

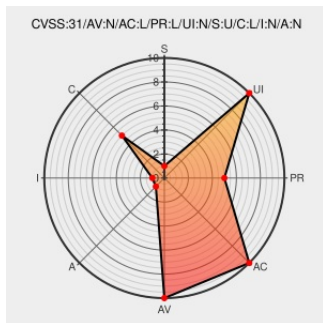


# CVE-2020-4029

Published on: 06/30/2020 12:00:00 AM UTC

Last Modified on: 03/30/2022 01:21:00 PM UTC

## CVE-2020-4029

[Source: Mitre](#)[Source: NIST](#)[CVE.ORG](#)[Print: PDF](#) 

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

The `/rest/project-templates/1.0/createshared` resource in Atlassian Jira Server and Data Center before version 8.5.5, from 8.6.0 before 8.7.2, and from 8.8.0 before 8.8.1 allows remote attackers to enumerate project names via an improper authorization vulnerability.

CVE-2020-4029 has been assigned by [security@atlassian.com](#) to track the vulnerability - currently rated as **MEDIUM** severity.

Affected Vendor/Software: [Atlassian](#) - **Jira Server and Data Center** version < 8.5.5

Affected Vendor/Software: [Atlassian](#) - **Jira Server and Data Center** version >= 8.6.0

Affected Vendor/Software: [Atlassian](#) - **Jira Server and Data Center** version < 8.7.2

Affected Vendor/Software: [Atlassian](#) - **Jira Server and Data Center** version >= 8.8.0

Affected Vendor/Software: [Atlassian](#) - **Jira Server and Data Center** version < 8.8.1

CVSS3 Score: **4.3 - MEDIUM**

| 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>LOW</b>             | <b>NONE</b>         | <b>NONE</b>         |

CVSS2 Score: **4 - MEDIUM**

| Access Vector          | Access Complexity | Authentication      |
|------------------------|-------------------|---------------------|
| <b>NETWORK</b>         | <b>LOW</b>        | <b>SINGLE</b>       |
| Confidentiality Impact | Integrity Impact  | Availability Impact |
|                        |                   |                     |

PARTIAL

NONE

NONE

## CVE References

## Description

## Tags

## Link

[JRASERVER-70926] Improper authorization on /rest/project-templates/1.0/createshared endpoint - CVE-2020-4029 - Create and track feature requests for Atlassian products.

Vendor Advisory  
jira.atlassian.com  
text/html

 MISC  
jira.atlassian.com/browse/JRASERVER-70926

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).

## Related QID Numbers

150379 Atlassian Jira Server Improper authorization (CVE-2020-4029)

## Known Affected Configurations (CPE V2.3)

| Type        | Vendor                    | Product                                   | Version | Update | Edition | Language |
|-------------|---------------------------|-------------------------------------------|---------|--------|---------|----------|
| Application | <a href="#">Atlassian</a> | <a href="#">Jira</a>                      | All     | All    | All     | All      |
| Application | <a href="#">Atlassian</a> | <a href="#">Jira</a>                      | All     | All    | All     | All      |
| Application | <a href="#">Atlassian</a> | <a href="#">Jira Data Center</a>          | All     | All    | All     | All      |
| Application | <a href="#">Atlassian</a> | <a href="#">Jira Server</a>               | All     | All    | All     | All      |
| Application | <a href="#">Atlassian</a> | <a href="#">Jira Software Data Center</a> | All     | All    | All     | All      |
| Application | <a href="#">Atlassian</a> | <a href="#">Jira Software Data Center</a> | All     | All    | All     | All      |

cpe:2.3:a:atlassian:jira:\*:\*:\*:\*:\*:

cpe:2.3:a:atlassian:jira:\*:\*:\*:\*:\*:

cpe:2.3:a:atlassian:jira\_data\_center:\*:\*:\*:\*:\*:

cpe:2.3:a:atlassian:jira\_server:\*:\*:\*:\*:\*:

cpe:2.3:a:atlassian:jira\_software\_data\_center:\*:\*:\*:\*:\*:

cpe:2.3:a:atlassian:jira\_software\_data\_center:\*:\*:\*:\*:\*:

No vendor comments have been submitted for this CVE

## Social Mentions

## Source

## Title

## Posted (UTC)



@RemotelyAlerts

Severity: ?? | The /rest/project-templates/1.0/createsh... | CVE-2020-4029 | Link for more:  
[alerts.remotelyymm.com/CVE-2020-4029](https://alerts.remotelyymm.com/CVE-2020-4029)

2022-03-30  
14:29:50

← 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](#)