CVE-2009-3960

Adobe BlazeDS Information Disclosure Vulnerability

CISA KEV since Mar 7, 2022 | Actively exploited | Ransomware use known | Public exploit module (Metasploit)

Unspecified vulnerability in BlazeDS 3.2 and earlier, as used in LiveCycle 8.0.1, 8.2.1, and 9.0, LiveCycle Data Services 2.5.1, 2.6.1, and 3.0, Flex Data Services 2.0.1, and ColdFusion 7.0.2, 8.0, 8.0.1, and 9.0, allows remote attackers to obtain sensitive information via vectors that are associated with a request, and related to injected tags and external entity references in XML documents.

EVRS	CVSS V3.1	EPSS	CISA DEADLINE
87/100 Immediate priority	6.5 Medium · NVD	0.901 99.8th percentile · FIRST	Sep 7, 2022 KEV since 2022 · 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	0.901 probability	− Pre-patch disclosure	Disclosure status unavailable
✓ CVSS	Base score 6.5	− Microsoft Exploitability Index	Not a Microsoft CVE

Remediation

Patch Immediately — No patch reported by the connected remediation source

CISA required action: Apply updates per vendor instructions.

Basis: CISA KEV required action

Affected and fixed versions

PACKAGE	AFFECTED	FIXED IN	SOURCE
blazeds	≤ 3.2	after 3.2	NVD
coldfusion	7.0.2 8.0 8.0.1 9.0	no fixed version listed	NVD
flex data services	2.0.1	no fixed version listed	NVD
livecycle	8.0.1 8.2.1 9.0	no fixed version listed	NVD
livecycle data services	2.5.1 2.6.1 3.0	no fixed version listed	NVD

Sources

Vendor guidance exploit-db.com/exploits/41855/

CISA KEV cisa.gov/known-exploited-vulnerabilities-catalog

Current data evulnable.com/vulnerability-management/cve/CVE-2009-3960

NVD nvd.nist.gov/vuln/detail/CVE-2009-3960

ENISA EUVD euvd.enisa.europa.eu/vulnerability/EUVD-2009-3931

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