

CVE-2023-33246

Apache RocketMQ Command Execution Vulnerability

Exigent CISA KEV since Sep 6, 2023 Actively exploited Public exploit module (Metasploit)

For RocketMQ versions 5.1.0 and below, under certain conditions, there is a risk of remote command execution. Several components of RocketMQ, including NameServer, Broker, and Controller, are leaked on the extranet and lack permission verification, an attacker can exploit this vulnerability by using the update configuration function to execute commands as the system users that RocketMQ is running as. Additionally, an attacker can achieve the same effect by forging the RocketMQ protocol content.

EVRS 86/100 Immediate priority	CVSS V3.1 9.8 Critical · NVD	EPSS 0.966 99.88th percentile · FIRST	CISA DEADLINE Sep 27, 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	No known ransomware campaign association	☐ KEV recency	On the CISA KEV catalog for over two years
☒ EPSS	0.966 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

To prevent these attacks, users are recommended to upgrade to version 5.1.1 or above for using RocketMQ 5.x or 4.9.6 or above for using RocketMQ 4.x.

Affected and fixed versions

PACKAGE	AFFECTED	FIXED IN	SOURCE
org.apache.rocketmq:rocketmq-broker	≥ 5.0.0, < 5.1.1	5.1.1	GitHub
org.apache.rocketmq:rocketmq-namesrv	≥ 4.0.0, < 4.9.6	4.9.6	GitHub
org.apache.rocketmq:rocketmq-namesrv	≥ 5.0.0, < 5.1.1	5.1.1	GitHub
org.apache.rocketmq:rocketmq-controller	≥ 5.0.0, < 5.1.1	5.1.1	GitHub
rocketmq	< 4.9.6 ≥ 5.0.0 < 5.1.1	4.9.6 · 5.1.1	NVD

Sources

Vendor guidance github.com/advisories/GHSA-x3cq-8f32-5f63

NVD nvd.nist.gov/vuln/detail/CVE-2023-33246

ENISA EUVD euvd.enisa.europa.eu/vulnerability/EUVD-2023-2175

Additional guidance lists.apache.org/thread/1s8j2c8kogthtpv3060yddk03zq0pxyp
CISA KEV cisa.gov/known-exploited-vulnerabilities-catalog
Current data evaluable.com/vulnerability-management/cve/CVE-2023-33246

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