



# scsi: storvsc: Fix scheduling while atomic on PREEMPT\_RT

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

## Summary

<b>CVE</b>	CVE-2026-43475
<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 15:17:00 UTC
<b>Updated</b>	2026-05-12 14:10:27 UTC

**Description** In the Linux kernel, the following vulnerability has been resolved: scsi: storvsc: Fix scheduling while atomic on PREEMPT\_RT

## Risk And Classification

**EPSS:** 0.000240000 probability, percentile 0.070210000 (date 2026-05-11)

## Vendor Declared Affected Products

Source	Vendor	Product	Version
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	affected d86adf482b843b3a58a9ec3b7c1ccdbf7c705db1 cf00cb15f2515e38d3b7571bf6800b7c6ce70a84 git
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	affected d86adf482b843b3a58a9ec3b7c1ccdbf7c705db1 b82462af23e45e066dd56d2736ea70159a6ad647 gi
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	affected d86adf482b843b3a58a9ec3b7c1ccdbf7c705db1 91ab59f76d0866079420ebff1c7959fcd87a242e git
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	affected d86adf482b843b3a58a9ec3b7c1ccdbf7c705db1 e7919a293f9b6101e38bde0d8613daea6c9955df git
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	affected d86adf482b843b3a58a9ec3b7c1ccdbf7c705db1 f8db760f4f52a73a022a3d6c84c488ead952a9b5 git
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	affected d86adf482b843b3a58a9ec3b7c1ccdbf7c705db1 c2e73d8acd056347a70047e6be7cd98e0e811dfa git
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	affected d86adf482b843b3a58a9ec3b7c1ccdbf7c705db1 c7984d196476adcbd51c0ce386d7e90277198d57 gi
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	affected d86adf482b843b3a58a9ec3b7c1ccdbf7c705db1 57297736c08233987e5d29ce6584c6ca2a831b12 gi
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	affected 4.11
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	unaffected 4.11 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/f8db760f4f52a73a022a3d6c84c488ead952a9b5">git.kernel.org/stable/c/f8db760f4f52a73a022a3d6c84c488ead952a9b5</a>	416baaa9-dc9f-4396-8d5f-8c081fb06d67	<a href="https://git.kernel.org">git.kernel.org</a>	
<a href="https://git.kernel.org/stable/c/c2e73d8acd056347a70047e6be7cd98e0e811dfa">git.kernel.org/stable/c/c2e73d8acd056347a70047e6be7cd98e0e811dfa</a>	416baaa9-dc9f-4396-8d5f-8c081fb06d67	<a href="https://git.kernel.org">git.kernel.org</a>	
<a href="https://git.kernel.org/stable/c/91ab59f76d0866079420ebff1c7959fcd87a242e">git.kernel.org/stable/c/91ab59f76d0866079420ebff1c7959fcd87a242e</a>	416baaa9-dc9f-4396-8d5f-8c081fb06d67	<a href="https://git.kernel.org">git.kernel.org</a>	
<a href="https://git.kernel.org/stable/c/b82462af23e45e066dd56d2736ea70159a6ad647">git.kernel.org/stable/c/b82462af23e45e066dd56d2736ea70159a6ad647</a>	416baaa9-dc9f-4396-8d5f-8c081fb06d67	<a href="https://git.kernel.org">git.kernel.org</a>	
<a href="https://git.kernel.org/stable/c/e7919a293f9b6101e38bde0d8613daea6c9955df">git.kernel.org/stable/c/e7919a293f9b6101e38bde0d8613daea6c9955df</a>	416baaa9-dc9f-4396-8d5f-8c081fb06d67	<a href="https://git.kernel.org">git.kernel.org</a>	
<a href="https://git.kernel.org/stable/c/c7984d196476adcbd51c0ce386d7e90277198d57">git.kernel.org/stable/c/c7984d196476adcbd51c0ce386d7e90277198d57</a>	416baaa9-dc9f-4396-8d5f-8c081fb06d67	<a href="https://git.kernel.org">git.kernel.org</a>	
<a href="https://git.kernel.org/stable/c/57297736c08233987e5d29ce6584c6ca2a831b12">git.kernel.org/stable/c/57297736c08233987e5d29ce6584c6ca2a831b12</a>	416baaa9-dc9f-4396-8d5f-8c081fb06d67	<a href="https://git.kernel.org">git.kernel.org</a>	
<a href="https://git.kernel.org/stable/c/cf00cb15f2515e38d3b7571bf6800b7c6ce70a84">git.kernel.org/stable/c/cf00cb15f2515e38d3b7571bf6800b7c6ce70a84</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)