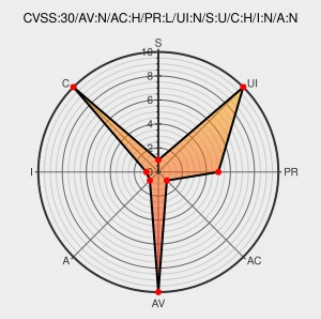
CVE-2017-16865

Published on: 01/17/2018 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:26:39 PM UTC

CVE-2017-16865

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



Certain versions of Jira from Atlassian contain the following vulnerability:

The Trello importer in Atlassian Jira before version 7.6.1 allows remote attackers to access the content of internal network resources via a Server Side Request Forgery (SSRF). When running in an environment like Amazon EC2, this flaw maybe used to access to a metadata resource that provides access credentials and other potentially confidential information.

CVE-2017-16865 has been assigned by security@atlassian.com to track the vulnerability - currently rated as MEDIUM severity.

Affected Vendor/Software: **Atlassian** - **Jira** version **All versions before 7.6.1**

CVSS3 Score: 5.3 - MEDIUM

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

CVSS2 Score: 3.5 - LOW

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

CVE References

Description	Tags	Link

[JRASERVER-66642] Server Side Request Forgery(SSRF) in the Jira Trello importer - CVE-2017-16865 - Create and track feature requests for Atlassian products.	Issue Tracking Vendor Advisory jira.atlassian.com text/html	CONFIRM jira.atlassian.com/browse/JRASERVER-66642

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

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

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

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→