



btrfs: fix transaction abort on set received ioctl due to item overflow

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF !\[\]\(003082e50e3009141f59bd5df831749f_img.jpg\)](#)

Summary

| | |
|------------------------|--|
| CVE | CVE-2026-43359 |
| State | PUBLISHED |
| Assigner | Linux |
| Source Priority | CVE Program / NVD first with legacy fallback |
| Published | 2026-05-08 15:16:46 UTC |
| Updated | 2026-05-12 14:10:27 UTC |

Description In the Linux kernel, the following vulnerability has been resolved: btrfs: fix transaction abort on set received ioctl due to item

Risk And Classification

EPSS: 0.000240000 probability, percentile 0.070360000 (date 2026-05-12)

Vendor Declared Affected Products

| Source | Vendor | Product | Version |
|--------|-----------------------|-----------------------|--|
| CNA | Linux | Linux | affected dd5f9615fc5c5e8d3751aab3a17b92768fb1ce70 b9914db13ac15aca3b74544c0bb1a2e0dad1f174 git |
| CNA | Linux | Linux | affected dd5f9615fc5c5e8d3751aab3a17b92768fb1ce70 b19c0465e4daad5aa8f60552ea0578cf31a11b1e git |
| CNA | Linux | Linux | affected dd5f9615fc5c5e8d3751aab3a17b92768fb1ce70 2e57b8cac2ba0d38aac76c1ecdfd8b899e3581a5 git |
| CNA | Linux | Linux | affected dd5f9615fc5c5e8d3751aab3a17b92768fb1ce70 d11aefe654a04fc41996d254748d6a38b6b0a7be git |
| CNA | Linux | Linux | affected dd5f9615fc5c5e8d3751aab3a17b92768fb1ce70 41fb97353ff58fa4f31904c343fc8e3df2f7517d git |
| CNA | Linux | Linux | affected dd5f9615fc5c5e8d3751aab3a17b92768fb1ce70 87f2c46003fce4d739138aab4af1942b1afdadac git |
| CNA | Linux | Linux | affected 3.12 |
| CNA | Linux | Linux | unaffected 3.12 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/d11aefe654a04fc41996d254748d6a38b6b0a7be | 416baaa9-dc9f-4396-8d5f-8c081fb06d67 | git.kernel.org | |
| git.kernel.org/stable/c/2e57b8cac2ba0d38aac76c1ecd8b899e3581a5 | 416baaa9-dc9f-4396-8d5f-8c081fb06d67 | git.kernel.org | |
| git.kernel.org/stable/c/b19c0465e4daad5aa8f60552ea0578cf31a11b1e | 416baaa9-dc9f-4396-8d5f-8c081fb06d67 | git.kernel.org | |
| git.kernel.org/stable/c/87f2c46003fce4d739138aab4af1942b1afdadac | 416baaa9-dc9f-4396-8d5f-8c081fb06d67 | git.kernel.org | |
| git.kernel.org/stable/c/b9914db13ac15aca3b74544c0bb1a2e0dad1f174 | 416baaa9-dc9f-4396-8d5f-8c081fb06d67 | git.kernel.org | |
| git.kernel.org/stable/c/41fb97353ff58fa4f31904c343fc8e3df2f7517d | 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](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://mitre.org) and the authoritative source of CVE content is [MITRE's CVE web site](https://mitre.org). This site includes MITRE data granted under the following [license](https://mitre.org).

Free CVE JSON API cve.report/api

CVE.report and Source URL Uptime Status status.cve.report