



rds: ib: reject FRMR registration before IB connection is established

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

Summary

CVE	CVE-2026-31425
State	PUBLISHED
Assigner	Linux
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-04-13 14:16:12 UTC
Updated	2026-04-18 09:16:32 UTC

Description In the Linux kernel, the following vulnerability has been resolved: rds: ib: reject FRMR registration before IB connection is e

Risk And Classification

EPSS: 0.000240000 probability, percentile 0.066100000 (date 2026-04-18)

Vendor Declared Affected Products

Source	Vendor	Product	Version
CNA	Linux	Linux	affected 1659185fb4d0025835eb2058a141f0746c5cab00 c506456ebf84c50ed9327473d4e9bd905def212b git
CNA	Linux	Linux	affected 1659185fb4d0025835eb2058a141f0746c5cab00 82e4a3b56b23b844802056c9e75a39d24169b0a4 g
CNA	Linux	Linux	affected 1659185fb4d0025835eb2058a141f0746c5cab00 450ec93c0f172374acbf236f1f5f02d53650aa2d git
CNA	Linux	Linux	affected 1659185fb4d0025835eb2058a141f0746c5cab00 6b0a8de67ac0c74e1a7df92b73c862cb36780dfc git
CNA	Linux	Linux	affected 1659185fb4d0025835eb2058a141f0746c5cab00 a5bfd14c9a299e6db4add4440430ee5e010b03ad gi
CNA	Linux	Linux	affected 1659185fb4d0025835eb2058a141f0746c5cab00 23e07c340c445f0ebff7757ba15434cb447eb662 git
CNA	Linux	Linux	affected 1659185fb4d0025835eb2058a141f0746c5cab00 47de5b73db3b88f45c107393f26aeba26e9e8fae git
CNA	Linux	Linux	affected 1659185fb4d0025835eb2058a141f0746c5cab00 a54ecccf62c5c85259ae5ea5d9c20009519049 git
CNA	Linux	Linux	affected 4.6
CNA	Linux	Linux	unaffected 4.6 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 6.1.168 6.1.* semver
CNA	Linux	Linux	unaffected 6.6.134 6.6.* semver
CNA	Linux	Linux	unaffected 6.12.81 6.12.* semver
CNA	Linux	Linux	unaffected 6.18.22 6.18.* semver

CNA	Linux	Linux	unaffected 6.19.12 6.19.* semver
CNA	Linux	Linux	unaffected 7.0 * original_commit_for_fix

References

Reference	Source	Link	Tags
git.kernel.org/stable/c/a54ecccfae62c5c85259ae5ea5d9c20009519049	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	
git.kernel.org/stable/c/c506456ebf84c50ed9327473d4e9bd905def212b	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	
git.kernel.org/stable/c/450ec93c0f172374acbf236f1f5f02d53650aa2d	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	
git.kernel.org/stable/c/6b0a8de67ac0c74e1a7df92b73c862cb36780dfc	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	
git.kernel.org/stable/c/47de5b73db3b88f45c107393f26aeba26e9e8fae	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	
git.kernel.org/stable/c/23e07c340c445f0ebff7757ba15434cb447eb662	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	
git.kernel.org/stable/c/a5bfd14c9a299e6db4add4440430ee5e010b03ad	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	
git.kernel.org/stable/c/82e4a3b56b23b844802056c9e75a39d24169b0a4	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