kernel.org/stable/c/83e6edd6358326c9c2de31a54bb4a1ec50703f1f</a>	416baaa9-dc9f-4396-8d5f-8c081fb06d67	<a href="https://git.kernel.org">git.kernel.org</a>	
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](https://cve.report/api)

CVE.report and Source URL Uptime Status [status.cve.report](https://status.cve.report)