

CVE-2025-49542

ColdFusion versions 2025.2, 2023.14, 2021.20 and earlier are affected by a reflected Cross-Site Scripting (XSS) vulnerability. If an unauthenticated attacker is able to convince a victim to visit a URL referencing a vulnerable page, malicious JavaScript content may be executed within the context of the victim's browser, scope is changed. The vulnerable component is restricted to internal IP addresses.

EVRS 8/100 Routine priority	CVSS V3.1 5.2 Medium · NVD	EPSS 0.013 70.8th percentile · FIRST	CISA DEADLINE — No CISA deadline
---	--	--	---

Signals behind the score

☒ counted in the score ☐ not counted evidence for 3 of 8 signals

☐ CISA KEV	Not currently CISA KEV-listed	☐ Vendor exploitation	Active-exploitation status not yet checked - scored at the population base rate (none) until known
☐ Ransomware	Ransomware association unavailable	☐ KEV recency	CISA KEV listing date unavailable
☒ EPSS	0.013 probability	☐ Pre-patch disclosure	Disclosure status unavailable
☒ CVSS	Base score 5.2	☐ Microsoft Exploitability Index	Not a Microsoft CVE

Remediation

Monitor Vendor advisory available; patch status is not confirmed

Review the vendor advisory to confirm the affected versions, available update, and any supported workaround or mitigation.

Basis: NVD vendor advisory

Affected and fixed versions

PACKAGE	AFFECTED	FIXED IN	SOURCE
coldfusion	2021 2023 2025	no fixed version listed	NVD

Sources

Vendor guidance helpx.adobe.com/security/products/coldfusion/apsb25-69.html

NVD nvd.nist.gov/vuln/detail/CVE-2025-49542

ENISA EUVD euvd.enisa.europa.eu/vulnerability/EUVD-2025-20700

Current data evulnable.com/vulnerability-management/cve/CVE-2025-49542

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