Vulnerability in Apache ActiveMQ

Severity Level: High

Components Affected

- Apache ActiveMQ 5.18.0 before 5.18.3
- Apache ActiveMQ 5.17.0 before 5.17.6
- Apache ActiveMQ 5.16.0 before 5.16.7
- Apache ActiveMQ before 5.15.16
- Apache ActiveMQ Legacy OpenWire Module 5.18.0 before 5.18.3
- Apache ActiveMQ Legacy OpenWire Module 5.17.0 before 5.17.6
- Apache ActiveMQ Legacy OpenWire Module 5.16.0 before 5.16.7
- Apache ActiveMQ Legacy OpenWire Module 5.8.0 before 5.15.16

Overview

A vulnerability have been identified in the Apache ActiveMQ, where a remote attacker could actively exploited this vulnerability that enables remote code execution.

Description

This vulnerability has been identified and tracked under CVE-2023-46604. The Java OpenWire protocol marshaller is vulnerable to Remote Code Execution. This vulnerability may allow a remote attacker with network access to either a Java-based OpenWire broker or client to run arbitrary shell commands by manipulating serialized class types in the OpenWire protocol to cause either the client or the broker (respectively) to instantiate any class on the classpath.

Impact

- Remote Code Execution

Solution/ Workarounds

It is recommended to upgrade both brokers and clients to version 5.15.16, 5.16.7, 5.17.6, or 5.18.3.

Reference

- https://thehackernews.com/2023/11/kinsing-hackers-exploit-apache-activemq.html
- https://activemq.apache.org/components/classic/security

Disclaimer

The information provided herein is on an "as is" basis, without warranty of any kind.