



# xfs: avoid dereferencing log items after push callbacks

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

## Summary

<b>CVE</b>	CVE-2026-31453
<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 14:16:39 UTC
<b>Updated</b>	2026-04-22 14:16:39 UTC
<b>Description</b>	In the Linux kernel, the following vulnerability has been resolved: xfs: avoid dereferencing log items after push callbacks Aft

## Vendor Declared Affected Products

Source	Vendor	Product	Version
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	affected 90c60e16401248a4900f3f9387f563d0178dcf34 c8a2ab339b88d10fc34a3318c92f07d8a467019d git
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	affected 90c60e16401248a4900f3f9387f563d0178dcf34 7121b22b0bac89394cc4c6a54b5aebc15347bdf5 git
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	affected 90c60e16401248a4900f3f9387f563d0178dcf34 c4d603e8e58a3bf35480135ccca2b4f7238abda5 git
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	affected 90c60e16401248a4900f3f9387f563d0178dcf34 95fb5d643cc70959baa54cd17f52f80ffc3295e7 git
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	affected 90c60e16401248a4900f3f9387f563d0178dcf34 451c6329d9afa45862c36fe6677eb7750db60617 git
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	affected 90c60e16401248a4900f3f9387f563d0178dcf34 79ef34ec0554ec04bdbafafbc9836423734e1bd6 git
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	affected 5.9
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	unaffected 5.9 semver
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	unaffected 6.1.168 6.1.* semver
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	unaffected 6.6.131 6.6.* semver
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	unaffected 6.12.80 6.12.* 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
git.kernel.org/stable/c/95fb5d643cc70959baa54cd17f52f80ffc3295e7	416baaa9-dc9f-4396-8d5f-8c081fb06d67	<a href="#">git.kernel.org</a>	
git.kernel.org/stable/c/7121b22b0bac89394cc4c6a54b5aebc15347bdf5	416baaa9-dc9f-4396-8d5f-8c081fb06d67	<a href="#">git.kernel.org</a>	
git.kernel.org/stable/c/c4d603e8e58a3bf35480135ccca2b4f7238abda5	416baaa9-dc9f-4396-8d5f-8c081fb06d67	<a href="#">git.kernel.org</a>	

git.kernel.org/stable/c/79ef34ec0554ec04bdbafafbc9836423734e1bd6	416baaa9-dc9f-4396-8d5f-8c081fb06d67	<a href="https://git.kernel.org">git.kernel.org</a>	
git.kernel.org/stable/c/451c6329d9afa45862c36fe6677eb7750db60617	416baaa9-dc9f-4396-8d5f-8c081fb06d67	<a href="https://git.kernel.org">git.kernel.org</a>	
git.kernel.org/stable/c/c8a2ab339b88d10fc34a3318c92f07d8a467019d	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>	canonica
NVD vulnerability detail	NVD	<a href="https://nvd.nist.gov">nvd.nist.gov</a>	canonica

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/licenses).

Free CVE JSON API [cve.report/api](https://cve.report/api)

CVE.report and Source URL Uptime Status [status.cve.report](https://status.cve.report)