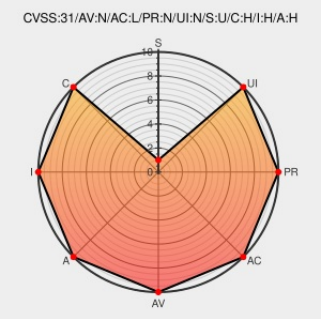
CVE-2020-14172

Published on: 07/02/2020 12:00:00 AM UTC

Last Modified on: 05/03/2022 01:59:00 PM UTC

CVE-2020-14172

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



Certain versions of Jira from Atlassian contain the following vulnerability:

This issue exists to document that a security improvement in the way that Jira Server and Data Center use velocity templates has been implemented. The way in which velocity templates were used in Atlassian Jira Server and Data Center in affected versions allowed remote attackers to achieve remote code execution via insecure deserialization, if they were able to exploit a server side template injection vulnerability. The affected versions are before version 7.13.0, from version 8.0.0 before 8.5.0, and from version 8.6.0 before version 8.8.1.

CVE-2020-14172 has been assigned by security@atlassian.com to track the vulnerability - currently rated as CRITICAL severity.

Affected Vendor/Software: **Atlassian** - **Jira Server** version **< 7.13.0**

Affected Vendor/Software: **Atlassian** - **Jira Server** version **>= 8.0.0**

Affected Vendor/Software: **Atlassian** - **Jira Server** version **< 8.5.0**

Affected Vendor/Software: **Atlassian** - **Jira Server** version **>= 8.6.0**

Affected Vendor/Software: **Atlassian** - **Jira Server** version **< 8.8.1**

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-70940] Template injection in Web Resources Manager - CVE-2020-14172 - Create and track feature requests for Atlassian products.	Permissions Required jira.atlassian.com text/html	MISC jira.atlassian.com/browse/JRASERVER-70940

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

Social Mentions

Source	Title	Posted (UTC)

← Previous ID

Next ID→

CVE.report and Source URL Uptime Status status.cve.report