

CVE-2023-38203

Adobe ColdFusion Deserialization of Untrusted Data Vulnerability

Exigent

CISA KEV since Jan 8, 2024

Actively exploited

Ransomware use known

Adobe ColdFusion versions 2018u17 (and earlier), 2021u7 (and earlier) and 2023u1 (and earlier) are affected by a Deserialization of Untrusted Data vulnerability that could result in Arbitrary code execution. Exploitation of this issue does not require user interaction.

EVRS 93 /100 Immediate priority	CVSS V3.1 9.8 Critical · NVD	EPSS 0.971 99.89th percentile · FIRST	CISA DEADLINE Jan 29, 2024 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	Known ransomware campaigns	☐ KEV recency	On the CISA KEV catalog for over two years
☒ EPSS	0.971 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

Affected and fixed versions

PACKAGE	AFFECTED	FIXED IN	SOURCE
coldfusion	2018 2021 2023	no fixed version listed	NVD

Sources

Vendor guidance	helpx.adobe.com/security/products/coldfusion/apsb23-41.html	NVD	nvd.nist.gov/vuln/detail/CVE-2023-38203
CISA KEV	cisa.gov/known-exploited-vulnerabilities-catalog	ENISA EUVD	euvd.enisa.europa.eu/vulnerability/EUVD-2023-42023
Current data	evulnable.com/vulnerability-management/cve/CVE-2023-38203		

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