



# CVE-2023-49298

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF !\[\]\(003082e50e3009141f59bd5df831749f\_img.jpg\)](#)

## Summary

<b>CVE</b>	CVE-2023-49298
<b>State</b>	PUBLISHED
<b>Assigner</b>	Unknown
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2023-11-24 19:15:00 UTC
<b>Updated</b>	2024-03-18 22:15:00 UTC
<b>Description</b>	Description unavailable.

## Risk And Classification

**Problem Types:** CWE-639

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	<a href="#">Freebsd</a>	<a href="#">Freebsd</a>	14.0	-	All	All
Application	<a href="#">Openzfs</a>	<a href="#">Openzfs</a>	2.2.0	-	All	All
Application	<a href="#">Openzfs</a>	<a href="#">Openzfs</a>	All	All	All	All

## References

Reference	Source	Link
<a href="https://github.com/openzfs/zfs/releases/tag/zfs-2.1.14">github.com/openzfs/zfs/releases/tag/zfs-2.1.14</a>		<a href="https://github.com">github.com</a>
<a href="#">dnode_is_dirty: check dnode and its data for dirtiness by robn · Pull Request #15571 · openzfs/zfs · GitHub</a>		<a href="https://github.com">github.com</a>
<a href="https://www.theregister.com/2023/12/04/two_new_versions_of_openzfs">www.theregister.com/2023/12/04/two_new_versions_of_openzfs</a>		<a href="https://www.theregister.com">www.theregister.com</a>
<a href="https://bugs.freebsd.org/bugzilla/show_bug.cgi">bugs.freebsd.org/bugzilla/show_bug.cgi</a>		<a href="https://bugs.freebsd.org">bugs.freebsd.org</a>
<a href="#">[debian-lts-announce] 20240318 [SECURITY] [DLA 3766-1] zfs-linux security update</a>		<a href="https://lists.debian.org">lists.debian.org</a>
<a href="https://web.archive.org/web/20231124172959/https://www.ibm.com/support/pages/how-remo...">web.archive.org/web/20231124172959/https://www.ibm.com/support/pages/how-remo...</a>		<a href="https://web.archive.org">web.archive.org</a>
<a href="https://news.ycombinator.com/item">news.ycombinator.com/item</a>		<a href="https://news.ycombinator.com">news.ycombinator.com</a>
<a href="https://bugs.gentoo.org/917224">bugs.gentoo.org/917224</a>		<a href="https://bugs.gentoo.org">bugs.gentoo.org</a>
<a href="https://news.ycombinator.com/item">news.ycombinator.com/item</a>		<a href="https://news.ycombinator.com">news.ycombinator.com</a>
<a href="https://github.com/openzfs/zfs/issues/15526">github.com/openzfs/zfs/issues/15526</a>		<a href="https://github.com">github.com</a>
<a href="https://github.com/openzfs/zfs/releases/tag/zfs-2.2.2">github.com/openzfs/zfs/releases/tag/zfs-2.2.2</a>		<a href="https://github.com">github.com</a>
<a href="#">CVE Program record</a>	CVE.ORG	<a href="https://www.cve.org">www.cve.org</a>

No vendor comments have been submitted for this CVE.

### Legacy QID Mappings

[505976](#) Alpine Linux Security Update for zfs-lts

[505977](#) Alpine Linux Security Update for zfs-rpi

[505978](#) Alpine Linux Security Update for zfs

[6000527](#) Debian Security Update for zfs-linux (DLA 3766-1)

© [CVE.report](http://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](http://cve.report/api)

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