



drbd: fix "LOGIC BUG" in drbd_al_begin_io_nonblock()

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

Summary

CVE	CVE-2026-23356
State	PUBLISHED
Assigner	Linux
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-03-25 11:16:34 UTC
Updated	2026-04-18 09:16:20 UTC

Description In the Linux kernel, the following vulnerability has been resolved: drbd: fix "LOGIC BUG" in drbd_al_begin_io_nonblock() Ev

Risk And Classification

EPSS: 0.000320000 probability, percentile 0.090980000 (date 2026-04-18)

Vendor Declared Affected Products

Source	Vendor	Product	Version
CNA	Linux	Linux	affected 08a1ddab6df7d3c7b6341774cb1cf4b21b96a214 933d161baa3794547adee621c0bf52cbf2c1b3cd git
CNA	Linux	Linux	affected 08a1ddab6df7d3c7b6341774cb1cf4b21b96a214 cf01aa6288e1190f89865e765056e2a9d8190639 git
CNA	Linux	Linux	affected 08a1ddab6df7d3c7b6341774cb1cf4b21b96a214 7752569fc78e89794ce28946529850282233f99d git
CNA	Linux	Linux	affected 08a1ddab6df7d3c7b6341774cb1cf4b21b96a214 e91d8d6565b7819d13dab21d4dbed5b45efba59b gi
CNA	Linux	Linux	affected 08a1ddab6df7d3c7b6341774cb1cf4b21b96a214 eef1390125b660b8b61f9f227a03bb9c5e6d36a5 git
CNA	Linux	Linux	affected 08a1ddab6df7d3c7b6341774cb1cf4b21b96a214 d1ef3aed4df2ef1fe46befd8f2da9a6ec5445508 git
CNA	Linux	Linux	affected 08a1ddab6df7d3c7b6341774cb1cf4b21b96a214 f558e5404a72054b525dced1a0c66aa95a144153 gi
CNA	Linux	Linux	affected 08a1ddab6df7d3c7b6341774cb1cf4b21b96a214 ab140365fb62c0bdab22b2f516aff563b2559e3b git
CNA	Linux	Linux	affected 3.10
CNA	Linux	Linux	unaffected 3.10 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 6.12.77 6.12.* semver
CNA	Linux	Linux	unaffected 6.18.17 6.18.* semver
CNA	Linux	Linux	unaffected 6.19.7 6.19.* semver

References

Reference	Source	Link	Tags
git.kernel.org/stable/c/cf01aa6288e1190f89865e765056e2a9d8190639	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	
git.kernel.org/stable/c/eef1390125b660b8b61f9f227a03bb9c5e6d36a5	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	
git.kernel.org/stable/c/d1ef3aed4df2ef1fe46befd8f2da9a6ec5445508	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	
git.kernel.org/stable/c/7752569fc78e89794ce28946529850282233f99d	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	
git.kernel.org/stable/c/ab140365fb62c0bdab22b2f516aff563b2559e3b	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	
git.kernel.org/stable/c/e91d8d6565b7819d13dab21d4dbed5b45efba59b	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	
git.kernel.org/stable/c/933d161baa3794547adee621c0bf52cbf2c1b3cd	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	
git.kernel.org/stable/c/f558e5404a72054b525dced1a0c66aa95a144153	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