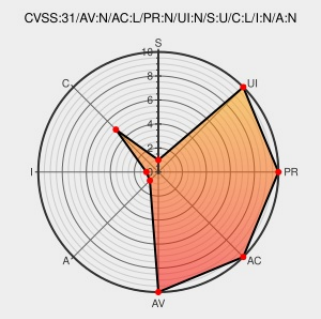
CVE-2020-36286

Published on: 03/31/2021 12:00:00 AM UTC

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

CVE-2020-36286

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Data Center from Atlassian contain the following vulnerability:

The membersOf JQL search function in Jira Server and Data Center before version 8.5.13, from version 8.6.0 before version 8.13.5, and from version 8.14.0 before version 8.15.1 allows remote anonymous attackers to determine if a group exists & members of groups if they are assigned to publicly visible issue field.

CVE-2020-36286 has been assigned by security@atlassian.com to track the vulnerability - currently rated as MEDIUM severity.

CVSS3 Score: 5.3 - MEDIUM

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

CVSS2 Score: 5 - MEDIUM

Access Vector	Access Complexity	Authentication
NETWORK	LOW	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
PARTIAL	NONE	NONE

CVE References

Description	Tags	Link
[JRASERVER-72272] Information Disclosure using JQL function membersOf - CVE-2020-36286 - Create and track feature requests for Atlassian products.	jira.atlassian.com text/html	MISC jira.atlassian.com/browse/JRASERVER-72272

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

730035 Atlassian Jira Server Information Disclosure Vulnerability(JRASERVER-72272)

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

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	CVE-2020-36286 : The membersOf of JQL search function in #Jira Server and Data Center before version 8.5.13, from v… twitter.com/i/web/status/1…	2021-04-01 03:12:08
/r/netcve	CVE-2020-36286	2021-04-01 03:52:06

← 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 registred 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