



# CVE-2014-0193

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

## Summary

<b>CVE</b>	CVE-2014-0193
<b>State</b>	PUBLIC
<b>Assigner</b>	secalert@redhat.com
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2014-05-06 14:55:00 UTC
<b>Updated</b>	2023-02-13 00:36:00 UTC
<b>Description</b>	WebSocket08FrameDecoder in Netty 3.6.x before 3.6.9, 3.7.x before 3.7.1, 3.8.x before 3.8.2, 3.9.x before 3.9.1, and 4.0.x

## Risk And Classification

**Problem Types:** CWE-399

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Netty	Netty	3.6.0	All	All	All
Application	Netty	Netty	3.6.1	All	All	All
Application	Netty	Netty	3.6.2	All	All	All
Application	Netty	Netty	3.6.3	All	All	All
Application	Netty	Netty	3.6.4	All	All	All
Application	Netty	Netty	3.6.5	All	All	All
Application	Netty	Netty	3.6.6	All	All	All
Application	Netty	Netty	3.6.7	All	All	All
Application	Netty	Netty	3.6.8	All	All	All
Application	Netty	Netty	3.7.0	All	All	All
Application	Netty	Netty	3.8.0	All	All	All
Application	Netty	Netty	3.8.1	All	All	All
Application	Netty	Netty	3.9.0	All	All	All
Application	Netty	Netty	4.0.0	All	All	All
Application	Netty	Netty	4.0.1	All	All	All
Application	Netty	Netty	4.0.10	All	All	All
Application	Netty	Netty	4.0.11	All	All	All

Application	Netty	Netty	4.0.12	All	All	All
Application	Netty	Netty	4.0.13	All	All	All
Application	Netty	Netty	4.0.14	All	All	All
Application	Netty	Netty	4.0.15	All	All	All
Application	Netty	Netty	4.0.16	All	All	All
Application	Netty	Netty	4.0.17	All	All	All
Application	Netty	Netty	4.0.18	All	All	All
Application	Netty	Netty	4.0.2	All	All	All
Application	Netty	Netty	4.0.3	All	All	All
Application	Netty	Netty	4.0.4	All	All	All
Application	Netty	Netty	4.0.5	All	All	All
Application	Netty	Netty	4.0.6	All	All	All
Application	Netty	Netty	4.0.7	All	All	All
Application	Netty	Netty	4.0.8	All	All	All
Application	Netty	Netty	4.0.9	All	All	All
Application	Netty	Netty	3.6.0	All	All	All
Application	Netty	Netty	3.6.1	All	All	All
Application	Netty	Netty	3.6.2	All	All	All
Application	Netty	Netty	3.6.3	All	All	All
Application	Netty	Netty	3.6.4	All	All	All
Application	Netty	Netty	3.6.5	All	All	All
Application	Netty	Netty	3.6.6	All	All	All
Application	Netty	Netty	3.6.7	All	All	All
Application	Netty	Netty	3.6.8	All	All	All
Application	Netty	Netty	3.7.0	All	All	All
Application	Netty	Netty	3.8.0	All	All	All
Application	Netty	Netty	3.8.1	All	All	All
Application	Netty	Netty	3.9.0	All	All	All
Application	Netty	Netty	4.0.0	All	All	All
Application	Netty	Netty	4.0.1	All	All	All
Application	Netty	Netty	4.0.10	All	All	All
Application	Netty	Netty	4.0.11	All	All	All
Application	Netty	Netty	4.0.12	All	All	All
Application	Netty	Netty	4.0.13	All	All	All
Application	Netty	Netty	4.0.14	All	All	All

Application	Netty	Netty	4.0.15	All	All	All
Application	Netty	Netty	4.0.16	All	All	All
Application	Netty	Netty	4.0.17	All	All	All
Application	Netty	Netty	4.0.18	All	All	All
Application	Netty	Netty	4.0.2	All	All	All
Application	Netty	Netty	4.0.3	All	All	All
Application	Netty	Netty	4.0.4	All	All	All
Application	Netty	Netty	4.0.5	All	All	All
Application	Netty	Netty	4.0.6	All	All	All
Application	Netty	Netty	4.0.7	All	All	All
Application	Netty	Netty	4.0.8	All	All	All
Application	Netty	Netty	4.0.9	All	All	All

## References

Reference	Source	Link
Red Hat Customer Portal	REDHAT	<a href="https://rhn.redhat.com">rhn.redhat.com</a>
Red Hat Customer Portal	REDHAT	<a href="https://rhn.redhat.com">rhn.redhat.com</a>
Security Advisory SA59290 - Red Hat update for Red Hat JBoss BRMS - Secunia	SECUNIA	<a href="https://secunia.com">secunia.com</a>
Security Advisory SA58280 - Netty WebSocket08FrameDecoder Denial of Service Vulnerability - Secunia	SECUNIA	<a href="https://secunia.com">secunia.com</a>
Netty.news: Release day!	CONFIRM	<a href="https://netty.io">netty.io</a>
Pony Mail!	MLIST	<a href="https://lists.apache.org">lists.apache.org</a>
[SECURITY] [DLA 2110-1] netty-3.9 security update	MLIST	<a href="https://lists.debian.org">lists.debian.org</a>
Pony Mail!	MISC	<a href="https://lists.apache.org">lists.apache.org</a>
Red Hat Customer Portal	REDHAT	<a href="https://rhn.redhat.com">rhn.redhat.com</a>
Red Hat Customer Portal	REDHAT	<a href="https://rhn.redhat.com">rhn.redhat.com</a>
Red Hat Customer Portal	REDHAT	<a href="https://rhn.redhat.com">rhn.redhat.com</a>
Fix a resource usage problem in the WebSocket08FrameDecoder · Issue #2441 · netty/netty · GitHub	CONFIRM	<a href="https://github.com">github.com</a>
Red Hat Customer Portal	REDHAT	<a href="https://rhn.redhat.com">rhn.redhat.com</a>
Red Hat Customer Portal	REDHAT	<a href="https://rhn.redhat.com">rhn.redhat.com</a>
Netty 'WebSocket08FrameDecoder' Class Denial of Service Vulnerability	BID	<a href="https://www.securityfocus.com">www.securityfocus.com</a>
CVE Program record	CVE.ORG	<a href="https://www.cve.org">www.cve.org</a>
NVD vulnerability detail	NVD	<a href="https://nvd.nist.gov">nvd.nist.gov</a>

No vendor comments have been submitted for this CVE.

## Legacy QID Mappings

[241029](#) Red Hat Update for JBoss Enterprise Application Platform 6.3.0 (RHSA-2014:1020)

[241030](#) Red Hat Update for JBoss Enterprise Application Platform 6.3.0 (RHSA-2014:1019)

[994824](#) Java (Maven) Security Update for io.netty:netty (GHSA-7vpq-g998-qpv7)

© [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](#)