Apache Artemis, Apache ActiveMQ Artemis: Auth bypass for Core downstream federation

MITRE | NVD | CVE.ORG | JSON API | Print: PDF

Summary

CVE	CVE-2026-27446
State	PUBLISHED
Assigner	apache
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-03-04 09:15:56 UTC
Updated	2026-05-12 13:17:33 UTC
Description	Missing Authentication for Critical Function (CWE-306) vulnerability in Apache Artemis, Apache ActiveMQ Artemis. An unau

Risk And Classification

Primary CVSS: v4.0 9.3 CRITICAL from security@apache.org

CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:H/VI:H/VA:L/SC:L/SI:L/SA:L/E:X/CR:X/IR:X/AR:X/MAV:X/MAC:X/MAT:X/MPR:X/MUI:X/MVC:X/MVI:X/MVA:X/MSC:X/MSI:X/MSA:X/S:X/AU:X/R:X/V:X/RE:X/U:X

Problem Types: CWE-306 | CWE-306 CWE-306 Missing Authentication for Critical Function

Version	Source	Type	Score	Severity	Vector
4.0	security@apache.org	Secondary	9.3	CRITICAL	CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:H/VI:H/VA:L/SC:L/SI:L/SA:L/E:X
4.0	CNA	CVSS	9.3	CRITICAL	CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:H/VI:H/VA:L/SC:L/SI:L/SA:L
3.1	nvd@nist.gov	Primary	9.8	CRITICAL	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

CVSS v4.0 Breakdown

Attack Vector

Network

Attack Complexity

Low

Attack Requirements

None

Privileges Required

None

User Interaction

None

Confidentiality

High

ntegrity

High

vailability

Low

Sub Conf.

Low

Sub Integrity

Low

Sub Availability

Low

CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:H/VI:H/VA:L/SC:L/SI:L/SA:L/E:X/CR:X/IR:X/AR:X/MAV:X/MAC:X/MAT:X/MPR:X/MUI:X/MVC:X/MVI:X/MVA:X/MSC:X/MSI:X/MSA:X/S:X/AU:X/R:X/V:X/RE:X/U:X

CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

None

User Interaction

None

Scope

Unchanged

Confidentiality

High

ntegrity

High

Availability

High

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

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Apache	Activemq Artemis	All	All	All	All
Application	Apache	Artemis	2.50.0	All	All	All

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Apache Software Foundation	Apache Artemis	affected 2.50.0 2.51.0 semver	Not specified

CNA	Apache Software Foundation	Apache ActiveMQ Artemis	affected 2.11.0 2.44.0 semver	Not specified
ADP	Siemens	Opcenter RDnL	affected * custom	Not specified

References

Reference	Source	Link	Tags
www.openwall.com/lists/oss-security/2026/03/04/1	af854a3a-2127-422b-91ae-364da2661108	www.openwall.com	Mailing
www.openwall.com/lists/oss-security/2026/03/03/4	af854a3a-2127-422b-91ae-364da2661108	www.openwall.com	Mailing
cert-portal.siemens.com/productcert/html/ssa-085541.html	0b142b55-0307-4c5a-b3c9-f314f3fb7c5e	cert-portal.siemens.com	
lists.apache.org/thread/jwpsdc8tdxotm98od8n8n30fqlzoc8gg	security@apache.org	lists.apache.org	Mailing
CVE Program record	CVE.ORG	www.cve.org	canoni
NVD vulnerability detail	NVD	nvd.nist.gov	canoni

Vendor Comments And Credit

Discovery Credit

CNA: Hardik Mehta <mehtahardik@proton.me> (en)

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