



CVE-2023-34462

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

Summary

CVE	CVE-2023-34462
State	PUBLIC
Assigner	security-advisories@github.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2023-06-22 23:15:00 UTC
Updated	2023-11-18 21:15:00 UTC
Description	Netty is an asynchronous event-driven network application framework for rapid development of maintainable high performan

Risk And Classification

Problem Types: CWE-400

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Netty	Netty	All	All	All	All

References

Reference	Source	Link	Tags
CVE-2023-34462 Apache Netty Vulnerability in NetApp Products NetApp Product Security	MISC	security.netapp.com	
Merge pull request from GHSA-6mj-q-h674-j845 · netty/netty@535da17 · GitHub	MISC	github.com	
www.debian.org/security/2023/dsa-5558		www.debian.org	
SniHandler 16MB allocation · Advisory · netty/netty · GitHub	MISC	github.com	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, e

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

20391 IBM DB2 Denial of Service (DoS) Vulnerability (7087234)
242105 Red Hat Update for JBoss Enterprise Application Platform 7.4.1 on RHEL 9 (RHSA-2023:5486)
242105 Red Hat Update for JBoss Enterprise Application Platform 7.4.1 on RHEL 9 (RHSA-2023:5486)

[242106](#) Red Hat Update for JBoss Enterprise Application Platform 7.4.1 on RHEL 7 (RHSA-2023:5484)

[242122](#) Red Hat Update for JBoss Enterprise Application Platform 7.4.1 on RHEL 8 (RHSA-2023:5485)

[378947](#) Oracle Coherence October 2023 Critical Patch Update (CPUOCT2023)

[6000331](#) Debian Security Update for netty (DSA 5558-1)

[754215](#) SUSE Enterprise Linux Security Update for netty, netty-tcnative (SUSE-SU-2023:2974-1)

© [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](#)