

CVE-2021-26085

Atlassian Confluence Server Pre-Authorization Arbitrary File Read Vulnerability

CISA KEV since Mar 28, 2022

Actively exploited

Ransomware use known

Affected versions of Atlassian Confluence Server allow remote attackers to view restricted resources via a Pre-Authorization Arbitrary File Read vulnerability in the /s/ endpoint. The affected versions are before version 7.4.10, and from version 7.5.0 before 7.12.3.

EVRS 88/100 Immediate priority	CVSS V3.1 5.3 Medium · NVD	EPSS 0.999 99.97th percentile · FIRST	CISA DEADLINE Apr 18, 2022 KEV since 2022 · 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 5.3	☐ Microsoft Exploitability Index	Not a Microsoft CVE

Remediation

Patch Immediately Patch or fixed version identified

CISA required action: Apply updates per vendor instructions.
Basis: CISA KEV required action

Affected and fixed versions

PACKAGE	AFFECTED	FIXED IN	SOURCE
confluence data center	< 7.4.10 ≥ 7.5.0 < 7.12.3	7.4.10 · 7.12.3	NVD
confluence server	< 7.4.10 ≥ 7.5.0 < 7.12.3	7.4.10 · 7.12.3	NVD

Sources

Vendor guidance	jira.atlassian.com/browse/CONFSERVER-67893	NVD	nvd.nist.gov/vuln/detail/CVE-2021-26085
CISA KEV	cisa.gov/known-exploited-vulnerabilities-catalog	ENISA EUVD	europa.eu/enisa/eu-vulnerability/EUVD-2021-12906
Current data	evulnable.com/vulnerability-management/cve/CVE-2021-26085		

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