



# CVE-2023-26049

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

## Summary

<b>CVE</b>	CVE-2023-26049
<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>	2023-04-18 21:15:00 UTC
<b>Updated</b>	2024-02-01 15:36:00 UTC
<b>Description</b>	Jetty is a java based web server and servlet engine. Nonstandard cookie parsing in Jetty may allow an attacker to smuggle

## Risk And Classification

**Problem Types:** CWE-200

## 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
Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	12.0	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>	12.0.0	alpha1	All	All
Application	<a href="#">Eclipse</a>	<a href="#">Jetty</a>	12.0.0	alpha2	All	All
Application	<a href="#">Eclipse</a>	<a href="#">Jetty</a>	12.0.0	alpha3	All	All
Application	<a href="#">Netapp</a>	<a href="#">Active Iq Unified Manager</a>	-	All	All	All
Application	<a href="#">Netapp</a>	<a href="#">Active Iq Unified Manager</a>	-	All	All	All
Application	<a href="#">Netapp</a>	<a href="#">E-series Santricity Os Controller</a>	All	All	All	All
Application	<a href="#">Netapp</a>	<a href="#">E-series Santricity Unified Manager</a>	-	All	All	All
Application	<a href="#">Netapp</a>	<a href="#">E-series Santricity Web Services</a>	-	All	All	All

## References

Reference	Source	Link
Fix/jetty 9.4.x cookie cutter legacy by gregw · Pull Request #9352 · eclipse/jetty.project · GitHub	MISC	<a href="#">github.com</a>
April 2023 Eclipse Jetty Vulnerabilities in NetApp Products   NetApp Product Security	MISC	<a href="#">security.neta</a>

RFC 2965: HTTP State Management Mechanism	MISC	<a href="http://www.rfc-editor.org/rfc/rfc2965">www.rfc-editor.org/rfc/rfc2965</a>
RFC 6265: HTTP State Management Mechanism	MISC	<a href="http://www.rfc-editor.org/rfc/rfc6265">www.rfc-editor.org/rfc/rfc6265</a>
Cookie parsing of quoted values can exfiltrate values from other cookies · Advisory · eclipse/jetty.project · GitHub	MISC	<a href="https://github.com">github.com</a>
[SECURITY] [DLA 3592-1] jetty9 security update	MISC	<a href="https://lists.debian.org">lists.debian.org</a>
Review Cookie Cutter by sbordet · Pull Request #9339 · eclipse/jetty.project · GitHub	MISC	<a href="https://github.com">github.com</a>
Debian -- Security Information -- DSA-5507-1 jetty9	MISC	<a href="http://www.debian.org">www.debian.org</a>
CVE Program record	CVE.ORG	<a href="http://www.cve.org">www.cve.org</a>
NVD vulnerability detail	NVD	<a href="http://nvd.nist.gov">nvd.nist.gov</a>

No vendor comments have been submitted for this CVE.

### Legacy QID Mappings

- [242565](#) Red Hat Update for JBoss Enterprise Application Platform 7.4.1 on RHEL 7 (RHSA-2023:7637)
- [242923](#) Red Hat Update for Satellite 6.14.2 (RHSA-2024:0797)
- [378675](#) Oracle Coherence July 2023 Critical Patch Update (CPUJUL2023)
- [6000122](#) Debian Security Update for jetty9 (DLA 3592-1)
- [6000216](#) Debian Security Update for jetty9 (DSA 5507-1)
- [754107](#) SUSE Enterprise Linux Security Update for jetty-minimal (SUSE-SU-2023:2539-1)

© [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](#)