CVE-2022-41915

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

Summary

CVE	CVE-2022-41915
State	PUBLIC
Assigner	security-advisories@github.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2022-12-13 07:15:00 UTC
Updated	2023-03-01 15:09:00 UTC
Description	Netty project is an event-driven asynchronous network application framework. Starting in version 4.1.83.Final and prior to 4

Risk And Classification

Problem Types: CWE-113 | CWE-436

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
Application	Netty	Netty	4.1.86	All	All	All

References

Reference	Source	Link
HTTP Response splitting from assigning header value iterator · Advisory · netty/netty · GitHub	MISC	github.com
[SECURITY] [DLA 3268-1] netty security update	MLIST	lists.debian.(
Merge pull request from GHSA-hh82-3pmq-7frp · netty/netty@fe18adf · GitHub	MISC	github.com
Debian -- Security Information -- DSA-5316-1 netty	DEBIAN	www.debian
CVE CVE-2022-41915: Incorrect range. Releases < 4.1.83.Final not affected · Issue #13084 · netty/netty · GitHub	MISC	github.com
Reject HTTP/2 header values with invalid characters by chrisvest · Pull Request #12760 · netty/netty · GitHub	MISC	github.com
December 2022 Apache Netty Vulnerabilities in NetApp Products | NetApp Product Security	CONFIRM	security.neta
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

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)

183803 Debian Security Update for netty (CVE-2022-41915)

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

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**