



CVE-2021-39126

Published on: 10/20/2021 12:00:00 AM UTC

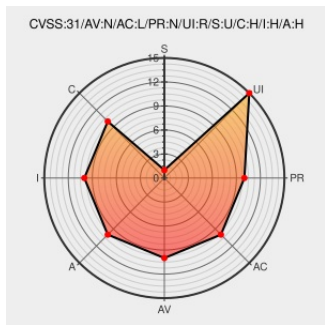
Last Modified on: 10/25/2021 08:42:00 PM UTC

CVE-2021-39126

Source: Mitre

Source: Nist

Print: PDF



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

Affected versions of Atlassian Jira Server and Data Center allow remote attackers to modify various resources via a Cross-Site Request Forgery (CSRF) vulnerability, following an Information Disclosure vulnerability in the referrer headers which discloses a user's CSRF token. The affected versions are before version 8.5.10, and from version 8.6.0 before 8.13.2.

CVE-2021-39126 has been assigned by [security@atlassian.com](#) to track the vulnerability - currently rated as **HIGH** severity.

CVSS3 Score: **8.8 - HIGH**

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	LOW	NONE	REQUIRED
Scope	Confidentiality Impact	Integrity Impact	Availability Impact
UNCHANGED	HIGH	HIGH	HIGH

CVSS2 Score: **6.8 - MEDIUM**

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

CVE References

Description	Tags	Link
[JRASERVER-71806] CSRF token theft through referrer headers - CVE-2021-39126 - Create and track feature requests for Atlassian products.	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

[150438](#) Atlassian Jira Server Multiple Security Vulnerabilities (JRASERVER-72009, JRASERVER-71806, JRASERVER-72003)

[730280](#) Atlassian Jira Server and Data Center Cross-Site Request Forgery (CSRF) Vulnerability (JRASERVER-71806)

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Atlassian	Jira	All	All	All	All
Application	Atlassian	Jira Software Data Center	All	All	All	All
cpe:2.3:a:atlassian:jira:*:*:*:*:*:						
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-2021-39126 : Affected versions of #Atlassian #Jira Server and Data Center allow remote attackers to modify vari... twitter.com/i/web/status/1...	2021-10-21 02:56:30
@ThorstenSiefert	Schon #Update angeworfen? #Atlassian #Jira	2021-10-21 14:19:48
@threatmeter	CVE-2021-39126 Affected versions of Atlassian Jira Server and Data Center allow remote attackers to modify various... twitter.com/i/web/status/1...	2021-10-22 07:09:29

[← Previous ID](#)

[Next ID →](#)

© [CVE.report](#) 2022 [T](#) [N](#) |

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