



# CVE-2022-24721

Published on: Not Yet Published

Last Modified on: 03/25/2022 01:06:00 PM UTC

## CVE-2022-24721 - advisory for GHSA-rjmq-6v55-4rjv

Source: Mitre

Source: NIST

CVE.ORG

Print: PDF

CVSS:31/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:N



Certain versions of [Cometd](#) from [Cometd](#) contain the following vulnerability:

CometD is a scalable comet implementation for web messaging. In any version prior to 5.0.11, 6.0.6, and 7.0.6, internal usage of Oort and Seti channels is improperly authorized, so any remote user could subscribe and publish to those channels. By subscribing to those channels, a remote user may be able to watch cluster-internal traffic that contains other users' (possibly sensitive) data. By publishing to those channels, a remote user may be able to create/modify/delete other user's data and modify the cluster structure. A fix is available in versions 5.0.11, 6.0.6, and 7.0.6. As a workaround, install a custom `SecurityPolicy` that forbids subscription and publishing to remote, non-Oort, sessions on Oort and Seti channels.

CVE-2022-24721 has been assigned by security-advisories@github.com to track the vulnerability - currently rated as **HIGH** severity.

Affected Vendor/Software: **cometd** - **cometd** version < 5.0.11

Affected Vendor/Software: **cometd** - **cometd** version >= 6.0.0, < 6.0.6

Affected Vendor/Software: **cometd** - **cometd** version >= 7.0.0, < 7.0.6

CVSS3 Score: **8.1 - HIGH**

Attack Vector	Attack Complexity	Privileges Required	User Interaction
<b>NETWORK</b>	<b>LOW</b>	<b>LOW</b>	<b>NONE</b>
Scope	Confidentiality Impact	Integrity Impact	Availability Impact
<b>UNCHANGED</b>	<b>HIGH</b>	<b>HIGH</b>	<b>NONE</b>

CVSS2 Score: **5.5 - MEDIUM**

Access Vector	Access Complexity	Authentication
<b>NETWORK</b>	<b>LOW</b>	<b>SINGLE</b>

<b>NETWORK</b>	<b>LOW</b>	<b>SINGLE</b>
<b>Confidentiality Impact</b>	<b>Integrity Impact</b>	<b>Availability Impact</b>
<b>PARTIAL</b>	<b>PARTIAL</b>	<b>NONE</b>

## CVE References

Description	Tags	Link
Improper Authorization in org.cometd.oort · Advisory · cometd/cometd · GitHub	<a href="#">github.com</a> <a href="#">text/html</a>	CONFIRM <a href="https://github.com/cometd/cometd/security/advisories/GHSA-rjmq-6v55-4rjv">github.com/cometd/cometd/security/advisories/GHSA-rjmq-6v55-4rjv</a>
Review Oort/Seti channel usage · Issue #1146 · cometd/cometd · GitHub	<a href="#">github.com</a> <a href="#">text/html</a>	MISC <a href="https://github.com/cometd/cometd/issues/1146">github.com/cometd/cometd/issues/1146</a>

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to [comment@cve.report](mailto:comment@cve.report).

There are currently no QIDs associated with this CVE

## Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Cometd	Cometd	All	All	All	All
cpe:2.3:a:cometd:cometd:*:*:*:*:*:*						

No vendor comments have been submitted for this CVE

## Social Mentions

Source	Title	Posted (UTC)
@CVEreport	CVE-2022-24721 : CometD is a scalable comet implementation for web messaging. In any version prior to 5.0.11, 6.0.6... <a href="https://twitter.com/i/web/status/1...">twitter.com/i/web/status/1...</a>	2022-03-15 13:50:21
/r/netcve	<a href="#">CVE-2022-24721</a>	2022-03-15 14:38:40

[← Previous ID](#)

[Next ID →](#)

© CVE.report 2023 |

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](https://status.cve.report)