REMEDIATION REPORT

RIPPLE LABS INC.

SIDE CHAINS SECURITY ASSESSMENT 2023 — EVM

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 EVM 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 - EVM - 20230724.pdf` as of September 29, 2023.

	SEVERITY	FINDING ID	VULNERABILITY	STATUS
Hybrid Application Assessment	Medium	1	Arbitrary Code Execution	Remediated
		2	Arbitrary Command Injection	Not Remediated
		3	Vulnerable Software	Partially Remediated
	Informational*	4	Insecure Network Transmission	Partially Remediated
		5	Insecure SSL/TLS Configuration	Partially Remediated
	Low	6	Insecure Software Configuration	Remediated
	Informational*	7	Missing Security Headers	Partially Remediated
	Low	8	Outdated Software	Partially Remediated
		9	Sensitive Information Disclosure	Partially Remediated
	Informational*	10	Weak Content Security Policy (CSP)	Partially Remediated
	Low	11	Weak Cryptography	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 ARBITRARY CODE EXECUTION

MEDIUM

Details

This finding has been retested and successfully resolved.

2 ARBITRARY COMMAND INJECTION

MEDIUM

Definition

Arbitrary command injection occurs when a user passes maliciously crafted input into an application, which then uses the unchecked data in a function that executes at the operating system level. The system cannot differentiate between these malicious commands and regular application commands and executes calls within the authority context of the original application.

Details

This finding has not been resolved and can still be exploited using the methods outlined in the previous report. After discussions with the developers, the development team determined that this issue will not be fixed as the EVM command-line interface (CLI) is not intended to be promoted for public use.

3 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 378 instances of vulnerable software. The team retested this finding and found that 272 of the original instances have been successfully remediated. Additionally, 83 of the unmitigated instances affecting the bridge-contracts package were determined to no longer be in use via discussions with the development team. There are 23 remaining instances that have not yet been remediated.

Affected Locations

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

4 INSECURE NETWORK TRANSMISSION INFORMATIONAL*

Definition

Insecure network transmission occurs when sensitive information is sent over a network without adequate protection. When data is sent across insecure communication channels, it may be susceptible to interception and modification by third parties, resulting in unauthorized information disclosure.

Details

The assessment team originally discovered two instances of HTTPS services affected by insecure network transmission. The team retested this finding and, after discussions with the development team, determined that the affected URLs were not intended to be publicly used.

*As the affected URLs were not intended to be used publicly, the risk rating of this finding was downgraded from low to informational.

Affected Locations

URLs

- `http://witness-evm-sidechain.peersyst.tech`
- `http://evm-poa-sidechain.peersyst.tech`

5 INSECURE SSL/TLS CONFIGURATION INFORMATIONAL*

Definition

The Secure Sockets Layer (SSL) and Transport Layer Security (TLS) protocols allow secure communication between a client and a server. Known vulnerabilities introduced by

insecure SSL/TLS configurations can potentially result in a successful Man-in-the-Middle (MitM) attack.

Details

The assessment team originally discovered four instances of insecure TLS services. The team retested this finding and found that one of the original instances has been successfully remediated. There are three remaining instances that have not yet been remediated.

*Due to partial remediation and the remaining affected URLs not intended to be used publicly, the risk rating of this finding was downgraded from low to informational.

Affected Locations

URLs

- `https://witness-evm-sidechain.peersyst.tech`
- `https://evm-sidechain.peersyst.tech`
- `https://evm-poa-sidechain.peersyst.tech`

6 INSECURE SOFTWARE CONFIGURATION

LOW

Details

This finding has been retested and successfully resolved.

7 MISSING SECURITY HEADERS

INFORMATIONAL*

Definition

HTTP security headers activate features in modern web browsers that help protect users against cross-site scripting (XSS), UI redress, and Man-in-the-Middle (MitM) attacks.

Details

The assessment team originally discovered five instances of missing security headers. The team retested this finding and found that one of the original instances has been successfully remediated. There are four remaining instances that have not yet been remediated.

Descriptions of the missing security headers are provided below:

Header Name	Description
`Strict-Transport-Security`	This header enforces HTTP Strict Transport Security (HSTS), which instructs browsers to communicate with the application over HTTPS and prevents any communications from being sent over HTTP.
`X-Frame-Options`	This header restricts which domains can render the resource within a frame, iframe, or object tag, which provides protection against UI redress attacks. The application can deny this ability entirely, restrict it to the same origin as the embedding page, or specify a safelist of allowed origins. While this header is considered deprecated, it is still widely supported by browsers.
`X-Content-Type-Options`	Setting the value of this header to `nosniff` prevents Internet Explorer and Google Chrome from attempting to determine the content type by inspecting the response. This helps protect users from untrusted content being rendered as HTML or other content types.

FIGURE 1 - Missing security headers

*Due to partial remediation and the remaining affected URLs not intended to be used publicly, the risk rating of this finding was downgraded from low to informational.

Affected Locations

URLs

- `https://witness-evm-sidechain.peersyst.tech`
- `https://custom.xrpl.org`
- `https://evm-poa-sidechain.peersyst.tech`
- `https://evm-sidechain.peersyst.tech`

8 OUTDATED SOFTWARE

LOW

Definition

Outdated dependencies exist when an application has not been updated with the latest patches or is using an outdated or deprecated version of a third-party library. Software

that has not been kept up to date could prove more difficult to upgrade at pace when a vulnerability is made public.

Details

The assessment team originally discovered 32 instances of outdated software. The team retested this finding and found that 24 of the original instances have been successfully remediated. There are eight remaining instances that have not yet been remediated.

Affected Locations

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

9 SENSITIVE INFORMATION DISCLOSURE LOW

Definition

Sensitive information disclosure occurs when private data is exposed to unauthorized parties. This may include financial data, personal privacy information, health records, proprietary information, or other important data.

Details

The assessment team originally discovered multiple categories of information disclosure including data exposed via Prometheus endpoints and sensitive data included in source code. After discussions with the Ripple development team, the assessment team determined that the two publicly available Prometheus endpoints were intentional and did not represent a security risk. Additionally, the assessment team discovered that the issue of sensitive data in source code had been partially mitigated by the removal of the eight affected files from the current version of the source repository. However, the assessment team determined that the affected files could still be accessed in the repository's Git history and any user with Git access to the repository could recover the potentially sensitive data.

Affected Locations

Affected Locations

- `xrp-evm/infra/devnet/terraform.tfstate`
- `xrp-evm/infra/devnet/terraform.tfstate.backup`
- `xrp-evm/.npmrc`
- `xrp-evm/packages/bridge-client-backend/.npmrc`
- `xrp-evm/packages/bridge-client-frontend/.npmrc`

- `xrp-evm/packages/bridge-node/.npmrc`
- `xrp-evm/packages/bridge-witness/.npmrc`
- `xrp-evm/packages/stress-tester/.npmrc`

10 WEAK CONTENT SECURITY POLICY (CSP) INFORMATIONAL*

Definition

Content Security Policy (CSP) is an HTML5 standard primarily designed to mitigate the issue of cross-site scripting (XSS) and other content injection vulnerabilities within web applications. Weak CSPs stem from overly permissive or ineffective content source directives

Details

The assessment team originally discovered five instances of a weak content security policy. The team retested this finding and found that one of the original instances has been successfully remediated. There are four remaining instances that have not yet been remediated.

*Due to partial remediation and the remaining affected URLs not intended to be used publicly, the risk rating of this finding was downgraded from low to informational.

Affected Locations

URLs

- `https://witness-evm-sidechain.peersyst.tech`
- `https://custom.xrpl.org`
- `https://evm-poa-sidechain.peersyst.tech`
- `https://evm-sidechain.peersyst.tech`

11 WEAK CRYPTOGRAPHY 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.