Overall rating: High

BRITISH COLUMBIA

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

Summary

The Vulnerability and Risk Management (VRM) Team is aware the RocketMQ NameServer component still has a remote command execution vulnerability as the CVE-2023-33246 issue was not completely fixed in version 5.1.1.

Technical Details

When NameServer addresses are leaked on the extranet and lack permission verification, an attacker can exploit this vulnerability by using the update configuration function on the NameServer component to execute commands as the system users that RocketMQ is running as. It is recommended for users to upgrade their NameServer version to 5.1.2 or above for RocketMQ 5.x or 4.9.7 or above for RocketMQ 4.x to prevent these attacks.

This vulnerability is rated as a **High** 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

- CVE-2023-37582
- http://www.openwall.com/lists/oss-security/2023/07/12/1
- https://lists.apache.org/thread/m614czxtpvlztd7mfgcs2xcsg36rdbnc
- https://rocketmq.apache.org/
- https://issues.apache.org/jira/browse/https://github.com/apache/rocketmq/pull/6843