



# writeback: don't block sync for filesystems with no data integrity guarantees

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

## Summary

|                        |  |
|------------------------|--|
| <b>CVE</b>             | CVE-2026-31465                               |
| <b>State</b>           | PUBLISHED                                    |
| <b>Assigner</b>        | Linux  |
| <b>Source Priority</b> | CVE Program / NVD first with legacy fallback |
| <b>Published</b>       | 2026-04-22 14:16:42 UTC                      |
| <b>Updated</b>         | 2026-04-22 14:16:42 UTC                      |

**Description** In the Linux kernel, the following vulnerability has been resolved: writeback: don't block sync for filesystems with no data int

## Vendor Declared Affected Products

| Source | Vendor                | Product               | Version   |
|--------|-----------------------|-----------------------|---|
| CNA    | <a href="#">Linux</a> | <a href="#">Linux</a> | affected 0c58a97f919c24fe4245015f4375a39ff05665b6 83800f8ef358ea2fc9b1 ae4986b83f2bc24be927 git |
| CNA    | <a href="#">Linux</a> | <a href="#">Linux</a> | affected 0c58a97f919c24fe4245015f4375a39ff05665b6 5c24a13d8a0466ca0446e58309e51f2606520164 git  |
| CNA    | <a href="#">Linux</a> | <a href="#">Linux</a> | affected 0c58a97f919c24fe4245015f4375a39ff05665b6 76f9377cd2ab7a9220c25d33940d9ca20d368172 git  |
| CNA    | <a href="#">Linux</a> | <a href="#">Linux</a> | affected 6.16   |
| CNA    | <a href="#">Linux</a> | <a href="#">Linux</a> | unaffected 6.16 semver  |
| CNA    | <a href="#">Linux</a> | <a href="#">Linux</a> | unaffected 6.18.21 6.18.* semver  |
| CNA    | <a href="#">Linux</a> | <a href="#">Linux</a> | unaffected 6.19.11 6.19.* semver  |
| CNA    | <a href="#">Linux</a> | <a href="#">Linux</a> | unaffected 7.0 * original_commit_for_fix  |

## References

| Reference   | Source                               | Link  | Tags    |
|---|--------------------------------------|---|---------|
| <a href="https://git.kernel.org/stable/c/76f9377cd2ab7a9220c25d33940d9ca20d368172">git.kernel.org/stable/c/76f9377cd2ab7a9220c25d33940d9ca20d368172</a> | 416baaa9-dc9f-4396-8d5f-8c081fb06d67 | <a href="https://git.kernel.org">git.kernel.org</a> |         |
| <a href="https://git.kernel.org/stable/c/83800f8ef358ea2fc9b1ae4986b83f2bc24be927">git.kernel.org/stable/c/83800f8ef358ea2fc9b1ae4986b83f2bc24be927</a> | 416baaa9-dc9f-4396-8d5f-8c081fb06d67 | <a href="https://git.kernel.org">git.kernel.org</a> |         |
| <a href="https://git.kernel.org/stable/c/5c24a13d8a0466ca0446e58309e51f2606520164">git.kernel.org/stable/c/5c24a13d8a0466ca0446e58309e51f2606520164</a> | 416baaa9-dc9f-4396-8d5f-8c081fb06d67 | <a href="https://git.kernel.org">git.kernel.org</a> |         |
| CVE Program record  | CVE.ORG                              | <a href="https://www.cve.org">www.cve.org</a>       | canonic |
| NVD vulnerability detail  | NVD                                  | <a href="https://nvd.nist.gov">nvd.nist.gov</a>     | 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](#)