



# CVE-2020-27218

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

## Summary

<b>CVE</b>	CVE-2020-27218
<b>State</b>	PUBLIC
<b>Assigner</b>	security@eclipse.org
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2020-11-28 01:15:00 UTC
<b>Updated</b>	2023-11-07 03:20:00 UTC
<b>Description</b>	In Eclipse Jetty version 9.4.0.RC0 to 9.4.34.v20201102, 10.0.0.alpha0 to 10.0.0.beta2, and 11.0.0.alpha0 to 11.0.0.beta2, i

## Risk And Classification

**Problem Types:** NVD-CWE-noinfo

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	<a href="#">Apache</a>	<a href="#">Kafka</a>	2.7.0	All	All	All
Application	<a href="#">Apache</a>	<a href="#">Spark</a>	2.4.8	All	All	All
Application	<a href="#">Apache</a>	<a href="#">Spark</a>	3.0.3	All	All	All
Application	<a href="#">Eclipse</a>	<a href="#">Jetty</a>	All	All	All	All
Application	<a href="#">Eclipse</a>	<a href="#">Jetty</a>	10.0.0	alpha0	All	All
Application	<a href="#">Eclipse</a>	<a href="#">Jetty</a>	10.0.0	alpha1	All	All
Application	<a href="#">Eclipse</a>	<a href="#">Jetty</a>	10.0.0	beta0	All	All
Application	<a href="#">Eclipse</a>	<a href="#">Jetty</a>	10.0.0	beta1	All	All
Application	<a href="#">Eclipse</a>	<a href="#">Jetty</a>	10.0.0	beta2	All	All
Application	<a href="#">Eclipse</a>	<a href="#">Jetty</a>	11.0.0	alpha0	All	All
Application	<a href="#">Eclipse</a>	<a href="#">Jetty</a>	11.0.0	beta1	All	All
Application	<a href="#">Eclipse</a>	<a href="#">Jetty</a>	11.0.0	beta2	All	All
Application	<a href="#">Eclipse</a>	<a href="#">Jetty</a>	All	All	All	All
Application	<a href="#">Eclipse</a>	<a href="#">Jetty</a>	10.0.0	alpha0	All	All
Application	<a href="#">Eclipse</a>	<a href="#">Jetty</a>	10.0.0	alpha1	All	All
Application	<a href="#">Eclipse</a>	<a href="#">Jetty</a>	10.0.0	beta0	All	All
Application	<a href="#">Eclipse</a>	<a href="#">Jetty</a>	10.0.0	beta1	All	All

Application	<a href="#">Eclipse</a>	<a href="#">Jetty</a>	10.0.0	beta2	All	All
Application	<a href="#">Eclipse</a>	<a href="#">Jetty</a>	11.0.0	alpha0	All	All
Application	<a href="#">Eclipse</a>	<a href="#">Jetty</a>	11.0.0	beta1	All	All
Application	<a href="#">Eclipse</a>	<a href="#">Jetty</a>	11.0.0	beta2	All	All
Application	<a href="#">Netapp</a>	<a href="#">Oncommand System Manager</a>	All	All	All	All
Application	<a href="#">Netapp</a>	<a href="#">Snap Creator Framework</a>	-	All	All	All
Application	<a href="#">Netapp</a>	<a href="#">Snap Creator Framework</a>	-	All	All	All
Application	<a href="#">Oracle</a>	<a href="#">Blockchain Platform</a>	All	All	All	All
Application	<a href="#">Oracle</a>	<a href="#">Communications Converged Application Server - Service Controller</a>	6.2	All	All	All
Application	<a href="#">Oracle</a>	<a href="#">Communications Offline Mediation Controller</a>	12.0.0.3.0	All	All	All
Application	<a href="#">Oracle</a>	<a href="#">Communications Pricing Design Center</a>	12.0.0.3.0	All	All	All
Application	<a href="#">Oracle</a>	<a href="#">Communications Services Gatekeeper</a>	7.0	All	All	All
Application	<a href="#">Oracle</a>	<a href="#">Communications Session Route Manager</a>	All	All	All	All
Application	<a href="#">Oracle</a>	<a href="#">Flexcube Private Banking</a>	12.0.0	All	All	All
Application	<a href="#">Oracle</a>	<a href="#">Flexcube Private Banking</a>	12.1.0	All	All	All
Application	<a href="#">Oracle</a>	<a href="#">Hyperion Infrastructure Technology</a>	11.1.2.6.0	All	All	All
Application	<a href="#">Oracle</a>	<a href="#">Rest Data Services</a>	All	All	All	All
Application	<a href="#">Oracle</a>	<a href="#">Retail Eftlink</a>	20.0.0	All	All	All
Application	<a href="#">Oracle</a>	<a href="#">Siebel Core - Automation</a>	All	All	All	All

## References

### Reference

Pony Mail!

Pony Mail!

Pony Mail!

Pony Mail!

Pony Mail!

Pony Mail!

Pony Mail!

Pony Mail!

Pony Mail!

Pony Mail!

Pony Mail!

Pony Mail!

Pony Mail!

Pony Mail!



Pony Mail!

Pony Mail!

Oracle Critical Patch Update Advisory - April 2022

Pony Mail!

Pony Mail!

Pony Mail!

[SECURITY] [DLA 3641-1] jetty9 security update

Pony Mail!

Pony Mail!

Pony Mail!

Pony Mail!

Pony Mail!

Pony Mail!

Pony Mail!

Pony Mail!

Pony Mail!

Pony Mail!

Pony Mail!

Pony Mail!

Pony Mail!

Pony Mail!

Pony Mail!

Pony Mail!

Pony Mail!

Pony Mail!

Pony Mail!

Pony Mail!

Pony Mail!

Pony Mail!

Pony Mail!

Pony Mail!

Pony Mail!

Pony Mail!

CVE-2020-27218 Eclipse Jetty Vulnerability in NetApp Products | NetApp Product Security

Pony Mail!

Oracle Critical Patch Update Advisory - July 2021

Pony Mail!

Pony Mail!

Pony Mail!

Pony Mail!

Pony Mail!

Pony Mail!

Pony Mail!

Pony Mail!

Pony Mail!

Pony Mail!

Pony Mail!

Pony Mail!

Oracle Critical Patch Update Advisory - October 2021

Pony Mail!

Pony Mail!

Pony Mail!

Pony Mail!

Pony Mail!

Pony Mail!

Pony Mail!

Pony Mail!

Pony Mail!

Pony Mail!

Pony Mail!

Pony Mail!

Pony Mail!

Pony Mail!

Pony Mail!

Pony Mail!

Pony Mail!

Pony Mail!

Pony Mail!

Pony Mail!

Pony Mail!

Pony Mail!

Pony Mail!

Pony Mail!

Pony Mail!

Pony Mail!

Pony Mail!

Pony Mail!

Pony Mail!

Pony Mail!

Pony Mail!

Pony Mail!

Pony Mail!

Pony Mail!

Pony Mail!

Pony Mail!

Pony Mail!

Pony Mail!

Pony Mail!

Pony Mail!

Pony Mail!

Pony Mail!

Pony Mail!

Pony Mail!

Pony Mail!

Pony Mail!

Pony Mail!

Pony Mail!

Pony Mail!

Pony Mail!

Pony Mail!

Pony Mail!

Pony Mail!

Pony Mail!

Pony Mail!

Pony Mail!

Pony Mail!

Pony Mail!

Pony Mail!

Pony Mail!

Pony Mail!

Pony Mail!

Pony Mail!

Pony Mail!

Pony Mail!

Pony Mail!

Pony Mail!

Pony Mail!

Pony Mail!

Pony Mail!

Pony Mail!

Pony Mail!

Pony Mail!

Buffer not correctly recycled in Gzip Request inflation - Advisory · eclipse/jetty.project · GitHub

Pony Mail!

Pony Mail!

Pony Mail!

Pony Mail!

Pony Mail!

Pony Mail!

Pony Mail!

Pony Mail!

Pony Mail!

Pony Mail!

Pony Mail!

[nifi-commits] 20210222 svn commit: r1886814 - /nifi/site/trunk/security.html

Pony Mail!

Pony Mail!

Pony Mail!

Pony Mail!

Pony Mail!

Pony Mail!

Pony Mail!

Pony Mail!

Pony Mail!

Pony Mail!

Pony Mail!

Pony Mail!

Pony Mail!

Pony Mail!

Pony Mail!

Pony Mail!

Pony Mail!

Pony Mail!

Pony Mail!

Pony Mail!

Pony Mail!

Pony Mail!

Pony Mail!

Pony Mail!

Pony Mail!

Pony Mail!

Pony Mail!

Pony Mail!

Pony Mail!

Pony Mail!

Pony Mail!

Pony Mail!

Pony Mail!

Pony Mail!

Pony Mail!

Pony Mail!

Pony Mail!

Pony Mail!

Oracle Critical Patch Update Advisory - April 2021

Pony Mail!

Pony Mail!

Pony Mail!

Pony Mail!

CVE Program record

NVD vulnerability detail

No vendor comments have been submitted for this CVE.

### Legacy QID Mappings

- [239471](#) Red Hat Update for OpenShift Container Platform 3.11 (RHSA-2021:2517)
- [239472](#) Red Hat Update for OpenShift Container Platform 4.6.36 (RHSA-2021:2499)
- [239473](#) Red Hat Update for OpenShift Container Platform 4.5.41 (RHSA-2021:2431)
- [6000267](#) Debian Security Update for jetty9 (DLA 3641-1)
- [750448](#) OpenSUSE Security Update for jetty-minimal (openSUSE-SU-2021:0012-1)
- [770073](#) Red Hat OpenShift Container Platform 4.6 Security Update (RHSA-2021:2499)
- [770075](#) Red Hat OpenShift Container Platform 4.5 Security Update (RHSA-2021:2431)
- [770115](#) Red Hat OpenShift Container Platform 4.5 Security Update (RHSA-2021-2431)
- [770123](#) Red Hat OpenShift Container Platform 4.6 Security Update (RHSA-2021-2499)
- [982094](#) Java (maven) Security Update for org.eclipse.jetty:jetty-server (GHSA-86wm-rrjm-8wh8)

© [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](#)**