

CVE-2023-22518

Atlassian Confluence Data Center and Server Improper Authorization Vulnerability

Exigent

CISA KEV since Nov 7, 2023

Actively exploited

Ransomware use known

Public exploit module (Metasploit)

All versions of Confluence Data Center and Server are affected by this unexploited vulnerability. This Improper Authorization vulnerability allows an unauthenticated attacker to reset Confluence and create a Confluence instance administrator account. Using this account, an attacker can then perform all administrative actions that are available to Confluence instance administrator leading to – but not limited to – full loss of confidentiality, integrity and availability.

EVRS

94/100

Immediate priority

CVSS V3.1

9.8

Critical · NVD

EPSS

0.999

99.99th percentile · FIRST

CISA DEADLINE

Nov 28, 2023

KEV since 2023 · listed over a year

Signals behind the score

☒ counted in the score ☐ not counted

evidence for 6 of 8 signals

☒ CISA KEV	Listed in the catalog	☐ Vendor exploitation	Confirmed exploitation in the wild
☒ Ransomware	Known ransomware campaigns	☐ KEV recency	On the CISA KEV catalog for over two years
☒ EPSS	0.999 probability	☐ Pre-patch disclosure	Disclosure status unavailable
☒ CVSS	Base score 9.8	☐ Microsoft Exploitability Index	Not a Microsoft CVE

Remediation

Out-of-band / urgent Patch or fixed version identified**CISA required action:** Apply mitigations per vendor instructions or discontinue use of the product if mitigations are unavailable.

Basis: CISA KEV required action

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.

Affected and fixed versions

PACKAGE	AFFECTED	FIXED IN	SOURCE
confluence data center	$\geq 1.0 < 7.19.16$ $\geq 7.20.0 < 8.3.4$ $\geq 8.4.0 < 8.4.4$ $\geq 8.5.0 < 8.5.3$ 8.6.0	7.19.16 · 8.3.4 · 8.4.4 · 8.5.3	NVD
confluence server	$\geq 1.0 < 7.19.16$ $\geq 7.20.0 < 8.3.4$ $\geq 8.4.0 < 8.4.4$ $\geq 8.5.0 < 8.5.3$ 8.6.0	7.19.16 · 8.3.4	NVD



Sources

Vendor guidance	github.com/advisories/GHSA-8prx-84h6-4fr5	Additional guidance	confluence.atlassian.com/pages/viewpage.action?pageId=1311473907
confluence.atlassian.com	confluence.atlassian.com/security/cve-2023-22518-improper-authorization-vulnerability-in-confluence-data-center-and-server-1311473907.html	NVD	nvd.nist.gov/vuln/detail/CVE-2023-22518
CISA KEV	cisa.gov/known-exploited-vulnerabilities-catalog	ENISA EUVD	euvd.enisa.europa.eu/vulnerability/EUVD-2023-26658
Current data	evulnable.com/vulnerability-management/cve/CVE-2023-22518		

Snapshot at generation time. EPSS can move quickly. A public exploit module is not evidence of active exploitation.