Post Date: 2026/05/13

Vulnerability Alert High-Risk Security Vulnerability in Apache ActiveMQ Classic (CVE-2026-34197), Please Verify and Patch Immediately

- Subject: Vulnerability Alert High-Risk Security Vulnerability in Apache ActiveMQ Classic (CVE-2026-34197), Please Verify and Patch Immediately

- Description:
  - Forwarded from National Information Sharing and Analysis Center (NISAC) Security Alert: NISAC-200-202604-00000011
  - Researchers have discovered Improper Input Validation and Code Injection vulnerabilities in Apache ActiveMQ Classic (CVE-2026-34197). Due to the Jolokia JMX-HTTP interface exposed by the Web Console allowing specific operations and lacking input validation, an authenticated remote attacker can pass malicious parameters to execute arbitrary code. This vulnerability has already been exploited by hackers; please verify and patch immediately.
- Affected Platforms:
  - Apache ActiveMQ Broker versions prior to 5.19.4
  - Apache ActiveMQ Broker versions 6.0.0 to 6.2.3 (exclusive)
  - Apache ActiveMQ versions prior to 5.19.4
  - Apache ActiveMQ versions 6.0.0 to 6.2.3 (exclusive)
- Recommended Actions:
  - Official fix updates have been released for this vulnerability. Please refer to the official announcement for updates at the following URL: https://activemq.apache.org/security-advisories.data/CVE-2026-34197-announcement.txt
- Reference Materials:
  1. https://nvd.nist.gov/vuln/detail/CVE-2026-34197
  2. https://activemq.apache.org/security-advisories.data/CVE-2026-34197-announcement.txt

---

Computer and Communication Center
Network Systems Division