Apache ActiveMQ, Apache ActiveMQ All Module, Apache ActiveMQ MQTT Module: MQTT control packet remaining length field is not properly validated

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

Summary

CVE	CVE-2025-66168
State	PUBLISHED
Assigner	apache
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-03-04 09:15:54 UTC
Updated	2026-04-10 11:16:21 UTC
Description	WARNING: Users of 6.x should upgrade to 6.2.4 or later as the fix was missed in previous 6.x releases. See the following f

Risk And Classification

Primary CVSS: v3.1 8.8 HIGH from nvd@nist.gov

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

EPSS: 0.000690000 probability, percentile 0.211220000 (date 2026-04-15)

Problem Types: CWE-190 | CWE-190 CWE-190 Integer Overflow or Wraparound

Version	Source	Type	Score	Severity	Vector
3.1	nvd@nist.gov	Primary	8.8	HIGH	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H
3.1	security@apache.org	Secondary	5.4	MEDIUM	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:L/A:N
3.1	CNA	CVSS	5.4	MEDIUM	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:L/A:N

CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

Low

User Interaction

None

Scope

Unchanged

Unchanged

Confidentiality

High

Integrity

High

Availability

High

CVSS:3.1/AV:N/AC:L/PR:L/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	All	All	All	All
Application	Apache	Activemq	6.2.0	All	All	All
Application	Apache	Activemq	All	All	All	All

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Apache Software Foundation	Apache ActiveMQ	affected 5.19.2 semver	Not specified
CNA	Apache Software Foundation	Apache ActiveMQ	affected 6.0.0 6.1.9 semver	Not specified
CNA	Apache Software Foundation	Apache ActiveMQ	affected 6.2.0 6.2.1 semver	Not specified
CNA	Apache Software Foundation	Apache ActiveMQ All Module	affected 5.19.2 semver	Not specified
CNA	Apache Software Foundation	Apache ActiveMQ All Module	affected 6.0.0 6.1.9 semver	Not specified
CNA	Apache Software Foundation	Apache ActiveMQ All Module	affected 6.2.0 6.2.1 semver	Not specified
CNA	Apache Software Foundation	Apache ActiveMQ MQTT Module	affected 5.19.2 semver	Not specified
CNA	Apache Software Foundation	Apache ActiveMQ MQTT Module	affected 6.0.0 6.1.9 semver	Not specified
CNA	Apache Software Foundation	Apache ActiveMQ MQTT Module	affected 6.2.0 6.2.1 semver	Not specified

References

Reference	Source	Link
activemq.apache.org/security-advisories.data/CVE-2026-40046-announcement.txt	security@apache.org	activemq.ap
www.openwall.com/lists/oss-security/2026/03/03/5	af854a3a-2127-422b-91ae-364da2661108	www.openw
www.cve.org/CVERecord	security@apache.org	www.cve.or
lists.apache.org/thread/13n8mkrb2jf2y6yyhpgrkmpqcm7djyto	security@apache.org	lists.apache
CVE Program record	CVE.ORG	www.cve.or
NVD vulnerability detail	NVD	nvd.nist.gov

Vendor Comments And Credit

Discovery Credit

CNA: Gai Tanaka <641.work123@gmail.com> (en)

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