



# CVE-2022-28796

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

## Summary

<b>CVE</b>	CVE-2022-28796
<b>State</b>	PUBLIC
<b>Assigner</b>	cve@mitre.org
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2022-04-08 05:15:00 UTC
<b>Updated</b>	2023-08-29 21:02:00 UTC
<b>Description</b>	jbd2_journal_wait_updates in fs/jbd2/transaction.c in the Linux kernel before 5.17.1 has a use-after-free caused by a transa

## Risk And Classification

**Problem Types:** CWE-362

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	<a href="#">Fedoraproject</a>	<a href="#">Fedora</a>	35	All	All	All
Operating System	<a href="#">Linux</a>	<a href="#">Linux Kernel</a>	All	All	All	All
Application	<a href="#">Netapp</a>	<a href="#">Active Iq Unified Manager</a>	-	All	All	All
Hardware	<a href="#">Netapp</a>	<a href="#">H300e</a>	-	All	All	All
Operating System	<a href="#">Netapp</a>	<a href="#">H300e Firmware</a>	-	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="#">H500e</a>	-	All	All	All
Operating System	<a href="#">Netapp</a>	<a href="#">H500e 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="#">H700e</a>	-	All	All	All
Operating System	<a href="#">Netapp</a>	<a href="#">H700e 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
Hardware	<a href="#">Netapp</a>	<a href="#">Hci Compute Node</a>	-	All	All	All
Operating System	<a href="#">Netapp</a>	<a href="#">Hci Compute Node Firmware</a>	-	All	All	All
Application	<a href="#">Netapp</a>	<a href="#">Solidfire Enterprise Sds Hci Storage Node</a>	-	All	All	All
Application	<a href="#">Netapp</a>	<a href="#">Solidfire Hci Management Node</a>	-	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux</a>	6.0	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux</a>	7.0	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux</a>	8.0	All	All	All

## References

Reference	Source	Link	Tags
<a href="https://cdn.kernel.org/pub/linux/kernel/v5.x/ChangeLog-5.17.1">cdn.kernel.org/pub/linux/kernel/v5.x/ChangeLog-5.17.1</a>	MISC	<a href="https://cdn.kernel.org">cdn.kernel.org</a>	
<a href="#">jbd2: fix use-after-free of transaction_t race · torvalds/linux@cc16eec · GitHub</a>	MISC	<a href="https://github.com">github.com</a>	
<a href="#">April 2022 Linux Kernel Vulnerabilities in NetApp Products   NetApp Product Security</a>	CONFIRM	<a href="https://security.netapp.com">security.netapp.com</a>	
<a href="#">CVE Program record</a>	CVE.ORG	<a href="https://www.cve.org">www.cve.org</a>	canonical
<a href="#">NVD vulnerability detail</a>	NVD	<a href="https://nvd.nist.gov">nvd.nist.gov</a>	canonical, analysis

No vendor comments have been submitted for this CVE.

## Legacy QID Mappings

<a href="#">900805</a> Common Base Linux Mariner (CBL-Mariner) Security Update for kernel (9328)
<a href="#">901012</a> Common Base Linux Mariner (CBL-Mariner) Security Update for kernel (9331)
<a href="#">901360</a> Common Base Linux Mariner (CBL-Mariner) Security Update for kernel (9328-1)
<a href="#">902104</a> Common Base Linux Mariner (CBL-Mariner) Security Update for kernel (9331-1)
<a href="#">905893</a> Common Base Linux Mariner (CBL-Mariner) Security Update for kernel (9328-2)
<a href="#">906424</a> Common Base Linux Mariner (CBL-Mariner) Security Update for kernel (9331-2)

© [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](https://cve.report/api)

