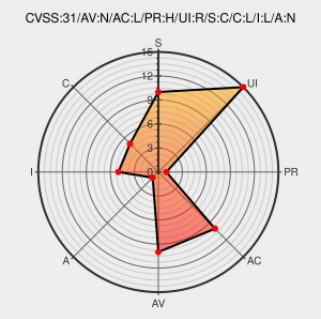
CVE-2020-4025

Published on: 06/30/2020 12:00:00 AM UTC

Last Modified on: 03/30/2022 01:21:00 PM UTC

CVE-2020-4025

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



Certain versions of Jira from Atlassian contain the following vulnerability:

The attachment download resource in Atlassian Jira Server and Data Center The attachment download resource in Atlassian Jira Server and Data Center before 8.5.5, and from 8.6.0 before 8.8.2, and from 8.9.0 before 8.9.1 allows remote attackers to inject arbitrary HTML or JavaScript via a Cross-Site Scripting (XSS) vulnerability issue attachments with a rdf content type.

CVE-2020-4025 has been assigned by security@atlassian.com to track the vulnerability - currently rated as MEDIUM severity.

Affected Vendor/Software: **Atlassian** - **Jira Server and Data Center** version **< 8.5.5**

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

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

Affected Vendor/Software: **Atlassian** - **Jira Server and Data Center** version **>= 8.9.0**

Affected Vendor/Software: **Atlassian** - **Jira Server and Data Center** version **< 8.9.1**

CVSS3 Score: 4.8 - MEDIUM

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

CVSS2 Score: 3.5 - LOW

Access Vector	Access Complexity	Authentication
NETWORK	MEDIUM	SINGLE

Confidentiality Impact	Integrity Impact	Availability Impact
NONE	PARTIAL	NONE

CVE References

Description	Tags	Link
[JRASERVER-71114] XSS in Issue - Attachments - CVE-2020-4025 - Create and track feature requests for Atlassian products.	Vendor Advisory jira.atlassian.com text/html	MISC jira.atlassian.com/browse/JRASERVER-71114

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 Data Center	All	All	All	All
Application	Atlassian	Jira Server	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_data_center:*:*:*:*:*:*:*:*:

cpe:2.3:a:atlassian:jira_server:*:*:*:*:*:*:*:*:

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)
@RemotelyAlerts	Severity: ? | The attachment download resource in Atla... | CVE-2020-4025 | Link for more: alerts.remotelyrmm.com/CVE-2020-4025	2022-03-25 19:30:56

← Previous ID Next ID →

← Previous ID Next ID →