Security Advisory 2022-047

Jira Full-Read SSRF Vulnerability

July 01, 2022 — v1.0

TLP:WHITE

History:

- *01/07/2022 — v1.0 – Initial publication*

Summary

On June 29th, Atlassian published a security advisory for a high severity security vulnerability in Mobile Plugin for Jira Data Center and Server. The vulnerability allows a remote authenticated user to perform a full read server-side request forgery via a batch endpoint. This vulnerability is tracked as **CVE-2022-26135**. Atlassian rates the severity level of this vulnerability as high, according to their published scale (7.0 - 8.9) [1,2].

Technical Details

A full-read server-side request forgery exists in Mobile Plugin for Jira, which is bundled with Jira and Jira Service Management. It is exploitable by any authenticated user (including a user who joined via the sign-up feature). It specifically affects the batch HTTP endpoint used in Mobile Plugin for Jira. It is possible to control the HTTP method and location of the intended URL through the method parameter in the body of the vulnerable endpoint [1].

Products and versions affected

All versions of Jira and Jira Service Management prior to the fixed version listed below are affected by this vulnerability. Jira Cloud and Jira Service Management Cloud are not affected [1].

Jira

- Jira Core Server
- Jira Software Server
- Jira Software Data Center

Versions after 8.0 and before 8.13.22 [1]:

- 8.14.x
- 8.15.x
- 8.16.x
- 8.17.x
- 8.18.x

- 8.19.x
- 8.20.x before 8.20.10
- 8.21.x
- 8.22.x before 8.22.4

Jira Service Management

- Jira Service Management Server
- Jira Service Management Data Center

Versions after 4.0 and before 4.13.22 [1]:

- 4.14.x
- 4.15.x
- 4.16.x
- 4.17.x
- 4.18.x
- 4.19.x
- 4.20.x before 4.20.10
- 4.21.x
- 4.22.x before 4.22.4

Recommendations

Atlassian recommends installing a fixed version of Jira or Jira Service Management to remediate the vulnerability.

Fixed Versions

Jira Core Server, Jira Software Server, and Jira Software Data Center [1]:

- 8.13.x >= 8.13.22
- 8.20.x >= 8.20.10
- 8.22.x >= 8.22.4
- 9.0.0

Jira Service Management Server and Data Center [1]:

- 4.13.x >= 4.13.22
- 4.20.x >= 4.20.10
- 4.22.x >= 4.22.4
- 5.0.0

Workarounds

If you are unable to immediately upgrade Jira or Jira Service Management, then as a temporary workaround, you can manually upgrade Mobile Plugin for Jira Data Center and Server (`com.atlassian.jira.mobile.jira-mobile-rest`) to the version 3.2.15 (compatible with Jira 8.3.x - 8.22.4 and Jira Service Management 4.3.x - 4.22.4) or disable the plugin [1,3,4].

References

[1] https://confluence.atlassian.com/jira/jira-server-security-advisory-29nd-june-2022-1142430667.html

[2] https://www.atlassian.com/trust/security/security-severity-levels

[3] https://marketplace.atlassian.com/apps/1220151/mobile-plugin-for-jira-data-center-and-server?tab=overview&hosting=datacenter

[4] https://confluence.atlassian.com/upm/disabling-and-enabling-apps-273875716.html