



# CVE-2023-2124

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF !\[\]\(e3f8612927870f2e0f9f5989e6dd3064\_img.jpg\)](#)

## Summary

<b>CVE</b>	CVE-2023-2124
<b>State</b>	PUBLIC
<b>Assigner</b>	secalert@redhat.com
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2023-05-15 22:15:00 UTC
<b>Updated</b>	2024-02-01 01:35:00 UTC
<b>Description</b>	An out-of-bounds memory access flaw was found in the Linux kernel's XFS file system in how a user restores an XFS image

## Risk And Classification

**Problem Types:** CWE-787

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	11.0	All	All	All
Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	12.0	All	All	All
Operating System	<a href="#">Linux</a>	<a href="#">Linux Kernel</a>	All	All	All	All
Operating System	<a href="#">Linux</a>	<a href="#">Linux Kernel</a>	All	All	All	All
Hardware	<a href="#">Netapp</a>	<a href="#">H300s</a>	-	All	All	All
Operating System	<a href="#">Netapp</a>	<a href="#">H300s Firmware</a>	-	All	All	All
Hardware	<a href="#">Netapp</a>	<a href="#">H410c</a>	-	All	All	All
Operating System	<a href="#">Netapp</a>	<a href="#">H410c Firmware</a>	-	All	All	All
Hardware	<a href="#">Netapp</a>	<a href="#">H410s</a>	-	All	All	All
Operating System	<a href="#">Netapp</a>	<a href="#">H410s Firmware</a>	-	All	All	All
Hardware	<a href="#">Netapp</a>	<a href="#">H500s</a>	-	All	All	All
Operating System	<a href="#">Netapp</a>	<a href="#">H500s Firmware</a>	-	All	All	All
Hardware	<a href="#">Netapp</a>	<a href="#">H700s</a>	-	All	All	All
Operating System	<a href="#">Netapp</a>	<a href="#">H700s Firmware</a>	-	All	All	All

## References

Reference	Source	Link	Tags
-----------	--------	------	------

kernel/git/torvalds/linux.git - Linux kernel source tree	MISC	<a href="https://git.kernel.org">git.kernel.org</a>	
Debian -- Security Information -- DSA-5480-1 linux	DEBIAN	<a href="https://www.debian.org">www.debian.org</a>	
KASAN: use-after-free Read in xfs_btree_lookup_get_block	MISC	<a href="https://syzkaller.appspot.com">syzkaller.appspot.com</a>	
Debian -- Security Information -- DSA-5448-1 linux	DEBIAN	<a href="https://www.debian.org">www.debian.org</a>	
[SECURITY] [DLA 3623-1] linux-5.10 security update	MLIST	<a href="https://lists.debian.org">lists.debian.org</a>	
CVE-2023-2124 Linux Kernel Vulnerability in NetApp Products   NetApp Product Security	CONFIRM	<a href="https://security.netapp.com">security.netapp.com</a>	
CVE Program record	CVE.ORG	<a href="https://www.cve.org">www.cve.org</a>	canonical
NVD vulnerability detail	NVD	<a href="https://nvd.nist.gov">nvd.nist.gov</a>	canonical, a

No vendor comments have been submitted for this CVE.

### Legacy QID Mappings

<a href="#">160806</a> Oracle Enterprise Linux Security Update for kernel (ELSA-2023-3723)
<a href="#">160859</a> Oracle Enterprise Linux Security Update for kernel (ELSA-2023-4517)
<a href="#">199452</a> Ubuntu Security Notification for Linux kernel (OEM) Vulnerabilities (USN-6206-1)
<a href="#">199464</a> Ubuntu Security Notification for Linux kernel Vulnerabilities (USN-6224-1)
<a href="#">199468</a> Ubuntu Security Notification for Linux kernel Vulnerabilities (USN-6228-1)
<a href="#">199469</a> Ubuntu Security Notification for Linux kernel (OEM) Vulnerabilities (USN-6231-1)
<a href="#">199521</a> Ubuntu Security Notification for Linux kernel (OEM) Vulnerabilities (USN-6235-1)
<a href="#">199615</a> Ubuntu Security Notification for Linux kernel Vulnerabilities (USN-6252-1)
<a href="#">199617</a> Ubuntu Security Notification for Linux kernel Vulnerabilities (USN-6254-1)
<a href="#">199650</a> Ubuntu Security Notification for Linux kernel Vulnerabilities (USN-6284-1)
<a href="#">199669</a> Ubuntu Security Notification for Linux kernel Vulnerabilities (USN-6301-1)
<a href="#">199670</a> Ubuntu Security Notification for Linux kernel Vulnerabilities (USN-6300-1)
<a href="#">241733</a> Red Hat Update for kernel (RHSA-2023:3723)
<a href="#">241740</a> Red Hat Update for kernel-rt (RHSA-2023:3708)
<a href="#">241823</a> Red Hat Update for kernel (RHSA-2023:4137)
<a href="#">241830</a> Red Hat Update for kernel-rt (RHSA-2023:4138)
<a href="#">241926</a> Red Hat Update for kernel (RHSA-2023:4515)
<a href="#">241927</a> Red Hat Update for kernel-rt (RHSA-2023:4541)
<a href="#">241936</a> Red Hat Update for kernel (RHSA-2023:4517)

<a href="#">283979</a> Fedora Security Update for kernel (FEDORA-2023-00393126a0)
<a href="#">283980</a> Fedora Security Update for kernel (FEDORA-2023-dfd4a6e8f2)
<a href="#">284139</a> Fedora Security Update for kernel (FEDORA-2023-26325e5399)
<a href="#">354903</a> Amazon Linux Security Advisory for kernel : ALAS2KERNEL-5.10-2023-031
<a href="#">354904</a> Amazon Linux Security Advisory for kernel : ALAS2KERNEL-5.4-2023-044
<a href="#">354905</a> Amazon Linux Security Advisory for kernel : ALAS2KERNEL-5.15-2023-017
<a href="#">354913</a> Amazon Linux Security Advisory for kernel : ALAS2-2023-2027
<a href="#">354923</a> Amazon Linux Security Advisory for kernel : ALAS-2023-1735
<a href="#">355254</a> Amazon Linux Security Advisory for kernel : ALAS2023-2023-169
<a href="#">355445</a> Amazon Linux Security Advisory for kernel-livepatch : ALAS2023LIVEPATCH-2023-006
<a href="#">355446</a> Amazon Linux Security Advisory for kernel-livepatch : ALAS2023LIVEPATCH-2023-008
<a href="#">355448</a> Amazon Linux Security Advisory for kernel-livepatch : ALAS2023LIVEPATCH-2023-009
<a href="#">355449</a> Amazon Linux Security Advisory for kernel-livepatch : ALAS2023LIVEPATCH-2023-007
<a href="#">355529</a> Amazon Linux Security Advisory for kernel-livepatch : ALAS2LIVEPATCH-2023-132
<a href="#">355530</a> Amazon Linux Security Advisory for kernel-livepatch : ALAS2LIVEPATCH-2023-133
<a href="#">378710</a> Alibaba Cloud Linux Security Update for cloud-kernel (ALINUX3-SA-2023:0079)
<a href="#">378889</a> Alibaba Cloud Linux Security Update for cloud-kernel (ALINUX2-SA-2023:0036)
<a href="#">379043</a> Alibaba Cloud Linux Security Update for cloud-kernel (ALINUX3-SA-2023:0136)
<a href="#">6000207</a> Debian Security Update for linux (DSA 5448-1)
<a href="#">6000212</a> Debian Security Update for linux (DSA 5480-1)
<a href="#">6000265</a> Debian Security Update for linux-5.10 (DLA 3623-1)
<a href="#">6140327</a> AWS Bottlerocket Security Update for kernel (GHSA-9xq2-9gvm-h3gj)
<a href="#">673232</a> EulerOS Security Update for kernel (EulerOS-SA-2023-2357)
<a href="#">673272</a> EulerOS Security Update for kernel (EulerOS-SA-2023-2584)
<a href="#">673372</a> EulerOS Security Update for kernel (EulerOS-SA-2023-2787)
<a href="#">673393</a> EulerOS Security Update for kernel (EulerOS-SA-2023-2647)
<a href="#">673498</a> EulerOS Security Update for kernel (EulerOS-SA-2023-3132)
<a href="#">673970</a> EulerOS Security Update for kernel (EulerOS-SA-2023-2879)

674113 EulerOS Security Update for kernel (EulerOS-SA-2023-2689)
753980 SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2023:2151-1)
753982 SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2023:2148-1)
753985 SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2023:2162-1)
754005 SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2023:2163-1)
754023 SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2023:2232-1)
754145 SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2023:2651-1)
755851 SUSE Enterprise Linux Security Update for the linux kernel (SUSE-SU-2023:2646-1)
907142 Common Base Linux Mariner (CBL-Mariner) Security Update for kernel (26773-1)
907179 Common Base Linux Mariner (CBL-Mariner) Security Update for kernel (26781-1)
941166 AlmaLinux Security Update for kernel (ALSA-2023:3723)
941167 AlmaLinux Security Update for kernel-rt (ALSA-2023:3708)
941227 AlmaLinux Security Update for kernel (ALSA-2023:4517)
941228 AlmaLinux Security Update for kernel-rt (ALSA-2023:4541)
961032 Rocky Linux Security Update for kernel (RLSA-2023:4517)
961046 Rocky Linux Security Update for kernel-rt (RLSA-2023:4541)

© [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](#).

**CVE.report and Source URL Uptime Status [status.cve.report](#)**