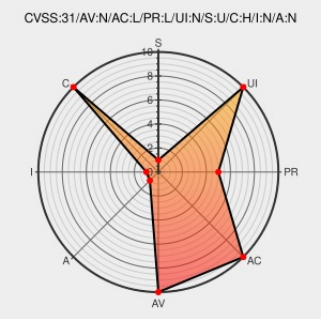
CVE-2019-10459

Published on: 10/23/2019 12:00:00 AM UTC

Last Modified on: 10/25/2023 06:16:00 PM UTC

CVE-2019-10459

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



Certain versions of Mattermost Notification from Jenkins contain the following vulnerability:

Jenkins Mattermost Notification Plugin 2.7.0 and earlier stored webhook URLs containing a secret token unencrypted in its global configuration file and job config.xml files on the Jenkins master where they could be viewed by users with Extended Read permission, or access to the master file system.

CVE-2019-10459 has been assigned by jenkinsci-cert@googlegroups.com to track the vulnerability - currently rated as MEDIUM severity.

Affected Vendor/Software: **Jenkins project** - **Jenkins Mattermost Notification Plugin** version **= 2.7.0 and earlier**

CVSS3 Score: 6.5 - MEDIUM

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

CVSS2 Score: 4 - MEDIUM

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

CVE References

Description	Tags	Link

Jenkins Security Advisory 2019-10-23	Vendor Advisory jenkins.io text/html	CONFIRM jenkins.io/security/advisory/2019-10-23/#SECURITY-1628
oss-security - Multiple vulnerabilities in Jenkins plugins	Mailing List Third Party Advisory www.openwall.com text/html	MLIST [oss-security] 20191023 Multiple vulnerabilities in Jenkins plugins

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Jenkins	Mattermost Notification	All	All	All	All

cpe:2.3:a:jenkins:mattermost_notification:*:*:*:*:*:jenkins:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→