



# CVE-2021-26080

Published on: 06/07/2021 12:00:00 AM UTC

Last Modified on: 05/05/2022 03:39:00 PM UTC

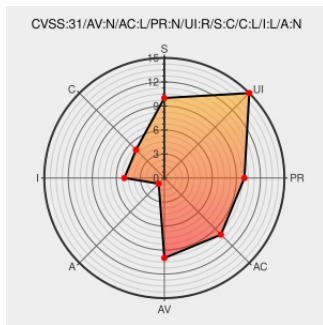
## CVE-2021-26080

[Source: Mitre](#)

[Source: NIST](#)

[CVE.ORG](#)

[Print: PDF](#)



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

EditworkflowScheme.jspa in Jira Server and Jira Data Center before version 8.5.14, and from version 8.6.0 before version 8.13.6, and from 8.14.0 before 8.16.1 allows remote attackers to inject arbitrary HTML or JavaScript via a cross site scripting (XSS) vulnerability.

CVE-2021-26080 has been assigned by [security@atlassian.com](#) to track the vulnerability - currently rated as **MEDIUM** severity.

CVSS3 Score: **6.1 - MEDIUM**

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

CVSS2 Score: **4.3 - MEDIUM**

Access Vector	Access Complexity	Authentication
<b>NETWORK</b>	<b>MEDIUM</b>	<b>NONE</b>
Confidentiality Impact	Integrity Impact	Availability Impact
<b>NONE</b>	<b>PARTIAL</b>	<b>NONE</b>

## CVE References

Description	Tags	Link
[JRASERVER-72432] XSS in Issue Type /editworkflowscheme.jspa - CVE 2021-26080 - Create and track feature requests for Atlassian products.	<a href="#">jira.atlassian.com</a> <a href="#">text/html</a>	<a href="#">MISC</a> <a href="https://jira.atlassian.com/browse/JRASERVER-72432">jira.atlassian.com/browse/JRASERVER-72432</a>

By selecting these links, you may be leaving CVEreport webpage. 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

[150510](#) Atlassian Jira Server Cross Site Scripting (XSS) Vulnerabilities (JRASERVER-72392, JRASERVER-72432)

[730217](#) Atlassian Jira Server and Data Center Cross-Site Scripting (XSS) Vulnerability (JRASERVER-72432)

## Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	<a href="#">Atlassian</a>	<a href="#">Data Center</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

cpe:2.3:a:atlassian:data\_center:\*:\*:\*:\*:\*:\*:

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

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

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

No vendor comments have been submitted for this CVE

## Social Mentions

Source	Title	Posted (UTC)
 @CVEreport	<a href="#">CVE-2021-26080</a> : EditworkflowScheme.jspa in #Jira Server and Jira Data Center before version 8.5.14, and from versi... <a href="https://twitter.com/i/web/status/1...">twitter.com/i/web/status/1...</a>	2021-06-07 22:29:23
 /r/netcve	<a href="#">CVE-2021-26080</a>	2021-06-07 23:41:11

[← 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](#)