



Apache ActiveMQ Deserialization of Untrusted Data Vulnerability

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF](#)

Summary

CVE	CVE-2023-46604
State	PUBLIC
Assigner	security@apache.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2023-10-27 15:15:00 UTC
Updated	2023-11-20 22:15:00 UTC
Description	Apache ActiveMQ is vulnerable to Remote Code Execution. The vulnerability may allow a remote attacker with network access to execute arbitrary code on the target system.

Risk And Classification

EPSS: 0.944360000 probability, percentile 0.999870000 (date 2026-04-01)

CISA KEV: Listed on 2023-11-02; due 2023-11-23; ransomware use Known

Problem Types: CWE-502

CISA Known Exploited Vulnerability

Vendor	Apache
Product	ActiveMQ
Name	Apache ActiveMQ Deserialization of Untrusted Data Vulnerability
Required Action	Apply mitigations per vendor instructions or discontinue use of the product if mitigations are unavailable.
Notes	https://activemq.apache.org/security-advisories.data/CVE-2023-46604-announcement.txt ; https://nvd.nist.gov/vuln/detail/CVE-2023-46604

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Apache	Activemq	All	All	All	All
Application	Apache	Activemq Legacy Openwire Module	All	All	All	All

References

Reference
oss-security - CVE-2023-46604: Apache ActiveMQ, Apache ActiveMQ Legacy OpenWire Module: Unbounded deserialization causes ActiveMQ
oss-security - CVE-2023-46604: Apache ActiveMQ, Apache ActiveMQ Legacy OpenWire Module: Unbounded deserialization causes ActiveMQ

oss-security - CVE-2023-46604: Apache ActiveMQ, Apache ActiveMQ Legacy Openwire module: Unbounded deserialization causes ActiveMQ

[CVE-2023-46604 Apache ActiveMQ Vulnerability in NetApp Products | NetApp Product Security](#)

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

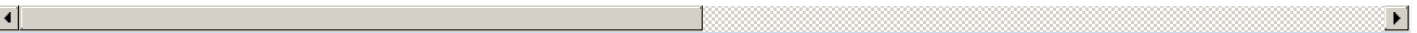
lists.debian.org/debian-lts-announce/2023/11/msg00013.html

packetstormsecurity.com/files/175676/Apache-ActiveMQ-Unauthenticated-Remote-Code-Exec...

[CVE Program record](#)

[NVD vulnerability detail](#)

[CISA Known Exploited Vulnerabilities catalog](#)



No vendor comments have been submitted for this CVE.

Legacy QID Mappings

[150757](#) Apache ActiveMQ Remote Code Execution (RCE) Vulnerability (CVE-2023-46604)

[379060](#) Apache ActiveMQ Remote Code Execution (RCE) Vulnerability

[379516](#) IBM Sterling Secure Proxy Multiple Vulnerabilities (7142038)

[6000335](#) Debian Security Update for activemq (DLA 3657-1)

[730963](#) Apache ActiveMQ Remote Code Execution (RCE) Vulnerability (CVE-2023-46604)

[731042](#) Atlassian Bamboo Server and Data Center Remote Code Execution (RCE) Vulnerability (CVE-2023-46604)

[995775](#) Java (Maven) Security Update for org.apache.activemq:activemq-client (GHSA-crg9-44h2-xw35)

© [CVE.report](#) 2026 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

CVE.report and Source URL Uptime Status status.cve.report