Posted Date: 2025/10/23

[Vulnerability Alert] Apache ActiveMQ NMS AMQP has a high-risk security vulnerability (CVE-2025-54539), please confirm and patch as soon as possible

- Subject: [Vulnerability Alert] Apache ActiveMQ NMS AMQP has a high-risk security vulnerability (CVE-2025-54539), please confirm and patch as soon as possible
- Content:
  - Forwarded from National Information Security Information Sharing and Analysis Center NISAC-200-202510-00000201
  - Researchers have discovered a Deserialization of Untrusted Data vulnerability (CVE-2025-54539) in the Apache ActiveMQ NMS AMQP client. An unauthenticated remote attacker can execute arbitrary code on the client by returning specially crafted serialized data when the affected client establishes a connection with an untrusted AMQP server. Please confirm and patch as soon as possible.
- Affected Platforms:
  - Apache ActiveMQ NMS AMQP versions up to and including 2.3.0
- Recommended Measures:
  - Please update Apache ActiveMQ NMS AMQP to version 2.4.0 or later (inclusive).
- References:
  1. https://nvd.nist.gov/vuln/detail/CVE-2025-54539
  2. https://lists.apache.org/thread/9k684j07ljrshy3hxwhj5m0xjmkz1g2n

---

Computer and Communications Center
Network Systems Group