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 mod_jk component of Apache Tomcat Connectors in some circumstances, such as when a configuration included "JkOptions + Forward Directories" did not provide explicit mounts for all possible proxied requests, mod_jk would use an implicit mapping and map the request to the first defined worker.

Technical Details

Such an implicit mapping could result in the unintended exposure of the status worker and/or bypass security constraints configured in httpd. As of JK 1.2.49, the implicit mapping functionality has been removed and all mappings must now be via explicit configuration. Only mod_jk is affected by this issue. The ISAPI redirector is not affected. This issue affects Apache Tomcat Connectors (mod_jk only): from 1.2.0 through 1.2.48. Users are recommended to upgrade to version 1.2.49, which fixes the issue.

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-2023-41081
- https://lists.apache.org/thread/rd1r26w7271jyqgzr4492tooyt583d8b
- http://www.openwall.com/lists/oss-security/2023/09/13/2
- https://lists.debian.org/debian-lts-announce/2023/09/msg00027.html