



# CVE-2022-41881

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

## Summary

<b>CVE</b>	CVE-2022-41881
<b>State</b>	PUBLIC
<b>Assigner</b>	security-advisories@github.com
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2022-12-12 18:15:00 UTC
<b>Updated</b>	2023-03-01 15:08:00 UTC
<b>Description</b>	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	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	10.0	All	All	All
Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	11.0	All	All	All
Application	<a href="#">Netty</a>	<a href="#">Netty</a>	All	All	All	All

## References

Reference	Source	Link	Tags
[SECURITY] [DLA 3268-1] netty security update	MLIST	<a href="https://lists.debian.org">lists.debian.org</a>	
Debian -- Security Information -- DSA-5316-1 netty	DEBIAN	<a href="https://www.debian.org">www.debian.org</a>	
HAProxyMessageDecoder Stack Exhaustion DoS · Advisory · netty/netty · GitHub	MISC	<a href="https://github.com">github.com</a>	
December 2022 Apache Netty Vulnerabilities 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, ...

No vendor comments have been submitted for this CVE.

## Legacy QID Mappings

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

<a href="#">181471</a> Debian Security Update for netty (DSA 5316-1)
<a href="#">182291</a> Debian Security Update for netty (CVE-2022-41881)
<a href="#">199574</a> Ubuntu Security Notification for Netty Vulnerabilities (USN-6049-1)
<a href="#">241301</a> Red Hat Update for JBoss Enterprise Application Platform 7.4.1 on RHEL 7 (RHSA-2023:1512)
<a href="#">241302</a> Red Hat Update for JBoss Enterprise Application Platform 7.4.1 on RHEL 8 (RHSA-2023:1513)
<a href="#">241303</a> Red Hat Update for JBoss Enterprise Application Platform 7.4.1 on RHEL 9 (RHSA-2023:1514)
<a href="#">378427</a> Oracle PeopleSoft Enterprise PeopleTools Product Multiple Vulnerabilities (CPUAPR2023)
<a href="#">378429</a> Oracle Coherence April 2023 Critical Patch Update (CPUAPR2023)
<a href="#">753971</a> 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 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](#)**