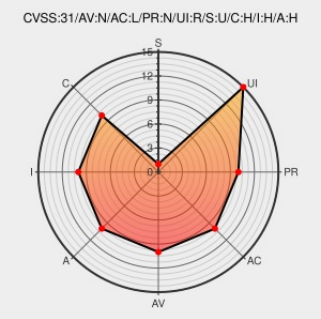
CVE-2017-18113

Published on: 08/01/2021 12:00:00 AM UTC

Last Modified on: 08/10/2021 01:51:00 PM UTC

CVE-2017-18113

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



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

The DefaultOSWorkflowConfigurator class in Jira Server and Jira Data Center before version 8.18.1 allows remote attackers who can trick a system administrator to import their malicious workflow to execute arbitrary code via a Remote Code Execution (RCE) vulnerability. The vulnerability allowed for various problematic OSWorkflow classes to be used as part of workflows. The fix for this issue blocks usage of unsafe conditions, validators, functions and registers that are build-in into OSWorkflow library and other Jira dependencies. Atlassian-made functions or functions provided by 3rd party plugins are not affected by this fix.

CVE-2017-18113 has been assigned by security@atlassian.com to track the vulnerability - currently rated as HIGH severity.

Affected Vendor/Software: **Atlassian** - **Jira Server** version **< 8.18.1**

Affected Vendor/Software: **Atlassian** - **Jira Data Center** version **< 8.18.1**

CVSS3 Score: 8.8 - HIGH

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

CVSS2 Score: 6.8 - MEDIUM

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

PARTIAL	PARTIAL	PARTIAL

CVE References

Description	Tags	Link
[JRASERVER-72660] Remote code execution in workflow import - CVE-2017-18113 - Create and track feature requests for Atlassian products.	jira.atlassian.com text/html	MISC jira.atlassian.com/browse/JRASERVER-72660

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

730148 Atlassian Jira Remote code execution Vulnerability (JRASERVER-72660)

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

cpe:2.3:a:atlassian:data_center:*:*:*:*:*:*:*:*:

cpe:2.3:a:atlassian:jira:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→