



# CVE-2023-1108

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

## Summary

<b>CVE</b>	CVE-2023-1108
<b>State</b>	PUBLIC
<b>Assigner</b>	secalert@redhat.com
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2023-09-14 15:15:00 UTC
<b>Updated</b>	2023-11-16 00:46:00 UTC
<b>Description</b>	A flaw was found in undertow. This issue makes achieving a denial of service possible due to an unexpected handshake st

## Risk And Classification

**Problem Types:** CWE-835

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	<a href="#">Netapp</a>	<a href="#">Oncommand Workflow Automation</a>	-	All	All	All
Application	<a href="#">Redhat</a>	<a href="#">Build Of Quarkus</a>	-	All	All	All
Application	<a href="#">Redhat</a>	<a href="#">Decision Manager</a>	7.0	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux</a>	7.0	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux</a>	8.0	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux</a>	9.0	All	All	All
Application	<a href="#">Redhat</a>	<a href="#">Fuse</a>	1.0.0	All	All	All
Application	<a href="#">Redhat</a>	<a href="#">Integration Camel K</a>	-	All	All	All
Application	<a href="#">Redhat</a>	<a href="#">Integration Service Registry</a>	-	All	All	All
Application	<a href="#">Redhat</a>	<a href="#">Jboss Enterprise Application Platform</a>	-	All	All	All
Application	<a href="#">Redhat</a>	<a href="#">Jboss Enterprise Application Platform</a>	7.4	All	All	All
Application	<a href="#">Redhat</a>	<a href="#">Jboss Enterprise Application Platform Expansion Pack</a>	-	All	All	All
Application	<a href="#">Redhat</a>	<a href="#">Openshift Application Runtimes</a>	-	All	All	All
Application	<a href="#">Redhat</a>	<a href="#">Openshift Container Platform</a>	4.11	All	All	All
Application	<a href="#">Redhat</a>	<a href="#">Openshift Container Platform</a>	4.12	All	All	All
Application	<a href="#">Redhat</a>	<a href="#">Openshift Container Platform For Linuxone</a>	4.10	All	All	All
Application	<a href="#">Redhat</a>	<a href="#">Openshift Container Platform For Linuxone</a>	4.9	All	All	All

Application	Redhat	Openshift Container Platform For Power	4.10	All	All	All
Application	Redhat	Openshift Container Platform For Power	4.9	All	All	All
Application	Redhat	Openstack Platform	13.0	All	All	All
Application	Redhat	Process Automation	7.0	All	All	All
Application	Redhat	Single Sign-on	-	All	All	All
Application	Redhat	Single Sign-on	7.6	All	All	All
Application	Redhat	Undertow	All	All	All	All

## References

Reference	Source	Link	Tags
CVE-2023-1108 Undertow Vulnerability in NetApp Products   NetApp Product Security	MISC	<a href="https://security.netapp.com">security.netapp.com</a>	
<a href="https://access.redhat.com/errata/RHSA-2023:3884">access.redhat.com/errata/RHSA-2023:3884</a>	MISC	<a href="https://access.redhat.com">access.redhat.com</a>	
<a href="https://access.redhat.com/errata/RHSA-2023:3885">access.redhat.com/errata/RHSA-2023:3885</a>	MISC	<a href="https://access.redhat.com">access.redhat.com</a>	
<a href="https://access.redhat.com/errata/RHSA-2023:3883">access.redhat.com/errata/RHSA-2023:3883</a>	MISC	<a href="https://access.redhat.com">access.redhat.com</a>	
cve-details	MISC	<a href="https://access.redhat.com">access.redhat.com</a>	
2174246 – (CVE-2023-1108) CVE-2023-1108 Undertow: Infinite loop in SslConduit during close	MISC	<a href="https://bugzilla.redhat.com">bugzilla.redhat.com</a>	
Red Hat	MISC	<a href="https://access.redhat.com">access.redhat.com</a>	
Red Hat	MISC	<a href="https://access.redhat.com">access.redhat.com</a>	
<a href="https://access.redhat.com/errata/RHSA-2023:3888">access.redhat.com/errata/RHSA-2023:3888</a>	MISC	<a href="https://access.redhat.com">access.redhat.com</a>	
Red Hat	MISC	<a href="https://access.redhat.com">access.redhat.com</a>	
Red Hat	MISC	<a href="https://access.redhat.com">access.redhat.com</a>	
Red Hat	MISC	<a href="https://access.redhat.com">access.redhat.com</a>	
<a href="https://access.redhat.com/errata/RHSA-2023:3892">access.redhat.com/errata/RHSA-2023:3892</a>	MISC	<a href="https://access.redhat.com">access.redhat.com</a>	
Red Hat	MISC	<a href="https://access.redhat.com">access.redhat.com</a>	
Red Hat	MISC	<a href="https://access.redhat.com">access.redhat.com</a>	
Red Hat	MISC	<a href="https://access.redhat.com">access.redhat.com</a>	
CVE Program record	CVE.ORG	<a href="https://www.cve.org">www.cve.org</a>	canonic
NVD vulnerability detail	NVD	<a href="https://nvd.nist.gov">nvd.nist.gov</a>	canonic

No vendor comments have been submitted for this CVE.

## Legacy QID Mappings

[241253](#) Red Hat Update for JBoss Enterprise Application Platform 7.4 (RHSA-2023:1185)

[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)

995297 Java (Maven) Security Update for io.undertow:undertow-core (GHSA-m4mm-pg93-fv78)

© [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](#)**