Hive Pro

Threat Level

Red

THREAT ADVISORY

VULNERABILITY REPORT

A zero-day vulnerability in Atlassian Confluence

Date of Publication	Last Updated Date	Admiralty code	TA Number
3 June 2022	6 June 2022	A1	TA2022112

Summary

The Cybersecurity and Infrastructure Security Agency (CISA) has warned organizations about a new vulnerability in Atlassian's Confluence Server and Data Center. This vulnerability is actively exploited in the wild.

CVEs

CVE	NAME	PATCH
CVE-2022-26134	Unauthenticated remote code execution vulnerability in Confluence Server and Data Center	✓

Potential MITRE ATT&CK TTPs

TA0042 Resource Development	**TA0001** Initial Access	**TA0002** Execution	**T1588** Obtain Capabilities
T1588.006 Obtain Capabilities: Vulnerabilities	**T1190** Exploit Public-Facing Application		

Technical Details

#1 Atlassian Confluence Server and Data Center products has a zero-day vulnerability (CVE-2022-26134). This vulnerability can be exploited by an unauthenticated remote attacker to execute code.

#2 This vulnerability has been fixed it versions 7.4.17, 7.13.7, 7.14.3, 7.15.2, 7.16.4, 7.17.4, and 7.18.1. However, organizations that cannot patch their system can follow the mitigations:

- Restrict access to Confluence Server and Data Center instances from the internet.
- Disable Confluence Server and Data Center instances
- Implement a WAF (Web Application Firewall) rule which blocks URLs containing ${

Vulnerability Details

CVE ID	AFFECTED PRODUCTS	AFFECTED CPE	CWE ID
CVE-2022-26134	All versions of Confluence Server & Confluence Data Center	cpe:2.3:a:atlassian:confluence_server:-:*:*:*:*:*:*:*, cpe:2.3:a:atlassian:confluence_data_center:-:*:*:*:*:*:*:*	CWE-74

Patch Link

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

References

https://www.cisa.gov/uscert/ncas/current-activity/2022/06/02/atlassian-releases-security-updates-confluence-server-and-data

https://jira.atlassian.com/browse/CONFSERVER-79016

What Next?

Book a free demo with **HivePro Uni5** to check your exposure to this advisory. HivePro Uni5 is a Threat Exposure Management Solution that proactively reduces an organization's attack surface before it gets exploited.

At Hive Pro we take a long hard look at your vulnerabilities so you can bolster your defenses and fine-tune your offensive cybersecurity tactics.

REPORT GENERATED ON

3 June 2022, 11:00 AM

© 2022 All Rights are Reserved by HivePro

More at www.hivepro.com