



CVE-2021-41304

Published on: 10/26/2021 12:00:00 AM UTC

Last Modified on: 03/30/2022 01:29:00 PM UTC

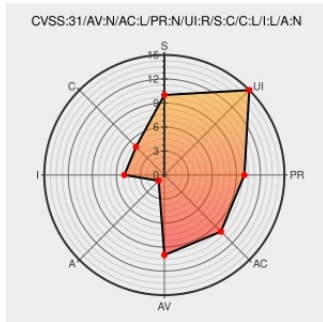
CVE-2021-41304

Source: Mitre

Source: NIST

CVE.ORG

Print: PDF



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

Affected versions of Atlassian Jira Server and Data Center allow anonymous remote attackers to inject arbitrary HTML or JavaScript via a Cross-Site Scripting (XSS) vulnerability in the `/secure/admin/ImporterFinishedPage.jspa` error message. The affected versions are before version 8.13.12, and from version 8.14.0 before

8.20.2.

CVE-2021-41304 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
NETWORK	LOW	NONE	REQUIRED
Scope	Confidentiality Impact	Integrity Impact	Availability Impact
CHANGED	LOW	LOW	NONE

CVSS2 Score: **4.3 - MEDIUM**

Access Vector	Access Complexity	Authentication
NETWORK	MEDIUM	NONE
Confidentiality Impact	Integrity Impact	Availability Impact
NONE	PARTIAL	NONE

CVE References

Description	Tags	Link
[JRASERVER-72939] Reflected XSS <code>/secure/admin/ImporterFinishedPage.jspa</code> via error message - CVE-2021-	jira.atlassian.com text/html	MISC jira.atlassian.com/browse/JRASERVER-

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.

Related QID Numbers

[150463](#) Atlassian Jira Server Cross-Site Scripting Vulnerability (JRASERVER-72939)

[730249](#) Atlassian Jira Server and Data Center Reflected Cross-Site Scripting (XSS) Vulnerability (JRASERVER-72939)

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Atlassian	Data Center	All	All	All	All
Application	Atlassian	Jira	All	All	All	All
Application	Atlassian	Jira Data Center	All	All	All	All
Application	Atlassian	Jira Server	All	All	All	All
Application	Atlassian	Jira Software Data Center	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:*:*:*:*:*:*:

cpe:2.3:a:atlassian:jira_software_data_center:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
 @CVEreport	CVE-2021-41304 : Affected versions of #Atlassian #Jira Server and Data Center allow anonymous remote attackers to i... twitter.com/i/web/status/1...	2021-10-26 04:19:04
 @SecRiskRptSME	RT: CVE-2021-41304 Affected versions of Atlassian Jira Server and Data Center allow anonymous remote attackers to... twitter.com/i/web/status/1...	2021-10-26 07:33:19

[← Previous ID](#)

[Next ID →](#)

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](#)