مجلس الأمن السيبراني
CYBER SECURITY COUNCIL

United Arab Emirates

Actively Exploited Apache ActiveMQ Vulnerability

Tracking #:432318801

Date:17-04-2026

THE INFORMATION CONTAINED WITHIN IS THE PROPERTY OF THE CYBER SECURITY COUNCIL OF THE UNITED ARAB EMIRATES GOVERNMENT AND IS TO BE USED EXCLUSIVELY FOR INTELLGIENCE PURPOSES. IT MAY NOT BE USED IN ANY LEGAL OR PUBLIC MATTER WITHOUT THE EXPLICIT APPROVAL OF THE CYBER SECURITY COUNCIL

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed a vulnerability affecting Apache ActiveMQ has been added to the Known Exploited Vulnerabilities (KEV) Catalog, indicating confirmed active exploitation in the wild.

TECHNICAL DETAILS:

A critical vulnerability, CVE-2026-34197, has been added to the Known Exploited Vulnerabilities (KEV) Catalog, confirming active exploitation in the wild. This vulnerability affects Apache ActiveMQ and enables authenticated remote code execution (RCE) due to improper input validation and unsafe handling of broker configuration parameters.

Vulnerability Details:

- **CVE ID:** CVE-2026-34197
- **Severity:** Important (High impact due to RCE potential)
- **Vulnerability Type:**
  - Improper Input Validation
  - Code Injection (CWE-94)
- **Vulnerability Description**
  - The issue resides in the Jolokia JMX-HTTP bridge exposed at: /api/jolokia/
- Root Cause
  - Default Jolokia access policies allow execution (exec) operations on all ActiveMQ MBeans.
  - Sensitive methods exposed:
  - BrokerService.addNetworkConnector(String)
  - BrokerService.addConnector(String)

Affected Products:

- Apache ActiveMQ Broker:
  - Versions before 5.19.4
  - Versions 6.0.0 to 6.2.2
- Apache ActiveMQ (all-in-one distribution):
  - Versions before 5.19.4
  - Versions 6.0.0 to 6.2.2

Fixed Versions:

- 5.19.4 or later
- 6.2.3 or later

RECOMMENDATIONS:

- **Patch Immediately**:
  - Upgrade urgently to patched versions.

Kindly circulate this information to your subsidiaries and partners as well as share with us any relevant information and findings.

The UAE Cyber Security Council extends its appreciation for the continued collaboration.

REFERENCES:

- https://activemq.apache.org/security-advisories.data/CVE-2026-34197-announcement.txt