CVE-2023-22515

Atlassian Confluence Data Center and Server Broken Access Control Vulnerability

Exigent | CISA KEV since Oct 5, 2023 | Actively exploited | Ransomware use known | Public exploit module (Metasploit)

Atlassian has been made aware of an issue reported by a handful of customers where external attackers may have exploited a previously unknown vulnerability in publicly accessible Confluence Data Center and Server instances to create unauthorized Confluence administrator accounts and access Confluence instances. 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.

EVRS	CVSS V3.1	EPSS	CISA DEADLINE
94/100 Immediate priority	9.8 Critical · NVD	0.992 99.94th percentile · FIRST	Oct 13, 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	0.992 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. Check all affected Confluence instances for evidence of compromise per vendor instructions and report any positive findings to CISA.

Basis: CISA KEV required action

Affected and fixed versions

PACKAGE	AFFECTED	FIXED IN	SOURCE
confluence data center	⩾ 8.0.0 < 8.3.3 ⩾ 8.4.0 < 8.4.3 ⩾ 8.5.0 < 8.5.2	8.3.3 · 8.4.3 · 8.5.2	NVD
confluence server	⩾ 8.0.0 < 8.3.3 ⩾ 8.4.0 < 8.4.3 ⩾ 8.5.0 < 8.5.2	8.3.3 · 8.4.3 · 8.5.2	NVD

Sources

Vendor guidance	github.com/advisories/GHSA-g458-xvmc-qg2r	Additional guidance	confluence.atlassian.com/display/KB/FAQ+for+CVE-2023-22515
confluence.atlassian.com	confluence.atlassian.com/security/cve-2023-22515-privilege-escalation-vulnerability-in-confluence-data-center-and-server-1295682276.html	NVD	nvd.nist.gov/vuln/detail/CVE-2023-22515
CISA KEV	cisa.gov/known-exploited-vulnerabilities-catalog	ENISA EUVD	euvd.enisa.europa.eu/vulnerability/EUVD-2023-26655
Current data	evulnable.com/vulnerability-management/cve/CVE-2023-22515		

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