December 6, 2023

Overall rating: Critical

This notification is intended as an informational bulletin for technical audiences.

Summary

The Vulnerability and Risk Management (VRM) Team is aware that Atlassian published security advisories to address vulnerabilities in multiple products. Included were critical updates for the following:

- Confluence Data Center and Server – multiple versions
- Atlassian Companion App for MacOS – versions prior to 2.0.0
- Assets Discovery – multiple versions
- SnakeYAML library – multiple versions

Exploitation of these vulnerabilities could result in execution of arbitrary code.

Technical Details

This Template Injection vulnerability allows 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 Remote Code Execution (RCE) on an affected instance. Publicly accessible Confluence Data Center and Server versions as listed below are at risk and require immediate attention. See the advisory for additional details Atlassian Cloud sites are not affected by this vulnerability. If your Confluence site is accessed via an atlassian.net domain, it is hosted by Atlassian and is not vulnerable to this issue.

These vulnerabilities are rated as an overall **Critical** Severity.

Recommended Action

- Investigate how your area of responsibility is affected.
- Notify business owner(s) as required.
- *Ensure mitigation is performed at your next change window.*

Please notify VRM with any questions or concerns you may have.

References

- CVE-2023-22522, CVE-2023-22524, CVE-2023-22523, CVE-2022-1471
- SnakeYAML library RCE Vulnerability In Multiple Products
- RCE Vulnerability In Confluence Data Center and Confluence Server
- RCE Vulnerability in Atlassian Companion App for MacOS
- RCE Vulnerability in Assets Discovery

- Atlassian December 2023 Security Advisories