

CVE-2023-46604

Apache ActiveMQ Deserialization of Untrusted Data Vulnerability

Exigent

CISA KEV since Nov 2, 2023

Actively exploited

Ransomware use known

Public exploit module (Metasploit)

The Java OpenWire protocol marshaller is vulnerable to Remote Code Execution. This vulnerability may allow a remote attacker with network access to either a Java-based OpenWire broker or client to run arbitrary shell commands by manipulating serialized class types in the OpenWire protocol to cause either the client or the broker (respectively) to instantiate any class on the classpath. Users are recommended to upgrade both brokers and clients to version 5.15.16, 5.16.7, 5.17.6, or 5.18.3 which fixes this issue.

EVRS

94/100

Immediate priority

CVSS V3.1

9.8

Critical · NVD

EPSS

0.999

99.97th percentile · FIRST

CISA DEADLINE

Nov 23, 2023

KEV since 2023 · 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	0.999 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
org.apache.activemq:activemq-client	< 5.15.16	5.15.16	GitHub
org.apache.activemq:activemq-client	≥ 5.16.0, < 5.16.7	5.16.7	GitHub
org.apache.activemq:activemq-client	≥ 5.17.0, < 5.17.6	5.17.6	GitHub
org.apache.activemq:activemq-client	≥ 5.18.0, < 5.18.3	5.18.3	GitHub
org.apache.activemq:activemq-openwire-legacy	≥ 5.8.0, < 5.15.16	5.15.16	GitHub
org.apache.activemq:activemq-openwire-legacy	≥ 5.16.0, < 5.16.7	5.16.7	GitHub
org.apache.activemq:activemq-openwire-legacy	≥ 5.17.0, < 5.17.6	5.17.6	GitHub
org.apache.activemq:activemq-openwire-legacy	≥ 5.18.0, < 5.18.3	5.18.3	GitHub

PACKAGE	AFFECTED	FIXED IN	SOURCE
activemq	$< 5.15.16$ $\geq 5.16.0 < 5.16.7$ $\geq 5.17.0 < 5.17.6$ $\geq 5.18.0 < 5.18.3$	no fixed version listed	NVD
activemq legacy openwire module	$< 5.15.16$ $\geq 5.16.0 < 5.16.7$ $\geq 5.17.0 < 5.17.6$ $\geq 5.18.0 < 5.18.3$	no fixed version listed	NVD
e-series santricity unified manager	–	no fixed version listed	NVD
e-series santricity web services proxy	–	no fixed version listed	NVD
santricity storage plugin	–	no fixed version listed	NVD
debian linux	10.0 11.0	no fixed version listed	NVD

Sources

Vendor guidance github.com/advisories/GHSA-crg9-44h2-xw35

Additional guidance activemq.apache.org/security-advisories.data/CVE-2023-46604-announcement.txt

NVD nvd.nist.gov/vuln/detail/CVE-2023-46604

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

ENISA EUVD euvd.enisa.europa.eu/vulnerability/EUVD-2023-2719

Current data evulnable.com/vulnerability-management/cve/CVE-2023-46604

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