SecurityRisk ADVISORS

Threat Bulletin

Atlassian Confluence Critical Vulnerability

Executive Summary

On June 2nd, 2022, Atlassian released a security advisory acknowledging the remote code execution vulnerability affecting Confluence servers. Currently there are no available patches, and the vulnerability is under active exploit from Chinese threat actors. Atlassian is working on patching the vulnerability and we will continue to update the threat bulletin as more information becomes available.

Affected Products

All supported versions of Confluence Server and Data Center, and Confluence Server and Data Center versions after 1.3.0 are affected.

Safeguards/Recommendations

Atlassian has released fixes for the vulnerability in versions 7.4.17, 7.13.7, 7.14.3, 7.15.2, 7.16.4, 7.17.4 and 7.18. If the fixes cannot be downloaded, it is recommended to restrict access to Confluence Server and Data Center instances from the internet, disable Confluence Server and Data Center instances, or implement a WAF (Web Application Firewall) rule that blocks URLs containing '${ ' to reduce the chances of an attack.

References

https://confluence.atlassian.com/doc/confluence-security-advisory-2022-06-02-1130377146.html

https://www.volexity.com/blog/2022/06/02/zero-day-exploitation-of-atlassian-confluence/

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

Version History

Version 1. Initial Report

Vendor: Atlassian

CVE-ID: CVE-2022-26134

Published: June 2, 2022

CVSS V3 Overall score: TBD

Criticality: Critical

Patch Availability: No

Vulnerability Type:
Remote Code Execution

Exploitability Metrics

Attack Vector: Remote

Attack Complexity: TBD

Privileges Required: TBD

User Interaction: TBD

Impact Metrics

Scope: TBD

Confidentiality: TBD

Integrity: TBD

Availability: TBD

Confidence Metrics

Exploitability: TBD

Remediation Level: Temp Fix

Report Confidence: TBD

Contact Us

24x7 SOC Phone: 215.867.9051
Email: soc@sra.io
Website: https://sra.io