

CVE-2023-29298

Adobe ColdFusion Improper Access Control Vulnerability

CISA KEV since Jul 20, 2023

Actively exploited

Adobe ColdFusion versions 2018u16 (and earlier), 2021u6 (and earlier) and 2023.0.0.330468 (and earlier) are affected by an Improper Access Control vulnerability that could result in a Security feature bypass. An attacker could leverage this vulnerability to access the administration CFM and CFC endpoints. Exploitation of this issue does not require user interaction.

EVRS 84/100 Urgent priority	CVSS V3.1 7.5 High · NVD	EPSS 0.998 99.96th percentile · FIRST	CISA DEADLINE Aug 10, 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	No known ransomware campaign association	☐ KEV recency	On the CISA KEV catalog for over two years
☒ EPSS	0.998 probability	☐ Pre-patch disclosure	Disclosure status unavailable
☒ CVSS	Base score 7.5	☐ 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	2018 2021 2023	no fixed version listed	NVD

Sources

Vendor guidance	github.com/advisories/GHSA-9fcc-rhq3-fh3c	Additional guidance	helpx.adobe.com/security/products/coldfusion/apsb23-40.html
NVD	nvd.nist.gov/vuln/detail/CVE-2023-29298	CISA KEV	cisa.gov/known-exploited-vulnerabilities-catalog
ENISA EUVD	euvd.enisa.europa.eu/vulnerability/EUVD-2023-32873	Current data	evulnable.com/vulnerability-management/cve/CVE-2023-29298

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