



# CVE-2020-10689

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF !\[\]\(e3f8612927870f2e0f9f5989e6dd3064\_img.jpg\)](#)

## Summary

<b>CVE</b>	CVE-2020-10689
<b>State</b>	PUBLIC
<b>Assigner</b>	secalert@redhat.com
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2020-04-03 15:15:00 UTC
<b>Updated</b>	2023-11-07 03:14:00 UTC
<b>Description</b>	A flaw was found in the Eclipse Che up to version 7.8.x, where it did not properly restrict access to workspace pods. An aut

## Risk And Classification

**Problem Types:** NVD-CWE-Other

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	<a href="#">Eclipse</a>	<a href="#">Che</a>	All	All	All	All
Application	<a href="#">Eclipse</a>	<a href="#">Che</a>	All	All	All	All

## References

### Reference

- Improve isolation of Che theia and che-machine-exec components · Issue #15651 · eclipse/che · GitHub
- 1816789 – (CVE-2020-10689) CVE-2020-10689 che: pods in kubernetes cluster can bypass JWT proxy and send unauthenticated requests to
- CVE Program record
- NVD vulnerability detail

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.

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](#)**