CERTIK

Certik Final Report For RioDeFi

Contents

Disclaimer

This report is subject to the terms and conditions (including without limitation, description of services, confidentiality, disclaimer and limitation of liability) set forth in the Verification Services Agreement between CertiK and RioDeFi (the "Company"), or the scope of services/verification, and terms and conditions provided to the Company in connection with the verification (collectively, the "Agreement"). This report provided in connection with the Services set forth in the Agreement shall be used by the Company only to the extent permitted under the terms and conditions set forth in the Agreement. This report may not be transmitted, disclosed, referred to or relied upon by any person for any purposes without CertiK's prior written consent.

About CertiK

CertiK is a technology-led blockchain security company founded by Computer Science professors from Yale University and Columbia University built to prove the security and correctness of smart contracts and blockchain protocols.

CertiK, in partnership with grants from IBM and the Ethereum Foundation, CertiK's mission of every audit is to apply different approaches and detection methods, ranging from manual, static, and dynamic analysis, to ensure that projects are checked against known attacks and potential vulnerabilities. CertiK leverages a team of seasoned engineers and security auditors to apply testing methodologies and assessments to each project, in turn creating a more secure and robust software system.

For more information: https://certik.org.

Executive Summary

This report has been prepared for RioDeFi to examine issues and vulnerabilities in the source code of their system in scope. A comprehensive examination has been performed, utilizing CertiK's Static Analysis, Manual and Dynamic Review techniques.

The auditing process pays special attention to the following considerations:

- Review the security and implementation soundness of the Rio Runtime.
- Review the security and implementation soundness of the Rio Assets.
- Review the security and implementation soundness of the Rio Bridge.
- Assessing the codebase to ensure compliance with current best practices and industry standards.
- Ensuring systems logic meets the specifications and intentions of the client.

Testing Summary

SECURITY LEVEL

This report has been prepared as a product of the Audit request by The RioDeFi team.
This audit was conducted to discover issues and vulnerabilities in the source code of The RioDeFi system.

TYPE	Smart Contracts & Token
SOURCE CODE	https://github.com/RioDefi/riodefi-node/tree/beta Fixes: https://github.com/RioDefi/riodefi-node/tree/beta-fix
PLATFORM	Substrate
LANGUAGE	Rust
REQUEST DATE	May 15, 2020
DELIVERY DATE	July 15, 2020
METHODS	A comprehensive examination has been performed using Dynamic Analysis, Static Analysis, and Manual Review.

Review Notes

Introduction

CertiK team was contracted by the RioDefi team to audit the design and implementations of the to be released Substrate based system. The audited modules:

- Rio-Bridge
- Rio-Assets
- Rio-Runtime

In the repository:

- https://github.com/RioDefi/riodefi-node/tree/beta

The goal of this audit is to review RioDeFi implementation for its business model, study potential security vulnerabilities, its general design and architecture, and uncover bugs that could compromise the software in production.

Documentation

There is clearly a lot of room for improvement when it comes to the documentation of the codebase. Although some parts of the codebase are well documented others are lacking proper documentation. Additionally all the documentation regarding the project, readme's, comments, whitepapers, yellow papers, should be at least English + level. Given the experience we had with the RioDefi team in this engagement we are confident that the documentation will be updated and fully in place for the mainnet release.

Summary

CertiK team audited the modules rio-bridge, rio-assets and the runtime and found the codebase to be in a good condition given the stage of the project(beta).
The code base makes good use of the framework specifics and the language best practices with only some minor exceptions pointed out in our findings and fixed by the team in complete.
Regarding the implementation of the privileged functionality handling and secure design around the framework with proper parameterization the codebase was found to respect the frameworks specifications and be in alignment with the intended functionality as modules.
Finally we have concluded that the team has a lot of room for improvement regarding the ethics, readability, testing and maintainability of the codebase on top of the good basis that has been already laid down.

Recommendations

We strongly advise projects for strict unit testing for ideally the complete codebase with emphasis on large code coverage to ensure that the intended functionality and outcome is achieved under all edge cases even before audits, this will ensure code quality and make audits more valuable. Additionally we recommend that due to the fact that the system runs a series of processes(database, rpc etc) panicking should be completely avoided even with the usage of expect, instead we should always gracefully exit properly shutting down all sub processes and freeing up resources.

Findings

Exhibit 1

TITLE	TYPE	SEVERITY	LOCATION
Asset_id is only used once	Optimization	Optimization	rio-bridge/lib.rs L156-159

Description:

Variable asset_id is only used in line 159.

Recommendations:

Remove the declaration and pass it directly to the function.

Update from RioDefi:

 Fixed in “beta-fix” branch.

Exhibit 2

TITLE	TYPE	SEVERITY	LOCATION
Asset_id is not used	Optimization	Optimization	rio-bridge/lib.rs L168

Description:

Variable asset_id is not used at all.

Recommendations:

Remove the unused variable.

Update from RioDefi:

 Fixed in “beta-fix” branch.

Exhibit 3

TITLE	TYPE	SEVERITY	LOCATION
Asset_id is only used once	Optimization	Optimization	rio-bridge/lib.rs L179-181

Description:

Variable asset_id is only used in line 181.

Recommendations:

Remove the declaration and pass it directly to the function.

Update from RioDefi:

 Fixed in “beta-fix” bradefnch.

Exhibit 4

TITLE	TYPE	SEVERITY	LOCATION
Use .is_empty() instead of > 0	Optimization	Optimization	rio-bridge/lib.rs L199

Description:

Use of > 0 rather than .is_empty().

Recommendations:

Use the build in .is_empty() function for better readability.

Update from RioDefi:

✓ Fixed in “beta-fix” branch.

Exhibit 5

TITLE	TYPE	SEVERITY	LOCATION
Use of unwrap unchecked may lead to panic	Minor	Minor	rio-bridge/lib.rs L201

Description:

Use of unwrap unchecked may lead to panic.

Recommendations:

On a production system we usually don't ever want to panic. Handle the case of none.

Update from RioDefi:

 Fixed in “beta-fix” branch.

Exhibit 6

TITLE	TYPE	SEVERITY	LOCATION
Use .is_empty() instead of > 0	Optimization	Optimization	rio-bridge/lib.rs L 213

Description:

Use of > 0 rather than .is_empty().

Recommendations:

Use the build in .is_empty() function for better readability.

Update from RioDefi:

 Fixed in “beta-fix” branch.

Exhibit 7

TITLE	TYPE	SEVERITY	LOCATION
Use of unwrap unchecked may lead to panic	Minor	Minor	rio-bridge/lib.rs L 214-215

Description:

Use of unwrap unchecked may lead to panic.

Recommendations:

On a production system we usually don't ever want to panic. Handle the case of none.

Update from RioDefi:

 Fixed in “beta-fix” branch.

Exhibit 8

TITLE	TYPE	SEVERITY	LOCATION
Comment represents the intended functionality	Minor	Minor	rio-assets/currency.rs L 80

Description:

Comment represents the intended functionality.

Recommendations:

Implement the comment.

Update from RioDefi:

✓ Fixed in “beta-fix” branch.

Exhibit 9

TITLE	TYPE	SEVERITY	LOCATION
Function slash is commented out and unimplemented, missing critical implementation to the system	Minor	Minor	rio-assets/currency.rs L 145-156

Description:

Function slash is commented out and unimplemented, missing critical implementation to the system.

Recommendations:

Implement the critical to the system functionality.

Update from RioDefi:

✓ Fixed in “beta-fix” branch.

Exhibit 10

TITLE	TYPE	SEVERITY	LOCATION
Comment, function naming and error message should be revised	Info	Info	rio-assets/lib.rs L 310

Description:

Comment, function naming and error message should be revised.

Update from RioDefi:

✓ Fixed in “beta-fix” branch.

Exhibit 11

TITLE	TYPE	SEVERITY	LOCATION
Total balance is represented by the comment	Minor	Minor	rio-assets/lib.rs L 325

Description:

Total balance represented by the comment.

Update from RioDefi:

✓ Fixed in “beta-fix” branch.