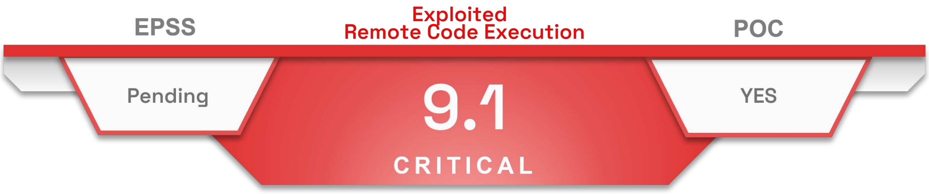
Security for the greater good

Newscast
Critical vulnerability in Atlassian Confluence

2023-11-07 I **TLP:CLEAR** I CERT aDvens - CTI
Advens - 16 Quai de la Mégisserie - 75001 Paris

Table of content

CVE-2023-22518 (Exploited)


EPSS

Pending

Exploited
Remote Code Execution

9.1

CRITICAL

POC

YES

On 31 October 2023, Atlassian published a security bulletin concerning the discovery of a new critical vulnerability in Confluence Data Center and Server. This flaw stems from a failure to control rights in the *WebSudo* feature.

By sending specially crafted requests, a remote, unauthenticated attacker can execute arbitrary commands on the server.

This vulnerability is currently being exploited to deploy the Cerber ransomware.

Type of vulnerability

- CWE-285: Improper Authorization

Risk

- Remote code execution

Severity (Base score CVSS 3.1)

Attack vector	Network	Scope	Unchanged
Attack complexity	Low	Impact on confidentiality	None
Privileges Required	None	Impact on integrity	High
User Interaction	None	Impact on availability	High

Impacted Product

- Atlassian Confluence Data Center and Server

Recommendations

aDvens' CERT recommends testing proposed workaround measures in a test environment before deploying them in production. This step is crucial to prevent any unintended side effects.

- Update Atlassian Confluence Data Center and Server versions 7.19.x and earlier to version 7.19.16.
- Update Atlassian Confluence Data Center and Server versions 7.20.x and later to version 8.3.4, 8.4.4, 8.5.3 or 8.6.1.

If the patch cannot be deployed, it is recommended to disable access to the following endpoints:

- /json/setup-restore.action
- /json/setup-restore-local.action
- /json/setup-restore-progress.action

Additional information is available on the editor's website.

Proof of concept

A proof of concept is available in open source.

Indicators of Compromise

TLP	TYPE	VALUE
TLP:CLEAR	IP	193.176.179.41
TLP:CLEAR	IP	193.43.72.11
TLP:CLEAR	IP	45.145.6.112
TLP:CLEAR	Domain	j3qxmk6g5sk3zw62i2yhjnwmhm55rfz47fdyfkhaithlpelfjdokdxad[.]onion
TLP:CLEAR	MD5 I Artefact	81b760d4057c7c704f18c3f6b3e6b2c4 I /tmp/agttydcb.bat
TLP:CLEAR	SHA256 I Artefact	4ed46b98d047f5ed26553c6f4fded7209933ca9632b998d265870e3557a5cdfe I /tmp/qnetd

Sources

- https://nvd.nist.gov/vuln/detail/CVE-2023-22518
- https://confluence.atlassian.com/security/cve-2023-22518-improper-authorization-vulnerability-in-confluence-data-center-and-server-1311473907.html
- https://jira.atlassian.com/browse/CONFSERVER-93142
- https://www.bleepingcomputer.com/news/security/critical-atlassian-confluence-bug-exploited-in-cerber-ransomware-attacks/