Security Advisory 2023-094

Multiple Critical Vulnerabilities in Atlassian Products

December 6, 2023 — v1.0

TLP:CLEAR

History:

- *06/12/2023 — v1.0 – Initial publication*

Summary

On December 5, 2023, Atlassian released several security advisories regarding critical vulnerabilities affecting multiple Atlassian products [1]. The exploitation of these vulnerabilities could lead to Remote Code Execution.

It is recommended to upgrade to a fixed version as soon as possible.

Technical Details

- The vulnerability **CVE-2022-1471** [2], with a CVSS score of 9.8 out 10, lies in the SnakeYaml library. This library's Constructor() class does not restrict types which can be instantiated during deserialisation. Deserialising yaml content provided by an attacker can lead to remote code execution [3].
- The vulnerability **CVE-2023-22522** [4], with a CVSS score of 9.0 out of 10, is a Template Injection vulnerability that would allow an authenticated attacker, including one with anonymous access, to inject unsafe user input into a Confluence page. Using this approach, an attacker is able to achieve RCE on an affected instance.
- The vulnerability **CVE-2023-22523** [5], with a CVSS score of 9.8 out of 10, lies in the Assets Discovery, which can be downloaded via Atlassian Marketplace, and which is a stand-alone network scanning tool that can be used with or without an agent with Jira Service Management Cloud, Data Center or Server. This vulnerability, if exploited, allows an attacker to perform privileged RCE (Remote Code Execution) on machines with the Assets Discovery agent installed. The vulnerability exists between the Assets Discovery application (formerly known as Insight Discovery) and the Assets Discovery agent.
- The vulnerability **CVE-2023-22524** [6], with a CVSS score of 9.6 out of 10, exists in the Atlassian Companion App desktop application for MacOS. An attacker could utilise WebSockets to bypass Atlassian Companion's blocklist and MacOS Gatekeeper to allow the execution of code.

Affected Products

- The vulnerability **CVE-2022-1471** affects the following products:
  - Automation for Jira app (including Server Lite edition)
  - Bitbucket Data Center
  - Bitbucket Server
  - Confluence Data Center
  - Confluence Server
  - Confluence Cloud Migration App
  - Jira Core Data Center
  - Jira Core Server
  - Jira Service Management Data Center
  - Jira Service Management Server
  - Jira Software Data Center
  - Jira Software Server

Please, refer to the Atlassian advisory for the exact version identifiers.

- The vulnerability **CVE-2023-22522** affects:
  - Confluence Data Center 8.6.0, and 8.6.1.
  - Confluence Server versions 4, 5, 6, 7, and 8 (*Please, refer to the Atlassian advisory for the exact version identifiers.*)
- The vulnerability **CVE-2023-22523** affects all versions prior to Assets Discovery 3.2.0-cloud / 6.2.0 data center and server.
- The vulnerability **CVE-2023-22524** affects all versions of the Atlassian Companion App for MacOS before `2.0.0`.

Recommendations

It is recommended applying patches and updates as soon as possible, as per Atlassian advisories [2, 4, 5, 6].

Mitigations

- **CVE-2023-22522**:

If it is not possible to apply the latest fixes, it is recommended to back up the affected instances, and remove them from the Internet until the patch is applied.

- **CVE-2023-22523**:

It is possible to mitigate the vulnerability, until the latest version is applied, by blocking the port used for communication with agents (the default port is 51337). This temporary mitigation is not a replacement for uninstalling the agents.

- **CVE-2023-22524**

If the Atlassian Companion App for MacOS is not showing a fixed version, and it is not possible to patch, one can completely mitigate this vulnerability by uninstalling the Atlassian Companion App.

References

[1] https://confluence.atlassian.com/security/december-2023-security-advisories-overview-1318892103.html

[2] https://confluence.atlassian.com/security/cve-2022-1471-snakeyaml-library-rce-vulnerability-in-multiple-products-1296171009.html

[3] https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-1471

[4] https://confluence.atlassian.com/security/cve-2023-22522-rce-vulnerability-in-confluence-data-center-and-confluence-server-1319570362.html

[5] https://confluence.atlassian.com/security/cve-2023-22523-rce-vulnerability-in-assets-discovery-1319248914.html

[6] https://confluence.atlassian.com/security/cve-2023-22524-rce-vulnerability-in-atlassian-companion-app-for-macos-1319249492.html