



powerpc/smp: Add check for kcalloc() failure in parse_thread_groups()

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

Summary

CVE	CVE-2026-43148
State	PUBLISHED
Assigner	Linux
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-05-06 12:16:32 UTC
Updated	2026-05-06 13:07:51 UTC

Description In the Linux kernel, the following vulnerability has been resolved: powerpc/smp: Add check for kcalloc() failure in parse_thre

Vendor Declared Affected Products

Source	Vendor	Product	Version
CNA	Linux	Linux	affected 790a1662d3a26fe9fa5f691386d8fde6bb8b0dc2 1de31dba19c3cd0c1caf388a286b46df638f0b91 git
CNA	Linux	Linux	affected 790a1662d3a26fe9fa5f691386d8fde6bb8b0dc2 b265e53d9adfb5751713185843f7188aa9dd066 git
CNA	Linux	Linux	affected 790a1662d3a26fe9fa5f691386d8fde6bb8b0dc2 9d0ca11258e7b452653d04310addfec1753de1a2 git
CNA	Linux	Linux	affected 790a1662d3a26fe9fa5f691386d8fde6bb8b0dc2 ca46d2092f307385a7acfb42632056570d6dbbbc git
CNA	Linux	Linux	affected 790a1662d3a26fe9fa5f691386d8fde6bb8b0dc2 9b85c8f624b0f8cf9b932f5a65dadcd56a1f47a72 git
CNA	Linux	Linux	affected 790a1662d3a26fe9fa5f691386d8fde6bb8b0dc2 8b221db0b7d24675e465e98d9326d298025a4e8d git
CNA	Linux	Linux	affected 790a1662d3a26fe9fa5f691386d8fde6bb8b0dc2 33c1c6d8a28a2761ac74b0380b2563cf546c2a3a git
CNA	Linux	Linux	affected 5.11
CNA	Linux	Linux	unaffected 5.11 semver
CNA	Linux	Linux	unaffected 5.15.202 5.15.* semver
CNA	Linux	Linux	unaffected 6.1.165 6.1.* semver
CNA	Linux	Linux	unaffected 6.6.128 6.6.* semver
CNA	Linux	Linux	unaffected 6.12.75 6.12.* semver
CNA	Linux	Linux	unaffected 6.18.16 6.18.* semver
CNA	Linux	Linux	unaffected 6.19.6 6.19.* semver
CNA	Linux	Linux	unaffected 7.0 * original_commit_for_fix

References

Reference	Source	Link	Tags
-----------	--------	------	------

git.kernel.org/stable/c/33c1c6d8a28a2761ac74b0380b2563cf546c2a3a	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	
git.kernel.org/stable/c/9d0ca11258e7b452653d04310addfec1753de1a2	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	
git.kernel.org/stable/c/ca46d2092f307385a7acfb42632056570d6dbbbc	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	
git.kernel.org/stable/c/b265e53d9adffb5751713185843f7188aa9dd066	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	
git.kernel.org/stable/c/9b85c8f624b0f8cf9b932f5a65dacd56a1f47a72	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	
git.kernel.org/stable/c/1de31dba19c3cd0c1caf388a286b46df638f0b91	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	
git.kernel.org/stable/c/8b221db0b7d24675e465e98d9326d298025a4e8d	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	
CVE Program record	CVE.ORG	www.cve.org	canonic
NVD vulnerability detail	NVD	nvd.nist.gov	canonic

No vendor comments have been submitted for this CVE.

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

© [CVE.report](https://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](https://www.mitre.org) and the authoritative source of CVE content is [MITRE's CVE web site](https://www.mitre.org/cve). This site includes MITRE data granted under the following [license](https://www.mitre.org/cve).

Free CVE JSON API cve.report/api

CVE.report and Source URL Uptime Status status.cve.report