



iomap: fix invalid folio access when i_blkbits differs from I/O granularity

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

Summary

CVE	CVE-2026-31463
State	PUBLISHED
Assigner	Linux
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-04-22 14:16:42 UTC
Updated	2026-04-22 14:16:42 UTC

Description In the Linux kernel, the following vulnerability has been resolved: iomap: fix invalid folio access when i_blkbits differs from I/O granularity

Vendor Declared Affected Products

Source	Vendor	Product	Version
CNA	Linux	Linux	affected b2f35ac4146d32d4424aaa941bbc681f12c1b9e6 4a927f670cdb0def226f9f85f42a9f19d9e09c88 git
CNA	Linux	Linux	affected b2f35ac4146d32d4424aaa941bbc681f12c1b9e6 bd71fb3fea9945987053968f028a948997cba8cc git
CNA	Linux	Linux	affected 6.19
CNA	Linux	Linux	unaffected 6.19 semver
CNA	Linux	Linux	unaffected 6.19.11 6.19.* semver
CNA	Linux	Linux	unaffected 7.0 * original_commit_for_fix

References

Reference	Source	Link	Tags
git.kernel.org/stable/c/4a927f670cdb0def226f9f85f42a9f19d9e09c88	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	
git.kernel.org/stable/c/bd71fb3fea9945987053968f028a948997cba8cc	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical

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](#)