مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Multiple Vulnerabilities in Apache ActiveMQ

Tracking #:432319060

Date:03-06-2026

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed Multiple vulnerabilities in Apache ActiveMQ allow authenticated attackers to achieve remote code execution through the Jolokia management interface and bypass previous security fixes.

TECHNICAL DETAILS:

Multiple vulnerabilities in Apache ActiveMQ allow authenticated attackers to achieve remote code execution through the Jolokia management interface and bypass previous security fixes. Successful exploitation may result in complete compromise of the ActiveMQ broker, unauthorized administrative actions, and disruption of enterprise messaging services.

Vulnerability Details

1. CVE-2026-42588 – Remote Code Execution via Jolokia addNetworkConnector- Base Score: 8.1 HIGH
2. CVE-2026-45505 – Jolokia Discovery Wrapper Bypass- Base Score: 8.8 HIGH
3. CVE-2026-42253 – Header Injection- Base Score: 6.1 MEDIUM
4. CVE-2026-49157 – Privilege Management Weakness- Base Score: 8.8 HIGH

Affected Versions

- Apache ActiveMQ Broker (org.apache.activemq:activemq-broker) before 5.19.7
- Apache ActiveMQ Broker (org.apache.activemq:activemq-broker) 6.0.0 before 6.2.6
- Apache ActiveMQ All (org.apache.activemq:activemq-all) before 5.19.7
- Apache ActiveMQ All (org.apache.activemq:activemq-all) 6.0.0 before 6.2.6
- Apache ActiveMQ (org.apache.activemq:apache-activemq) before 5.19.7
- Apache ActiveMQ (org.apache.activemq:apache-activemq) 6.0.0 before 6.2.6

Fixed Version

- Apache ActiveMQ 5.19.7 or 6.2.6

RECOMMENDATIONS:

Organizations should upgrade to fixed versions immediately and restrict access to management interfaces.

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://lists.apache.org/thread/ns0zktfo16s9ql2mmtqtlb6p6xcs45xm
- https://lists.apache.org/thread/7n97nddyw96w6ykldjv1h40jx86xdo0w
- https://lists.apache.org/thread/rrcsf6s90hj4tdh89nvkko75q5505rj8