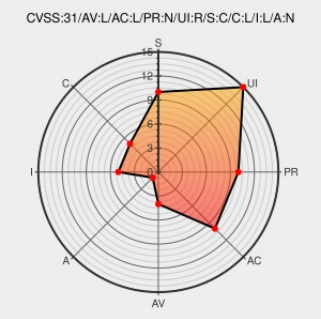
CVE-2021-21371

Published on: 03/10/2021 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:28:57 PM UTC

CVE-2021-21371 - advisory for GHSA-8278-88vv-x98r

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



Certain versions of Jira Cloud from Tenable contain the following vulnerability:

Tenable for Jira Cloud is an open source project designed to pull Tenable.io vulnerability data, then generate Jira Tasks and sub-tasks based on the vulnerabilities' current state. It published in pypi as "tenable-jira-cloud". In tenable-jira-cloud before version 1.1.21, it is possible to run arbitrary commands through the yaml.load() method. This could allow an attacker with local access to the host to run arbitrary code by running the application with a specially crafted YAML configuration file. This is fixed in version 1.1.21 by using yaml.safe_load() instead of yaml.load().

CVE-2021-21371 has been assigned by security-advisories@github.com to track the vulnerability - currently rated as HIGH severity.

Affected Vendor/Software: **tenable** - **integration-jira-cloud** version **< 1.1.21**

CVSS3 Score: 8.6 - HIGH

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

CVSS2 Score: 4.6 - MEDIUM

Access Vector	Access Complexity	Authentication
LOCAL	LOW	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
PARTIAL	PARTIAL	PARTIAL

CVE References

CVE References

Description	Tags	Link
Execution of untrusted code through config file · Advisory · tenable/integration-jira-cloud · GitHub	Third Party Advisory github.com text/html	CONFIRM github.com/tenable/integration-jira-cloud/security/advisories/GHSA-8278-88vv-x98r
switched yaml.load() to yaml.safe_load() to not load serialized pytho… · tenable/integration-jira-cloud@f8c2095 · GitHub	Patch Third Party Advisory github.com text/html	MISC github.com/tenable/integration-jira-cloud/commit/f8c2095fd529e664e7fa25403a0a4a85bb3907d0
tenable-jira-cloud · PyPI	Product Third Party Advisory pypi.org text/html	MISC pypi.org/project/tenable-jira-cloud/
Documentation - PyYAML - DocsForge	Third Party Advisory pyyaml.docsforge.com text/html	MISC pyyaml.docsforge.com/master/documentation/#loading-yaml

Related QID Numbers

982923 Python (pip) Security Update for tenable-jira-cloud (GHSA-8278-88vv-x98r)

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Tenable	Jira Cloud	All	All	All	All

cpe:2.3:a:tenable:jira_cloud:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→