November 2, 2023

Overall rating: Critical

BRITISH COLUMBIA

This notification is intended as an informational bulletin for technical audiences.

Summary

On October 26, 2023, Apache published security advisories to address vulnerabilities in multiple products. Included were updates for the following:

- ActiveMQ 5.18 – versions prior to 5.18.3
- ActiveMQ 5.17 – versions prior to 5.17.6
- ActiveMQ 5.16 – versions prior to 5.16.7
- ActiveMQ – versions prior to 5.15.16
- ActiveMQ Legacy OpenWire Module 5.18 – versions prior to 5.18.3
- ActiveMQ Legacy OpenWire Module 5.17 – versions prior to 5.17.6
- ActiveMQ Legacy OpenWire Module 5.16 – versions prior to 5.16.7
- ActiveMQ Legacy OpenWire Module 5.8 – versions prior to 5.15.16

Open source has reported that CVE-2023-46604 has been exploited. Successful exploitation of this vulnerability can permit remote code execution to a threat actor.

Technical Details

Apache ActiveMQ is vulnerable to Remote Code Execution. The vulnerability may allow a remote attacker with network access to a broker to run arbitrary shell commands by manipulating serialized class types in the OpenWire protocol to cause the broker to instantiate any class on the classpath.

Users are recommended to upgrade to version 5.15.16, 5.16.7, 5.17.6, or 5.18.3, which fixes this issue.

This vulnerability is rated as a **Critical** Severity.

Recommended Action

- Investigate how your area of responsibility is affected.
- Notify business owner(s) as required.
- *Ensure mitigation is performed at your next change window.*

Please notify VRM with any questions or concerns you may have.

References

- Apache security advisory – AMQ-9370

- CVE-2023-46604
- Apache Security Advisories

Please note that we will be transitioning to a new site on August 31, 2023, where we will post the vulnerability reports.

You will be able to find all the reports that we have published as well as all future reports here: Cybersecurity Alerts