Hive Pro®

Threat Level

Red

HiveForce Labs

THREAT ADVISORY

VULNERABILITY REPORT

Critical RCE Flaw in Atlassian Confluence Sparks Active Exploitation

Date of Publication	Admiralty Code	TA Number
January 24, 2024	A1	TA2024030

Summary

First Seen: January 16, 2024
Affected Platform: Atlassian Confluence
Impact: CVE-2023-22527 is a critical Remote Code Execution vulnerability in outdated Atlassian Confluence versions, actively exploited by malicious actors. Immediate patching to recommended versions is crucial, as nearly 40,000 exploitation attempts have been recorded within three days of disclosure.

CVEs

CVE	NAME	AFFECTED PRODUCT	ZERO -DAY	CISA KEV	PATCH
CVE-2023-22527	Atlassian Confluence Data Center and Server Template Injection Vulnerability	Atlassian Confluence Data Center and Server	✗	✓	✓

Vulnerability Details

#1

CVE-2023-22527 is a critical Remote Code Execution (RCE) vulnerability impacting out-of-date versions of Atlassian Confluence Data Center and Confluence Server. Malicious actors are actively exploiting this flaw, which has a CVSS score of 10.0, allowing unauthenticated attackers to achieve remote code execution.

#2

Affected versions include Confluence Data Center and Server 8 versions released before December 5, 2023, and version 8.4.5. Atlassian recommends immediate patching to the latest version, with versions 8.5.4 and 8.5.5 (LTS) identified as fixes, along with Confluence Data Center versions 8.6.0, 8.7.1, and 8.7.2 for Data Center installations.

#3

Within three days of public disclosure, approximately 40,000 exploitation attempts originating from over 600 unique IP addresses, primarily from Russia, have been recorded. The attackers are conducting testing callback attempts and 'whoami' execution, indicating opportunistic scanning for vulnerable servers. As of January 21, 2024, over 11,000 Atlassian instances are accessible over the internet, and the extent of vulnerability to CVE-2023-22527 remains unknown.

#4

The vulnerability has the potential to allow unauthenticated attackers to inject OGNL expressions, leading to the execution of arbitrary code and system commands. Atlassian has clarified that Atlassian Cloud sites and Confluence sites accessed via an atlassian.net domain hosted by Atlassian are not affected. There are no known workarounds for the vulnerability, and Atlassian emphasizes updating each affected product installation to the latest version as the recommended remediation measure.

Vulnerabilities

CVE ID	AFFECTED PRODUCTS	AFFECTED CPE	CWE ID
CVE-2023-22527	Atlassian Confluence Data Center and Server: 8.0.x 8.1.x 8.2.x 8.3.x 8.4.x 8.5.0-8.5.3	cpe:2.3:a:atlassian:confluence_data_center:*:*:*:*:*:*:*:* cpe:2.3:a:atlassian:confluence_server:*:*:*:*:*:*:*:*	CWE-94

Recommendations

Immediate Patching: Organizations using Atlassian Confluence Data Center and Confluence Server should promptly apply the recommended patches provided by Atlassian. Upgrade to the latest versions (8.5.4 and 8.5.5 for Confluence Data Center and Server) to mitigate the CVE-2023-22527 vulnerability.

Regular Software Updates: Establish a practice of regularly updating software and systems to the latest versions. This ensures that security patches are promptly applied, reducing the risk of exploitation through known vulnerabilities.

Security Audits and Scans: Conduct thorough security audits and vulnerability scans on your IT infrastructure to identify and address any potential weaknesses. Regular scans can help detect vulnerabilities before malicious actors exploit them.

Network Monitoring: Implement comprehensive network monitoring to detect and respond to any unusual or suspicious activities. Pay special attention to unexpected access patterns or connections, as these may indicate attempted exploits.

Potential MITRE ATT&CK TTPs

TA0002 Execution	TA0042 Resource Development	TA0001 Initial Access	TA0005 Defense Evasion
TA0004 Privilege Escalation	T1588.005 Exploits	T1588.006 Vulnerabilities	T1055 Process Injection
T1190 Exploit Public-Facing Application	T1203 Exploitation for Client Execution	T1588 Obtain Capabilities	

Indicators of Compromise (IOCs)

TYPE	VALUE
IPv4	38.150.12[.]131, 38.180.75[.]124, 67.181.73[.]197, 134.122.186[.]223, 38.150.12[.]144, 186.117.138[.]210, 45.61.137[.]90

Patch Details

Upgrade Atlassian Confluence Data Center and Server to 8.5.4 (LTS), 8.5.5 (LTS) or later versions and for Atlassian Confluence Data Center to 8.6.0, 8.7.1, 8.7.2 or later versions

Link:
https://confluence.atlassian.com/security/cve-2023-22527-rce-remote-code-execution-vulnerability-in-confluence-data-center-and-confluence-server-1333990257.html

References

https://blog.projectdiscovery.io/atlassian-confluence-ssti-remote-code-execution/

https://twitter.com/Shadowserver/status/1749372138685915645

https://twitter.com/TheDFIRReport/status/1749066611678466205

https://twitter.com/TheDFIRReport/status/1749424404063232099

https://github.com/Avento/CVE-2023-22527_Confluence_RCE

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.

Contextualize
Uni5 Threat Exposure Management
Prioritize
Resolve

REPORT GENERATED ON

January 24, 2024 • 3:30 AM

© 2024 All Rights are Reserved by Hive Pro ®

More at www.hivepro.com