مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Multiple Vulnerabilities in Apache ActiveMQ

Tracking #:432318844

Date:27-04-2026

TLP: WHITE

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed Multiple Vulnerabilities in Apache ActiveMQ that could allow authenticated attackers to execute arbitrary code on the broker's JVM and perform cross-site scripting (XSS) attacks via the web console.

TECHNICAL DETAILS:

Vulnerability Details

- **CVE-2026-41044 – RCE via Improper Broker Name Validation**
  - **Severity:** High
  - An authenticated attacker can bypass broker name validation in the admin web console by injecting a malicious broker name containing an xbean binding. When a VM transport is created, the broker references this name, triggering the loading of a remote Spring XML application context.
    This leads to arbitrary code execution on the JVM through Spring bean instantiation mechanisms such as Runtime.exec().
- **CVE-2026-40466 – RCE via Jolokia HTTP Discovery Transport**
  - **Severity:** High
  - This vulnerability allows attackers to bypass prior mitigations by leveraging the Jolokia interface. An attacker can configure an HTTP Discovery transport that points to a malicious endpoint, which returns a crafted VM transport.
    This results in remote loading of a Spring XML configuration and subsequent execution of arbitrary code on the broker.
- **CVE-2026-41043 – Cross-Site Scripting (XSS) in Web Console**
  - **Severity:** Medium
  - An authenticated attacker can inject malicious HTML into a JMS selector field in the ActiveMQ Web Console. By manipulating the response content type to HTML, the application renders and executes the malicious script when accessed by an administrator.
    Successful exploitation may lead to session hijacking or further compromise of administrative accounts.

Fixed Versions

- Apache ActiveMQ 5.19.6 or later
- Apache ActiveMQ 6.2.5 or later

RECOMMENDATIONS:

The UAE Cyber Security Council recommends updating the affected versions to the fixed or latest versions released by Apache ActiveMQ.

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://www.tenable.com/cve/CVE-2026-40466
- https://www.tenable.com/cve/CVE-2026-41043
- https://www.tenable.com/cve/CVE-2026-41044