CVE-2025-49541

ColdFusion versions 2025.2, 2023.14, 2021.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a high-privileged attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field, scope is changed. The vulnerable component is restricted to internal IP addresses.

EVRS	CVSS V3.1	EPSS	CISA DEADLINE
7/100 Routine priority	4.3 Medium · NVD	0.009 58.8th percentile · FIRST	— 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
☐ **Ransomware**	Ransomware association unavailable
☑ **EPSS**	0.009 probability
☑ **CVSS**	Base score 4.3
☐ **Vendor exploitation**	Active-exploitation status not yet checked - scored at the population base rate (none) until known
☐ **KEV recency**	CISA KEV listing date unavailable
☐ **Pre-patch disclosure**	Disclosure status unavailable
☐ **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

ENISA EUVD euvd.enisa.europa.eu/vulnerability/EUVD-2025-20705

NVD nvd.nist.gov/vuln/detail/CVE-2025-49541

Current data evulnable.com/vulnerability-management/cve/CVE-2025-49541

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