



Threat Level

 **Amber**

HiveForce Labs

# THREAT ADVISORY

 **VULNERABILITY REPORT**

## **Atlassian Addresses Critical RCE Flaws**

Date of Publication

December 07, 2023

Admiralty Code

A1

TA Number

TA2023493













# Summary

**First Discovered:** December 05, 2023

**Affected Product:** Confluence, Jira, Bitbucket servers, Atlassian Companion App for MacOS

**Impact:** Four critical vulnerabilities, namely CVE-2023-22522, CVE-2023-22523, CVE-2023-22524, and CVE-2022-1471, have been identified impacting the Confluence, Jira, and Bitbucket servers, along with a companion app for macOS. If successfully exploited, these vulnerabilities could lead to remote code execution, posing a significant security risk.

## CVEs

CVE	NAME	AFFECTED PRODUCTS	ZERO-DAY	CISA	PATCH
CVE-2023-22522	Atlassian Confluence RCE Vulnerability	Confluence Data Center, Confluence Server			
CVE-2023-22523	Atlassian Confluence RCE Vulnerability	Jira Service Management Cloud, Jira Service Management Data Center and Server			
CVE-2023-22524	Atlassian Confluence RCE Vulnerability	Atlassian Companion App for MacOS			
CVE-2022-1471	Atlassian SnakeYAML library RCE Vulnerability	Confluence, Jira, Bitbucket servers			

# Vulnerability Details

## #1

Four critical vulnerabilities, identified as CVE-2023-22522, CVE-2023-22523, CVE-2023-22524, and CVE-2022-1471, have been discovered by Atlassian. These vulnerabilities impact Confluence, Jira, and Bitbucket servers, as well as a companion app for macOS. Successful exploitation of these vulnerabilities could result in remote code execution.

## #2

CVE-2023-22522 the Template Injection vulnerability is a problem where a remote attacker can inject unsafe user input into a Confluence page, execute arbitrary code, and potentially compromise the system, posing a significant security risk.

## #3

The CVE-2023-22523 vulnerability allows an attacker to execute privileged remote code on machines where the Assets Discovery agent is installed. Assets Discovery is a network scanning tool that identifies hardware and software, gathering detailed information for asset management in Jira Service Management.

## #4

The CVE-2023-22524 exposes a security loophole that enables a remote attacker to compromise the affected system that arises due to inadequate access restrictions. An attacker can exploit this vulnerability by deceiving the victim into visiting a specifically crafted website. Through the utilization of WebSockets, the attacker can bypass Atlassian Companion's blocklist and manipulate MacOS Gatekeeper, thereby enabling the execution of malicious code.

## #5

The CVE-2022-1471 vulnerability creates an opportunity for a remote attacker to execute arbitrary code on the targeted system. This vulnerability is rooted in insecure input validation during the processing of serialized data within the Constructor() class of SnakeYaml. By providing specifically crafted YAML content, a remote attacker can exploit this flaw, leading to the execution of arbitrary code on the target system.

## #6

As of now, none of these security issues have been reported as being exploited in the wild. However, given the historical attractiveness of Atlassian products as attack vectors, it is strongly advised that users promptly update affected installations to the patched versions to mitigate potential risks and enhance overall security.

# Vulnerability

CVE ID	AFFECTED PRODUCTS	AFFECTED CPE	CWE ID
CVE-2023-22522	Atlassian Confluence Server: 4.0 - 8.5.3 Confluence Data Center: 4.0 - 8.7.0	cpe:2.3:a:atlassian:atlassian_confluence_server:*:*:*:*:*	CWE-94
CVE-2023-22523	Assets Discovery: before 6.2.0	cpe:2.3:a:atlassian:assets_discovery:*:*:*:*:*	CWE-345
CVE-2023-22524	Atlassian Companion App for MacOS: before 2.0.0	cpe:2.3:a:atlassian:atlassian_companion_app_for_macos:*:*:*:*:*	CWE-284
CVE-2022-1471	Jira Service Management Server: 5.4.0 - 5.11.1 Jira Service Management Data Center: 5.4.0 - 5.11.1 Bitbucket Data Center: 7.17.0 - 8.12.0 Bitbucket Server: 7.17.0 - 8.12.0 Confluence Data Center and Server 6.13.x - 8.3.0	cpe:2.3:a:snakeyaml:project:snakeyaml:*:*:*:*:*	CWE-502, CWE-20

## Recommendations



**Apply Patch:** Install the security patch provided by Atlassian to address the CVE-2023-22522, CVE-2023-22523, CVE-2023-22524, and CVE-2022-1471 RCE vulnerabilities. These patches close the security gap that allows attackers to exploit the vulnerabilities.



**Back up and Isolate your instances:** If you cannot apply the patch immediately, backup your Atlassian instance with a recent, secure backup for any issues during or after the patching process. Temporarily remove your instance from the internet, restricting access to public instances, even with user authentication, to minimize potential attacks.



**Block the default communication Port:** To improve security and data protection, uninstall Assets Discovery agents. Block the default port 51337 for communication with agents as a temporary measure, but uninstalling the agents remains the preferred and more secure option.



**Least Privilege:** Adhere to the idea of "least privilege" by giving users only the essential permissions they need for their tasks. This strategy reduces the effects of vulnerabilities related to privilege escalation.

## Potential MITRE ATT&CK TTPs

<b><u>TA0042</u></b> Resource Development	<b><u>TA0002</u></b> Execution	<b><u>TA0005</u></b> Defense Evasion	<b><u>T1190</u></b> Exploit Public-Facing Application
<b><u>T1588</u></b> Obtain Capabilities	<b><u>T1588.006</u></b> Vulnerabilities	<b><u>T1059</u></b> Command and Scripting Interpreter	<b><u>T1221</u></b> Template Injection
<b><u>T1203</u></b> Exploitation for Client Execution			

## Patch Details

It is recommended to update to the latest version of Atlassian products which addresses CVE-2023-22522, CVE-2023-22523, CVE-2023-22524, and CVE-2022-1471. Atlassian have fixed these vulnerabilities in following versions.

- Confluence Data Center and Server 7.19.17 (LTS), 8.4.5, and 8.5.4 (LTS)
- Jira Service Management Cloud (Assets Discovery) 3.2.0 or later, and Jira Service Management Data Center and Server (Assets Discovery) 6.2.0 or later.
- Atlassian Companion App for MacOS 2.0.0 or later
- Automation for Jira (A4J) Marketplace App 9.0.2, and 8.2.4
- Bitbucket Data Center and Server 7.21.16 (LTS), 8.8.7, 8.9.4 (LTS), 8.10.4, 8.11.3, 8.12.1, 8.13.0, 8.14.0, 8.15.0 (Data Center Only), and 8.16.0 (Data Center Only)
- Confluence Cloud Migration App (CCMA) 3.4.0
- Jira Core Data Center and Server, Jira Software Data Center and Server 9.11.2, 9.12.0 (LTS), and 9.4.14 (LTS)
- Jira Service Management Data Center and Server 5.11.2, 5.12.0 (LTS), and 5.4.14 (LTS)

Patch Link:

<https://www.atlassian.com/software/confluence/download-archives>

<https://www.atlassian.com/software/jira/download-archives>

<https://www.atlassian.com/software/bitbucket/download-archives>

## References

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

<https://confluence.atlassian.com/security/cve-2023-22523-rce-vulnerability-in-assets-discovery-1319248914.html>

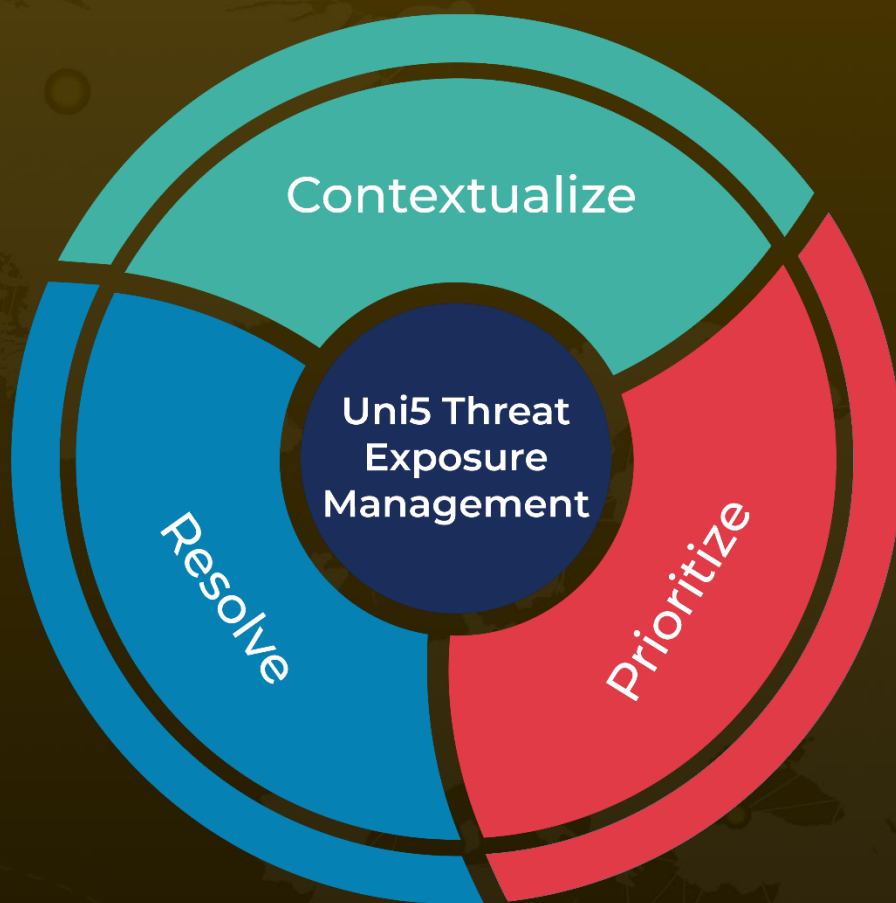
<https://confluence.atlassian.com/security/cve-2023-22524-rce-vulnerability-in-atlassian-companion-app-for-macos-1319249492.html>

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

# What Next?

At Hive Pro, it is our mission to detect the most likely threats to your organization and to help you prevent them from happening.

Book a free demo with HivePro Uni5: Threat Exposure Management Platform.



REPORT GENERATED ON

**December 07, 2023 • 4:10 AM**

© 2023 All Rights are Reserved by Hive Pro®



More at [www.hivepro.com](http://www.hivepro.com)