Jira Server for Slack (Official) - 2021-02-17

Communcation by Vendor

Date	17 Feb 2021
Product	Jira Server for Slack (Official)
Vulnerability	Critical
Marketplace link	https://marketplace.atlassian.com/apps/1220099/
Base product	Jira
Vendor	Atlassian

Summary	*CVE-2021-26068 - Remote Code Execution in Jira Server for Slack*
Advisory Release Date	*17 Feb 2021, 10 AM PDT*
Product	*Jira Server for Slack plugin*
Affected Versions	*All versions < 2.0.15*
Fixed Versions	*2.0.15*
CVE ID(s)	*CVE-2021-26068*

Summary of Vulnerability

This advisory discloses a critical severity security vulnerability in Jira Server for Slack plugin. All versions of this plugin up to and including 2.0.14 are affected by this vulnerability. Jira Server and Data Center instances that don't have this plugin installed are NOT affected by this vulnerability. By default, this plugin does not come installed in the Jira server and data center instances. However, if you do have this plugin installed in your server or data center instances, upgrade your app/plugin installations to version 2.0.15 immediately to fix this vulnerability. Also, note that this does NOT affect any Jira cloud instances.

Description

There is a remote code execution vulnerability affecting the Jira Server for Slack plugin that can be potentially exploited by any authenticated Jira user by sending malicious payloads to the affected endpoint. In a successful exploitation of this vulnerability, an attacker could potentially execute arbitrary code on the system.

This issue can be tracked here (currently restricted to Atlassian staff): https://confluence.atlassian.com/pages/viewpage.action?spaceKey=JIRA&title=Jira+Server+for+Slack+Security+Advisory+17th+February+2021&permissionViolation=true

What You Need to Do

Check whether your Jira server/DC instance has the vulnerable plugin installed or not. To do this, go to your applications and search for "Jira Server for Slack" plugin. If it is installed, check the version. If the version is less than 2.0.15, then the instance is vulnerable.

Upgrading the Plugin

Upgrade the plugin to the latest version. Details on how to update apps can be found here.

Mitigation

If you are unable to upgrade the plugin immediately, then as a temporary workaround, you can:

- *Disable the plugin; or*
- *Uninstall the plugin; or*
- *Block the /rest/slack/1.0/message/render endpoint from being accessed. This can be achieved by denying access in the reverse-proxy, load balancer, or Tomcat directly (see instructions).*

For a full description of the latest version of Jira Server for Slack, see the release notes - https://marketplace.atlassian.com/apps/1220099/jira-server-for-slack-official/version-history. You can download the latest version of the plugin from the Atlassian Marketplace.

Recommendation by bitvoodoo

- Upgrade to version 2.0.15 of the app

If you need any assistance please contact our Support Team.