安全通告

关于 Apache ActiveMQ Jolokia REST API 存在未授权访问漏洞的预警通报

发布日期：2024-7-18

[2024]017 号

漏洞描述

2024 年 7 月 18 日监测发现 Apache ActiveMQ Jolokia REST API 存在未授权访问漏洞（CVE-2024-32114），Apache ActiveMQ 是基于 Java Message Service (JMS)的开源消息中间件。该漏洞是由于未对 Jolo kia JMX REST API 和 Message REST API 进行身份校验，未授权的攻击者可利用暴露通过 Jolokia JMX REST API 与消息代理进行交互，或者使用 Message REST API 发送和接收消息，甚至清除或删除消息队列和主题。

漏洞编号

CVE-2024-32114

漏洞危害

攻击者可利用暴露通过 Jolokia JMX REST API 与消息代理进行交互，或者使用 Message REST API 发送和接收消息，甚至清除或删除消息队列和主题。

漏洞等级

高危

受影响版本

6.0.0 <= Apache ActiveMQ < 6.12

修复方案

目前官方已经发布了解决此漏洞的相关补丁，建议受影响用户升级至安全版本。

参考链接

https://activemq.apache.org/security-advisories.data/CVE-2024-32114-announcement.txt