

CVE-2016-3088

Apache ActiveMQ Improper Input Validation Vulnerability

Exigent

CISA KEV since Feb 10, 2022

Actively exploited

Public exploit module (Metasploit)

The Fileserver web application in Apache ActiveMQ 5.x before 5.14.0 allows remote attackers to upload and execute arbitrary files via an HTTP PUT followed by an HTTP MOVE request.

EVRS

87/100

Immediate priority

CVSS V3.1

9.8

Critical · NVD

EPSS

0.985

99.92nd percentile · FIRST

CISA DEADLINE

Aug 10, 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	No known ransomware campaign association	☐ KEV recency	On the CISA KEV catalog for over two years
☒ EPSS	0.985 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 updates per vendor instructions.

Basis: CISA KEV required action

Affected and fixed versions

PACKAGE	AFFECTED	FIXED IN	SOURCE
org.apache.activemq:activemq-client	≥ 5.0.0, < 5.14.0	5.14.0	GitHub
activemq	≥ 5.0.0 < 5.14.0	no fixed version listed	NVD

Sources

Vendor guidance	lists.apache.org/thread.html/a859563f05f7c31916b3178c2697165bd9bbf5a65d1cf62aef27d2%40%3Ccommits.activemq.apache.org%3E	Additional guidance	lists.apache.org/thread.html/r6d03e45b81eab03580cf7f8bb51cb3e9a1b10a2cc0c6a2d3cc92ed0c%40%3Cannounce.apache.org%3E
NVD	nvd.nist.gov/vuln/detail/CVE-2016-3088	CISA KEV	cisa.gov/known-exploited-vulnerabilities-catalog
GitHub advisory	github.com/advisories/GHSA-rxqh-fc23-gxp2	ENISA EUVD	euvd.enisa.europa.eu/vulnerability/EUVD-2022-5255
Current data	evulnable.com/vulnerability-management/cve/CVE-2016-3088		

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