



cgroup: fix race between task migration and iteration

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

Summary

CVE	CVE-2026-43439
State	PUBLISHED
Assigner	Linux
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-05-08 15:16:56 UTC
Updated	2026-05-08 15:16:56 UTC

Description In the Linux kernel, the following vulnerability has been resolved: cgroup: fix race between task migration and iteration Whe

Vendor Declared Affected Products

Source	Vendor	Product	Version
CNA	Linux	Linux	affected b636fd38dc40113f853337a7d2a6885ad23b8811 7c85debc35e6d131bd29c64f2ae78c6ede0e55c4 git
CNA	Linux	Linux	affected b636fd38dc40113f853337a7d2a6885ad23b8811 3b95abab7369235a37b15eac6e1a0b443bba7c7 g
CNA	Linux	Linux	affected b636fd38dc40113f853337a7d2a6885ad23b8811 4a9654a2b46cfdaae287fb8995f536245635e467 git
CNA	Linux	Linux	affected b636fd38dc40113f853337a7d2a6885ad23b8811 3dfd1328c05234e8d8fa61948b2ba82680594988 git
CNA	Linux	Linux	affected b636fd38dc40113f853337a7d2a6885ad23b8811 9cca530c7cc1b3e02cb8fa7f80060dd4b38562ce git
CNA	Linux	Linux	affected b636fd38dc40113f853337a7d2a6885ad23b8811 86ceaccfdfa16dad05addb33dc206e03589bcfd1 git
CNA	Linux	Linux	affected b636fd38dc40113f853337a7d2a6885ad23b8811 9dc76f6fc0d28d2382583715bc4ec22f28104845 git
CNA	Linux	Linux	affected b636fd38dc40113f853337a7d2a6885ad23b8811 5ee01f1a7343d6a3547b6802ca2d4cdce0edacb1 gi
CNA	Linux	Linux	affected b0af004fd58ded5f898630db008c5b824c27d7db git
CNA	Linux	Linux	affected 370b9e6399da09fe10005fe455878b356de7b85f git
CNA	Linux	Linux	affected 5.2
CNA	Linux	Linux	unaffected 5.2 semver
CNA	Linux	Linux	unaffected 5.10.253 5.10.* semver
CNA	Linux	Linux	unaffected 5.15.203 5.15.* semver
CNA	Linux	Linux	unaffected 6.1.167 6.1.* semver
CNA	Linux	Linux	unaffected 6.6.130 6.6.* semver
CNA	Linux	Linux	unaffected 6.12.78 6.12.* semver
CNA	Linux	Linux	unaffected 6.18.19 6.18.* semver
CNA	Linux	Linux	unaffected 6.19.9 6.19.* semver
CNA	Linux	Linux	unaffected 7.0 * original_commit_for_fix

References			
Reference	Source	Link	Tags
git.kernel.org/stable/c/3dfd1328c05234e8d8fa61948b2ba82680594988	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	
git.kernel.org/stable/c/4a9654a2b46cfdaae287fb8995f536245635e467	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	
git.kernel.org/stable/c/9dc76f6c0d28d2382583715bc4ec22f28104845	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	
git.kernel.org/stable/c/3b95abab7369235a37b15eaec6e1a0b443bba7c7	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	
git.kernel.org/stable/c/7c85debc35e6d131bd29c64f2ae78c6ede0e55c4	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	
git.kernel.org/stable/c/9cca530c7cc1b3e02cb8fa7f80060dd4b38562ce	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	
git.kernel.org/stable/c/5ee01f1a7343d6a3547b6802ca2d4cdce0edacb1	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	
git.kernel.org/stable/c/86ceaccfdfa16dad05adb33dc206e03589bcfd1	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 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