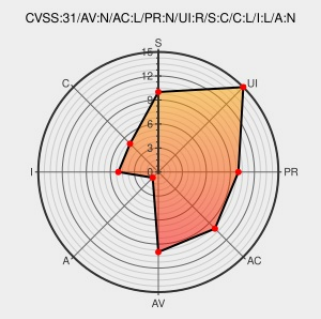
CVE-2020-36236

Published on: 02/14/2021 12:00:00 AM UTC

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

CVE-2020-36236

Source: Mitre | Source: NIST | CVE.ORG | 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 inject arbitrary HTML or JavaScript via a Cross-Site Scripting (XSS) vulnerability in the ViewWorkflowSchemes.jspa and ListWorkflows.jspa endpoints. The affected versions are before version 8.5.11, from version 8.6.0 before 8.13.3, and from version 8.14.0 before 8.15.0.

CVE-2020-36236 has been assigned by security@atlassian.com to track the vulnerability - currently rated as MEDIUM severity.

CVSS3 Score: 6.1 - MEDIUM

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

CVSS2 Score: 4.3 - MEDIUM

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

CVE References

Description	Tags	Link
[JRASERVER-72015] XSS via ViewWorkflowSchemes.jspa, ListWorkflows.jspa - CVE-2020-36236 - Create and track feature requests for	Issue Tracking Vendor Advisory	MISC jira.atlassian.com/browse/JRASERVER-

Atlassian products. jira.atlassian.com 72015 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.

Related QID Numbers

730028 Atlassian Jira Server And Data Center Multiple Vulnerabilities(JRASERVER-72014,JRASERVER-72015,JRASERVER-72064)

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: ?? | Affected versions of Atlassian Jira Serv... | CVE-2020-36236 | Link for more: alerts.remotelyrmm.com/CVE-2020-36236	2022-03-30 14:33:25

← Previous ID Next ID→

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