



# Apache ActiveMQ Client, Apache ActiveMQ Broker, Apache ActiveMQ All, Apache ActiveMQ Web, Apache ActiveMQ: Improper Limitation of a Pathname to a Restricted Classpath Directory

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

## Summary

<b>CVE</b>	CVE-2026-33227
<b>State</b>	PUBLISHED
<b>Assigner</b>	apache
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2026-04-07 09:16:20 UTC
<b>Updated</b>	2026-04-08 16:16:23 UTC
<b>Description</b>	Improper validation and restriction of a classpath path name vulnerability in Apache ActiveMQ Client, Apache ActiveMQ Bro

## Risk And Classification

**Primary CVSS:** v3.1 4.3 MEDIUM from ADP

**CVSS:** 3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:N/A:N

**EPSS:** 0.000360000 probability, percentile 0.104380000 (date 2026-04-07)

**Problem Types:** CWE-22 | CWE-22 CWE-22 Improper input validation for resource loading

Version	Source	Type	Score	Severity	Vector
3.1	ADP	DECLARED	4.3	MEDIUM	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:N/A:N
3.1	134c704f-9b21-4f2e-91b3-4a467353bcc0	Secondary	4.3	MEDIUM	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:N/A:N

## CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

Low

User Interaction

None

Scope

Unauthenticated

Unchanged

Confidentiality

Low

Integrity

None

Availability

None

CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:N/A:N

### Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	<a href="#">Apache Software Foundation</a>	<a href="#">Apache ActiveMQ Client</a>	affected 5.19.3 semver	Not specified
CNA	<a href="#">Apache Software Foundation</a>	<a href="#">Apache ActiveMQ Client</a>	affected 6.0.0 6.2.2 semver	Not specified
CNA	<a href="#">Apache Software Foundation</a>	<a href="#">Apache ActiveMQ Broker</a>	affected 5.19.3 semver	Not specified
CNA	<a href="#">Apache Software Foundation</a>	<a href="#">Apache ActiveMQ Broker</a>	affected 6.0.0 6.2.2 semver	Not specified
CNA	<a href="#">Apache Software Foundation</a>	<a href="#">Apache ActiveMQ All</a>	affected 5.19.3 semver	Not specified
CNA	<a href="#">Apache Software Foundation</a>	<a href="#">Apache ActiveMQ All</a>	affected 6.0.0 6.2.2 semver	Not specified
CNA	<a href="#">Apache Software Foundation</a>	<a href="#">Apache ActiveMQ Web</a>	affected 5.19.3 semver	Not specified
CNA	<a href="#">Apache Software Foundation</a>	<a href="#">Apache ActiveMQ Web</a>	affected 6.0.0 6.2.2 semver	Not specified
CNA	<a href="#">Apache Software Foundation</a>	<a href="#">Apache ActiveMQ</a>	affected 5.19.3 semver	Not specified
CNA	<a href="#">Apache Software Foundation</a>	<a href="#">Apache ActiveMQ</a>	affected 6.0.0 6.2.2 semver	Not specified

### References

Reference	Source	Link
<a href="https://activemq.apache.org/security-advisories.data/CVE-2026-33227-announcement.txt">activemq.apache.org/security-advisories.data/CVE-2026-33227-announcement.txt</a>	<a href="mailto:security@apache.org">security@apache.org</a>	<a href="https://activemq.apache.org/">activemq.ap</a>
<a href="https://www.openwall.com/lists/oss-security/2026/04/06/4">www.openwall.com/lists/oss-security/2026/04/06/4</a>	af854a3a-2127-422b-91ae-364da2661108	<a href="https://www.openwall.com/">www.openv</a>
CVE Program record	CVE.ORG	<a href="https://www.cve.or">www.cve.or</a>
NVD vulnerability detail	NVD	<a href="https://nvd.nist.gov">nvd.nist.gov</a>

### Vendor Comments And Credit

Discovery Credit

**CNA:** Dawei Wang (en)

There are currently no legacy QID mappings associated with this CVE.

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](#).

**Free CVE JSON API** [cve.report/api](https://cve.report/api)

**CVE.report and Source URL Uptime Status** [status.cve.report](https://status.cve.report)