REMEDIATION REPORT

RIPPLE LABS INC.

SIDE CHAINS SECURITY ASSESSMENT 2023 — XRP

OCTOBER 6, 2023

This engagement was performed in accordance with the Statement of Work, and the procedures were limited to those described in that agreement. The findings and recommendations resulting from the assessment are provided in the attached report. Given the time-boxed scope of this assessment and its reliance on client-provided information, the findings in this report should not be taken as a comprehensive listing of all security issues.

This report is intended solely for the information and use of Ripple Labs Inc.

Bishop Fox Contact Information:
+1 (480) 621-8967
contact@bishopfox.com
8240 S. Kyrene Road
Suite A-113
Tempe, AZ 85284

REMEDIATION TEST SUMMARY

On September 26, 2023, Bishop Fox began performing remediation validation testing for the XRP portion of the Ripple — Side Chains Security Assessment 2023 engagement. The objective was to confirm that the identified findings were successfully remediated. Please refer to Appendix A for detailed remediation status explanations.

The following table summarizes the remediation status of vulnerabilities outlined in `Ripple - Side Chains Security Assessment 2023 - Assessment Report - 20230615.pdf` as of September 29, 2023. Per Bishop Fox's remediation testing policy, informational findings were not retested and are not included in this report.

	SEVERITY	FINDING ID	VULNERABILITY	STATUS
Hybrid Application Assessment	Medium	1	Insufficient Binary Hardening	Remediated
		2	Vulnerable Software	Partially Remediated
	Low	3	Authentication Check without Constant Time	Remediated
		4	Insecure Network Transmission	Remediated
	Informational*	5	Insecure Software Configuration	Partially Remediated
	Low	6	Undefined Behavior	Remediated
		7	Unnecessary Code	Remediated

*Due to partial remediation, the risk rating of this finding was downgraded from low to informational.

REMEDIATION TEST DETAILS

The following information details the results of the remediation validation testing performed by the Bishop Fox assessment team.

Hybrid Application Assessment

1 INSUFFICIENT BINARY HARDENING — MEDIUM

Details

This finding has been retested and successfully resolved.

2 VULNERABLE SOFTWARE — MEDIUM

Definition

Vulnerable software exists when an application has not been updated with the latest security patches. These insecure versions of software can contain issues (e.g., arbitrary remote code execution or SQL injection) that could allow a malicious user to gain elevated access to the application itself or its supporting infrastructure.

Details

The assessment team originally discovered 17 instances of vulnerable software. The team retested this finding and found that ten of the original instances have been successfully remediated. There are seven remaining instances that have not yet been remediated.

Affected Locations

For a full list of affected dependencies, please see the attached spreadsheet.

3 AUTHENTICATION CHECK WITHOUT CONSTANT TIME — LOW

Details

This finding has been retested and successfully resolved.

4 INSECURE NETWORK TRANSMISSION

LOW

Details

This finding has been retested and successfully resolved.

5 INSECURE SOFTWARE CONFIGURATION

INFORMATIONAL

Definition

Insecure software configuration occurs when applications and infrastructure are configured in a manner that is inconsistent with industry best practices. These misconfigurations could allow unauthorized access to affected systems, the disclosure of sensitive information, and the exposure of critical application logs.

Details

The assessment team originally identified multiple software configuration issues including an absence of integrity checks on downloaded software as well as a lack of downgraded permissions on docker images at runtime. During remediation testing, the team discovered that issues related to missing integrity checks within the Docker builds had been mitigated which reduced the number of affected locations from eight to four. However, the issues related to downgraded user permissions had not been addressed.

* Due to the mitigations introduced and the limited benefit from introducing downgraded permissions, the assessment team reduced the risk of this finding from low to informational.

Affected Locations

Affected Files

- `rippled-docker/ubuntu-22.04/Dockerfile`
- `rippled-docker/ubuntu-21.10/Dockerfile`
- `rippled-docker/ubuntu-20.04/Dockerfile`
- `rippled-docker/ubuntu-18.04/Dockerfile`

6 UNDEFINED BEHAVIOR

LOW

Details

This finding has been retested and successfully resolved.

7 UNNECESSARY CODE

LOW

Details

This finding has been retested and successfully resolved.

APPENDIX A — REMEDIATION STATUS DEFINITIONS

The assessment team used the following criteria to rate the findings in this report.

Remediation Rating

Remediated	A finding with a “Remediated” status indicates that the finding’s remediation efforts have been validated and that the affected systems/applications are no longer vulnerable to the issue as detailed in the original assessment report.
Not Remediated	A finding with a “Not Remediated” status indicates that the finding remains unresolved and is still vulnerable to the attack methods outlined in the original assessment report.
Partially Remediated	A finding with a “Partially Remediated” status indicates that some instances of the finding have been resolved or partially resolved. This occurs when there are multiple instances of a vulnerability (e.g., SQL injection) and only some of those instances have been remediated or when the client has implemented a solution that partially resolves the issues. This also occurs when the team finds additional instances introduced as unintended consequences of ongoing remediation efforts.
Unknown	A finding with an “Unknown” status indicates that the team was unable to test a finding or that the client asked the team not to retest the finding. In some cases, findings cannot be retested if they are contingent on other findings or if changes to the environment have affected the ability to retest.