CVE-2022-41881

MITRE | NVD | CVE.ORG | JSON API | Print: PDF

Summary

CVE	CVE-2022-41881
State	PUBLIC
Assigner	security-advisories@github.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2022-12-12 18:15:00 UTC
Updated	2023-03-01 15:08:00 UTC
Description	Netty project is an event-driven asynchronous network application framework. In versions prior to 4.1.86.Final, a StackOver

Risk And Classification

Problem Types: CWE-674

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Debian	Debian Linux	10.0	All	All	All
Operating System	Debian	Debian Linux	11.0	All	All	All
Application	Netty	Netty	All	All	All	All

References

Reference	Source	Link	Tags
[SECURITY] [DLA 3268-1] netty security update	MLIST	lists.debian.org	
Debian -- Security Information -- DSA-5316-1 netty	DEBIAN	www.debian.org	
HAProxyMessageDecoder Stack Exhaustion DoS · Advisory · netty/netty · GitHub	MISC	github.com	
December 2022 Apache Netty Vulnerabilities in NetApp Products | NetApp Product Security	CONFIRM	security.netapp.com	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical,

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

181469 Debian Security Update for netty (DLA 3268-1)

181471 Debian Security Update for netty (DSA 5316-1)

182291 Debian Security Update for netty (CVE-2022-41881)

199574 Ubuntu Security Notification for Netty Vulnerabilities (USN-6049-1)

241301 Red Hat Update for JBoss Enterprise Application Platform 7.4.1 on RHEL 7 (RHSA-2023:1512)

241302 Red Hat Update for JBoss Enterprise Application Platform 7.4.1 on RHEL 8 (RHSA-2023:1513)

241303 Red Hat Update for JBoss Enterprise Application Platform 7.4.1 on RHEL 9 (RHSA-2023:1514)

378427 Oracle PeopleSoft Enterprise PeopleTools Product Multiple Vulnerabilities (CPUAPR2023)

378429 Oracle Coherence April 2023 Critical Patch Update (CPUAPR2023)

753971 SUSE Enterprise Linux Security Update for netty, netty-tcnative (SUSE-SU-2023:2096-1)

© 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 registred 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

CVE.report and Source URL Uptime Status **status.cve.report**