RubicTokenStaking Audit Report

Version 1.0.0

Serial No. 2021121800022021

Presented by Fairyproof

December 18, 2021

FAIRYPROOF

01. Introduction

This document includes the results of the audit performed by the Fairyproof team on the RubicTokenStaking project.

Audit Start Time:

December 15, 2021

Audit End Time:

December 16, 2021

Audited Code's Github Repository:

https://github.com/Cryptorubic/RubicTokenStaking

Audited Code's Github Commit Number When Audit Started:

bfa613a5e84d143424c90f0a5aec2d224a794df0

Audited Code's Github Commit Number When Audit Ended:

66922107844726ad6a7616ed36e7b03f5bea1e1d

Audited Source Files:

The calculated SHA-256 values for the audited files when the audit was done are as follows:

```
RubicTokenStaking.sol:
0xe7cfe9802ef555d1a225e16070de6525e0ee1fd147d7e135f67f602a3a12af1a
ERC20.sol             :
0x3bdffff0bf165794d262697f5db596625e061ca3073228500ac7968c2cda7a10
FreezableToken.sol    :
0x2072c04ad315869b608d83c3e0d51651f8c5de5f5e6a3d1c743878930d682c11
IERC20Minimal.sol     :
0xe1c35b78cd0c23d09812e0aec5e48f0b4e47773f6610ddceaca0cb567de56583
```

The source files audited include all the files with the extension "sol" as follows:

```
contracts/
├── RubicTokenStaking.sol
└── base
    ├── ERC20.sol
    ├── FreezableToken.sol
    └── IERC20Minimal.sol

1 directory, 4 files
```

The goal of this audit is to review RubicTokenStaking's solidity implementation for its staking function, study potential security vulnerabilities, its general design and architecture, and uncover bugs that could compromise the software in production.

We make observations on specific areas of the code that present concrete problems, as well as general observations that traverse the entire codebase horizontally, which could improve its quality as a whole.

This audit only applies to the specified code, software or any materials supplied by the Rubic team for specified versions. Whenever the code, software, materials, settings, enviroment etc is changed, the comments of this audit will no longer apply.

— Disclaimer

Note that as of the date of publishing, the contents of this report reflect the current understanding of known security patterns and state of the art regarding system security. You agree that your access and/or use, including but not limited to any associated services, products, protocols, platforms, content, and materials, will be at your sole risk.

The review does not extend to the compiler layer, or any other areas beyond the programming language, or other programming aspects that could present security risks. If the audited source files are smart contract files, risks or issues introduced by using data feeds from offchain sources are not extended by this review either.

Given the size of the project, the findings detailed here are not to be considered exhaustive, and further testing and audit is recommended after the issues covered are fixed.

To the fullest extent permitted by law, we disclaim all warranties, expressed or implied, in connection with this report, its content, and the related services and products and your use thereof, including, without limitation, the implied warranties of merchantability, fitness for a particular purpose, and non-infringement.

We do not warrant, endorse, guarantee, or assume responsibility for any product or service advertised or offered by a third party through the product, any open source or third-party software, code, libraries, materials, or information linked to, called by, referenced by or accessible through the report, its content, and the related services and products, any hyperlinked websites, any websites or mobile applications appearing on any advertising, and we will not be a party to or in any way be responsible for monitoring any transaction between you and any third-party providers of products or services.

FOR AVOIDANCE OF DOUBT, THE REPORT, ITS CONTENT, ACCESS, AND/OR USAGE THEREOF, INCLUDING ANY ASSOCIATED SERVICES OR MATERIALS, SHALL NOT BE CONSIDERED OR RELIED UPON AS ANY FORM OF FINANCIAL, INVESTMENT, TAX, LEGAL, REGULATORY, OR OTHER ADVICE.

— The Rubic Team's Consent/Acknowledgement:

The audited materials of the project including but not limited to the documents, home site, source code, etc are all developed, deployed, managed, and maintained outside Mainland CHINA.

The members of the team, the foundation, and all the organizations that participate in the audited project are not Mainland Chinese residents.

The audited project doesn’t provide services or products for Mainland Chinese residents.

— Methodology

The above files' code was studied in detail in order to acquire a clear impression of how the its specifications were implemented. The codebase was then subject to deep analysis and scrutiny, resulting in a series of observations. The problems and their potential solutions are discussed in this document and, whenever possible, we identify common sources for such problems and comment on them as well.

The Fairyproof auditing process follows a routine series of steps:

1. Code review that includes the following
   i. Review of the specifications, sources, and instructions provided to Fairyproof to make sure we understand the size, scope, and functionality of the project's source code.
   ii. Manual review of code, which is the process of reading source code line-by-line in an attempt to identify potential vulnerabilities.
   iii. Comparison to specification, which is the process of checking whether the code does what the specifications, sources, and instructions provided to Fairyproof describe.
2. Testing and automated analysis that includes the following:
   i. Test coverage analysis, which is the process of determining whether the test cases are actually covering the code and how much code is exercised when we run the test cases.
   ii. Symbolic execution, which is analyzing a program to determine what inputs cause each part of a program to execute.
3. Best practices review, which is a review of the source code to improve maintainability, security, and control based on the established industry and academic practices, recommendations, and research.

— Structure of the document

This report contains a list of issues and comments on all the above source files. Each issue is assigned a severity level based on the potential impact of the issue and recommendations to fix it, if applicable. For ease of navigation, an index by topic and another by severity are both provided at the beginning of the report.

— Documentation

For this audit, we used the following sources of truth about how the staking function should work:

https://github.com/Cryptorubic/RubicTokenStaking

These were considered the specification, and when discrepancies arose with the actual code behavior, we consulted with the Rubic team or reported an issue.

— Comments from Auditor

Serial Number	Auditor	Audit Time	Result
2021121500022018	Fairyproof Security Team	December 15, 2021 - December 16, 2021	Passed

Summary:

The Fairyproof security team used its auto analysis tools and manual work to audit the project. During the audit, 1 neutral suggestion was listed.

02. About Fairyproof

Fairyproof is a leading technology firm in the blockchain industry, providing consulting and security audits for organizations. Fairyproof has developed industry security standards for designing and deploying blockchain applications.

03. Major functions of audited code

RubicTokenStaking.sol is a staking contract. After users stake a specified token (BRBC) in the application they will get a certificate token (xBRBC). The staked tokens will be locked for at most 24 hours. After the locking period ends, users can withdraw their staked tokens.

Each time when a user stakes the BRBC token, the minimum quantity is 1000. Each user can stake a maximum total quantity of 100000 BRBCs. The maximum total quantity of the BRBC token all users can stake is 7000000.

Note:

Each staking or withdrawal operation calls looping instructions. This would result in relatively high gas consumption. Users would better be careful about too many staking or withdrawal operations.

The staking mechanism doesn't apply to a token whose transaction quantity is reduced in a transaction..

04. Coverage of issues

The issues that the Fairyproof team covered when conducting the audit include but are not limited to the following ones:

- Re-entrancy Attack
- Replay Attack
- Reordering Attack
- Miner's Advantage
- Rollback Attack
- DDos Attack
- Transaction Ordering Attack
- Race Condition
- Access Control
- Integer Overflow/Underflow
- Timestamp Attack
- Gas Consumption
- Inappropriate Callback Function
- Function Visibility
- Implementation Vulnerability
- Uninitialized Storage Pointer
- Arithmetic Precision
- Tx.origin
- Fake Deposit
- Shadow Variable
- Design Vulnerability
- Token Issurance
- Admin Rights
- Inappropriate Proxy Design
- Inappropriate Use of Slots
- Asset Security
- Contract Upgrade/Migration
- Code Improvement
- Misc

05. Severity level reference

Every issue in this report was assigned a severity level from the following:

Critical severity issues need to be fixed as soon as possible.

High severity issues will probably bring problems and should be fixed.

Medium severity issues could potentially bring problems and should eventually be fixed.

Low severity issues are minor details and warnings that can remain unfixed but would be better fixed at some point in the future.

Neutral is not an issue or risk but a suggestion for code improvement.

06. List of issues by severity

Index	Title	Issue/Risk	Severity	Status
N1	Missing check for interger overflow/underflow	Integer Overflow/Underflow	Neutral	Fixed

07. Issue descriptions

[N1] [Neutral] Missing check for interger overflow/underflow

Risk Severity: Neutral

Issue/Risk: Interger Overflow/Underflow

Description:

The `_enter` function defined in line 42 of the `RubicTokenStaking.sol` file had the following code section:

```
userEnteredAmount[_to] += _amount;
totalRBCEntered += _amount;
```

This code here didn't check if the operation would cause interger overflow/underflow.

Recommendation:

Consider changing the above code to the following one:

```
userEnteredAmount[_to] = userEnteredAmount[_to].add(_amount);
totalRBCEntered = totalRBCEntered.add(_amount);
```

Status:

This suggestion has been adopted by the team.

08. Recommendations to enhance the overall security

We list some recommendations in this section. They are not mandatory but will enhance the overall security of the system if they are adopted.

- N/A