

CVE-2024-20767

Adobe ColdFusion Improper Access Control Vulnerability

CISA KEV since Dec 16, 2024

Actively exploited

Public exploit module (Metasploit)

ColdFusion versions 2023.6, 2021.12 and earlier are affected by an Improper Access Control vulnerability that could result in arbitrary file system read. An attacker could leverage this vulnerability to access or modify restricted files. Exploitation of this issue does not require user interaction. Exploitation of this issue requires the admin panel be exposed to the internet.

EVRS 84/100 Urgent priority	CVSS V3.1 7.4 High · NVD	EPSS 0.985 99.92nd percentile · FIRST	CISA DEADLINE Jan 6, 2025 KEV since 2024 · 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	No known ransomware campaign association	☐ KEV recency	Added to CISA KEV within the last two years
☒ EPSS	0.985 probability	☐ Pre-patch disclosure	Disclosure status unavailable
☒ CVSS	Base score 7.4	☐ Microsoft Exploitability Index	Not a Microsoft CVE

Remediation

Patch This Cycle 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

Affected and fixed versions

PACKAGE	AFFECTED	FIXED IN	SOURCE
coldfusion	2021 2023	no fixed version listed	NVD

Sources

Vendor guidance	github.com/advisories/GHSA-r73p-8gx8-7pvg	Additional guidance	helpx.adobe.com/security/products/coldfusion/apsb24-14.html
NVD	nvd.nist.gov/vuln/detail/CVE-2024-20767	CISA KEV	cisa.gov/known-exploited-vulnerabilities-catalog
ENISA EUVD	euvd.enisa.europa.eu/vulnerability/EUVD-2024-18482	Current data	evulnable.com/vulnerability-management/cve/CVE-2024-20767

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