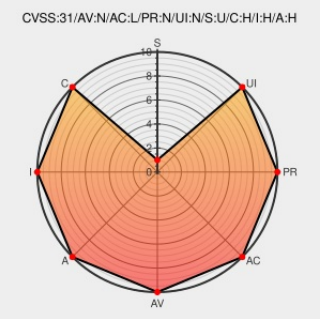
CVE-2019-20409

Published on: 06/23/2020 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:27:50 PM UTC

CVE-2019-20409

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



Certain versions of Jira from Atlassian contain the following vulnerability:

The way in which velocity templates were used in Atlassian Jira Server and Data Center prior to version 8.8.0 allowed remote attackers to gain remote code execution if they were able to exploit a server side template injection vulnerability.

CVE-2019-20409 has been assigned by security@atlassian.com to track the vulnerability - currently rated as CRITICAL severity.

Affected Vendor/Software: **Atlassian** - **Jira Server** version **< 8.8.0**

CVSS3 Score: 9.8 - CRITICAL

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

CVSS2 Score: 7.5 - HIGH

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

CVE References

Description	Tags	Link
[JRASERVER-70944] Make use of Secure Introspector in Velocity Templates - CVE-2019-20409 - Create and track feature requests for Atlassian products.	Issue Tracking Vendor Advisory jira.atlassian.com	MISC jira.atlassian.com/browse/JRASERVER-70944

text/html

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.

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

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

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

← Previous ID

Next ID→