CERTIK

Security Assessment

Rubic Finance

Nov 29th, 2021

Table of Contents

Summary

This report has been prepared for Rubic Finance to discover issues and vulnerabilities in the source code of the Rubic Finance project as well as any contract dependencies that were not part of an officially recognized library. A comprehensive examination has been performed, utilizing Static Analysis and Manual Review techniques.

The auditing process pays special attention to the following considerations:

- Testing the smart contracts against both common and uncommon attack vectors.
- Assessing the codebase to ensure compliance with current best practices and industry standards.
- Ensuring contract logic meets the specifications and intentions of the client.
- Cross referencing contract structure and implementation against similar smart contracts produced by industry leaders.
- Thorough line-by-line manual review of the entire codebase by industry experts.

The security assessment resulted in findings that ranged from critical to informational. We recommend addressing these findings to ensure a high level of security standards and industry practices. We suggest recommendations that could better serve the project from the security perspective:

- Enhance general coding practices for better structures of source codes;
- Add enough unit tests to cover the possible use cases;
- Provide more comments per each function for readability, especially contracts that are verified in public;
- Provide more transparency on privileged activities once the protocol is live.

Overview

Project Summary

Project Name	Rubic Finance
Platform	Custom
Language	Solidity
Codebase	https://github.com/Cryptorubic/CrossChainTokenSwap
Commit	7d01d19c9471615e80d31b19ae87da922f7ee405 aaf37206f3f146de8caca62eabe1b3ee6c68f38a a3845b09c4bdea9dec141af0b2166075e0e4312e 6c55d71932729d7a177c8f68ab0a48ce6e506e2f

Audit Summary

Delivery Date	Nov 29, 2021
Audit Methodology	Static Analysis, Manual Review
Key Components	

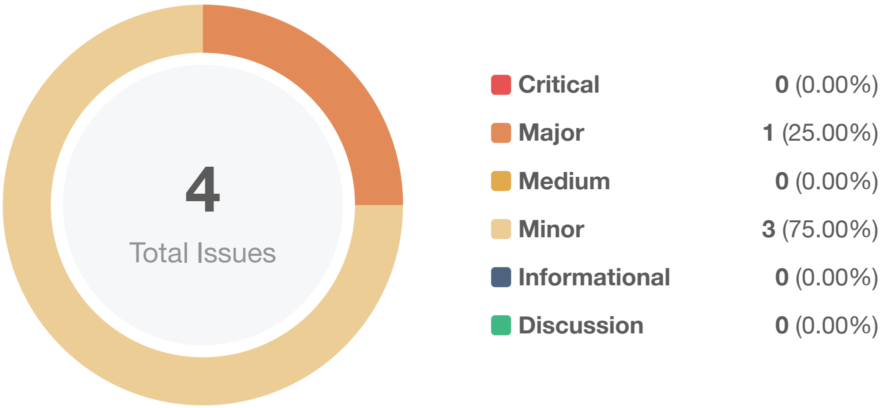
Vulnerability Summary

Vulnerability Level	Total	Pending	Declined	Acknowledged	Partially Resolved	Resolved
● Critical	0	0	0	0	0	0
● Major	1	0	0	0	0	1
● Medium	0	0	0	0	0	0
● Minor	3	0	0	0	0	3
● Informational	0	0	0	0	0	0
● Discussion	0	0	0	0	0	0

Audit Scope

ID	File	SHA256 Checksum
IPR	interfaces/IPangolinRouter.sol	a74d709bcf8014ce87b2695f380680e44d7387a66a7c4db7833c94bca5d3949c
ECD	libraries/ECDSAOffsetRecovery.sol	2153a7e16657e037e82b42c09bf053aefe10e0441f3a82584a32a096d6ebd32c
FMR	libraries/FullMath.sol	921e3025fa1fc030a75370d6cff6476126fdc57c613b4aceb3feb5edc861bebf
SCR	SwapContract.sol	bb570c1504c016e99b9a86cab8e4d3abd7ee5c47a538ed3956b115472e4cc771

Findings



ID	Title	Category	Severity	Status
SCR-01	Centralization Risk	**Centralization / Privilege**	● **Major**	✓ Resolved
SCR-02	Missing Input Validation	Volatile Code	● Minor	✓ Resolved
SCR-03	Usage Of `send()` For Sending Ether	Volatile Code	● Minor	✓ Resolved
SCR-04	Documentation Discrepancy	Inconsistency	● Minor	✓ Resolved

SCR-01 | Centralization Risk

Category	Severity	Location	Status
Centralization / Privilege	● **Major**	projects/RubicFinance/SwapContract.sol (23688cf)	✓ Resolved

Description

In the contract `SwapContract`, the role `OWNER_ROLE` has the authority over the following functions:

- `addOtherBlockchain()`
- `removeOtherBlockchain()`
- `changeOtherBlockchain()`
- `collectCryptoFee()`
- `collectTokenFee()`
- `setMinConfirmationSignatures()`
- `transferOwnerAndSetManager()`
- `pauseExecution()`
- `continueExecution()`
- `setRouter()`
- `setFeeAmountOfBlockchain()`
- `setCryptoFeeOfBlockchain()`
- `setRubicAddressOfBlockchain()`
- `setMinTokenAmount()`
- `setMaxTokenAmount()`
- `setMaxGasPrice()`
- `setMinConfirmationBlocks()`
- `setRefundSlippage()`
- `poolBalancing()`

Any compromise to the `OWNER_ROLE` account may allow the hacker to take advantage of this and manipulate the entire project. Especially in the functions `collectCryptoFee()` and `collectTokenFee()`, hacker can take advantage of these two functions to withdraw all the ETH/BNB & tokens to the hacker's address.

Meanwhile, the role `MANAGER_ROLE` has the authority over the following functions:

- `setRouter()`
- `setFeeAmountOfBlockchain()`

- `setCryptoFeeOfBlockchain()`
- `setRubicAddressOfBlockchain()`
- `setMinTokenAmount()`
- `setMaxTokenAmount()`
- `setMaxGasPrice()`
- `setMinConfirmationBlocks()`
- `setRefundSlippage()`

Any compromise to the `MANAGER_ROLE` account may allow the hacker to take advantage of this and change the sensitive variables without any restriction.

Meanwhile, the role `RELAYER_ROLE` has the authority over the following functions:

- `swapTokensToUserWithFee()`
- `swapCryptoToUserWithFee()`
- `refundTokensToUser()`
- `refundCryptoToUser()``
- `changeTxStatus()`
- `setCryptoFeeOfBlockchain()`

`RELAYER_ROLE` is supposed to be the relayer contract or EOA to relay the cross-chain swap event messages. However, any compromise to the `RELAYER_ROLE` account may allow the hacker to take advantage of this and control the entire cross-chain swap mechanism.

Recommendation

We advise the client to carefully manage the privileged account's private key to avoid any potential risks of being hacked. In general, we strongly recommend centralized privileges or roles in the protocol to be improved via a decentralized mechanism or smart-contract-based accounts with enhanced security practices, e.g., Multisignature wallets.

Indicatively, here is some feasible suggestions that would also mitigate the potential risk at the different level in term of short-term and long-term:

- Time-lock with reasonable latency, e.g., 48 hours, for awareness on privileged operations;
- Assignment of privileged roles to multi-signature wallets to prevent a single point of failure due to the private key;
- Introduction of a DAO/governance/voting module to increase transparency and user involvement.

Alleviation

`[Rubic Finance Team]`: According to medium post published by the team, Multisig wallet will be used for privileged roles. The addresses are listed as follows:

- MULTISIG ADDRESS: 0x6129B000f43D82E533CF20A7FD89c43E5A772BCD
    - Vladimir Tikhomirov: 0x105A3BA3637A29D36F61c7F03f55Da44B4591Cd1
    - Korneva Alexandra: 0x836f2051cDe3ba744aafE668F6a6070BA80668F9
    - Dmitry Ershov: 0x9499179d309B6Bf0253DcE9A35c2E37a75C41E47

Multisig, which is used for `OWNER_ROLE`, requires 2 out of 3 signatures for a transaction to be approved.

Reference: Rubic Multi-Chain routing Decentralization https://cryptorubic.medium.com/rubic-multi-chain-routing-decentralization-530241d3c89d

SCR-02 | Missing Input Validation

Category	Severity	Location	Status
Volatile Code	● Minor	projects/RubicFinance/SwapContract.sol (23688cf): 276~285	✓ Resolved

Description

The given input is missing the check for the non-zero address.

Recommendation

We advise adding the check for the passed-in values to prevent unexpected error as below:

```
require( address(_blockchainRouter) != address(0), "_blockchainRouter is address 0" );
```

Alleviation

`[Rubic Finance Team]`: The client heeded the advice and fixed the issue in the commit aaf37206f3f146de8caca62eabe1b3ee6c68f38a

SCR-03 | Usage Of `send()` For Sending Ether

Category	Severity	Location	Status
Volatile Code	● Minor	projects/RubicFinance/SwapContract.sol (23688cf): 445~447, 685	✓ Resolved

Description

After EIP-1884 was included in the Istanbul hard fork, it is not recommended to use `.transfer()` or `.send()` for transferring ether as these functions have a hard-coded value for gas costs making them obsolete as they are forwarding a fixed amount of gas, specifically `2300`. This can cause issues in case the linked statements are meant to be able to transfer funds to other contracts instead of EOAs.

Recommendation

We advise that the linked `.transfer()` and `.send()` calls are substituted with the utilization of the `sendValue()` function from the `Address.sol` implementation of OpenZeppelin either by directly importing the library or copying the linked code.

Alleviation

`[Rubic Finance Team]`: The client heeded the advice and fixed the issue in the commit aaf37206f3f146de8caca62eabe1b3ee6c68f38a

SCR-04 | Documentation Discrepancy

Category	Severity	Location	Status
Inconsistency	● Minor	projects/RubicFinance/SwapContract.sol (23688cf): 376, 428	✓ Resolved

Description

Due to refactoring the following functions in the commit a3845b09c4bdea9dec141af0b2166075e0e4312e, the comment of these functions lacks the detailed explanation of the params. Especially `params.exactRBCtokenOut` and `params.tokenInAmount` in the function `swapTokensToOtherBlockchain()`, as this function is external function, user could be confused.

- `swapTokensToOtherBlockchain()`
- `swapCryptoToOtherBlockchain()`

Recommendation

We advise to rectify the comment on the aforementioned functions to increase the legibility of the codebase.

Alleviation

`[Rubic Finance Team]`: The client heeded the advice and updated the annotations in the commit 6c55d71932729d7a177c8f68ab0a48ce6e506e2f

Appendix

Finding Categories

Centralization / Privilege

Centralization / Privilege findings refer to either feature logic or implementation of components that act against the nature of decentralization, such as explicit ownership or specialized access roles in combination with a mechanism to relocate funds.

Volatile Code

Volatile Code findings refer to segments of code that behave unexpectedly on certain edge cases that may result in a vulnerability.

Inconsistency

Inconsistency findings refer to functions that should seemingly behave similarly yet contain different code, such as a constructor assignment imposing different require statements on the input variables than a setter function.

Checksum Calculation Method

The "Checksum" field in the "Audit Scope" section is calculated as the SHA-256 (Secure Hash Algorithm 2 with digest size of 256 bits) digest of the content of each file hosted in the listed source repository under the specified commit.

The result is hexadecimal encoded and is the same as the output of the Linux "sha256sum" command against the target file.

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 Services Agreement, or the scope of services, and terms and conditions provided to you (“Customer” or the “Company”) in connection with 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, nor may copies be delivered to any other person other than the Company, without CertiK’s prior written consent in each instance.

This report is not, nor should be considered, an “endorsement” or “disapproval” of any particular project or team. This report is not, nor should be considered, an indication of the economics or value of any “product” or “asset” created by any team or project that contracts CertiK to perform a security assessment. This report does not provide any warranty or guarantee regarding the absolute bug-free nature of the technology analyzed, nor do they provide any indication of the technologies proprietors, business, business model or legal compliance.

This report should not be used in any way to make decisions around investment or involvement with any particular project. This report in no way provides investment advice, nor should be leveraged as investment advice of any sort. This report represents an extensive assessing process intending to help our customers increase the quality of their code while reducing the high level of risk presented by cryptographic tokens and blockchain technology.

Blockchain technology and cryptographic assets present a high level of ongoing risk. CertiK’s position is that each company and individual are responsible for their own due diligence and continuous security. CertiK’s goal is to help reduce the attack vectors and the high level of variance associated with utilizing new and consistently changing technologies, and in no way claims any guarantee of security or functionality of the technology we agree to analyze.

The assessment services provided by CertiK is subject to dependencies and under continuing development. You agree that your access and/or use, including but not limited to any services, reports, and materials, will be at your sole risk on an as-is, where-is, and as-available basis. Cryptographic tokens are emergent technologies and carry with them high levels of technical risk and uncertainty. The assessment reports could include false positives, false negatives, and other unpredictable results. The services may access, and depend upon, multiple layers of third-parties.

ALL SERVICES, THE LABELS, THE ASSESSMENT REPORT, WORK PRODUCT, OR OTHER MATERIALS, OR ANY PRODUCTS OR RESULTS OF THE USE THEREOF ARE PROVIDED “AS IS” AND “AS

AVAILABLE” AND WITH ALL FAULTS AND DEFECTS WITHOUT WARRANTY OF ANY KIND. TO THE MAXIMUM EXTENT PERMITTED UNDER APPLICABLE LAW, CERTIK HEREBY DISCLAIMS ALL WARRANTIES, WHETHER EXPRESS, IMPLIED, STATUTORY, OR OTHERWISE WITH RESPECT TO THE SERVICES, ASSESSMENT REPORT, OR OTHER MATERIALS. WITHOUT LIMITING THE FOREGOING, CERTIK SPECIFICALLY DISCLAIMS ALL IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, TITLE AND NON-INFRINGEMENT, AND ALL WARRANTIES ARISING FROM COURSE OF DEALING, USAGE, OR TRADE PRACTICE. WITHOUT LIMITING THE FOREGOING, CERTIK MAKES NO WARRANTY OF ANY KIND THAT THE SERVICES, THE LABELS, THE ASSESSMENT REPORT, WORK PRODUCT, OR OTHER MATERIALS, OR ANY PRODUCTS OR RESULTS OF THE USE THEREOF, WILL MEET CUSTOMER’S OR ANY OTHER PERSON’S REQUIREMENTS, ACHIEVE ANY INTENDED RESULT, BE COMPATIBLE OR WORK WITH ANY SOFTWARE, SYSTEM, OR OTHER SERVICES, OR BE SECURE, ACCURATE, COMPLETE, FREE OF HARMFUL CODE, OR ERROR-FREE. WITHOUT LIMITATION TO THE FOREGOING, CERTIK PROVIDES NO WARRANTY OR UNDERTAKING, AND MAKES NO REPRESENTATION OF ANY KIND THAT THE SERVICE WILL MEET CUSTOMER’S REQUIREMENTS, ACHIEVE ANY INTENDED RESULTS, BE COMPATIBLE OR WORK WITH ANY OTHER SOFTWARE, APPLICATIONS, SYSTEMS OR SERVICES, OPERATE WITHOUT INTERRUPTION, MEET ANY PERFORMANCE OR RELIABILITY STANDARDS OR BE ERROR FREE OR THAT ANY ERRORS OR DEFECTS CAN OR WILL BE CORRECTED.

WITHOUT LIMITING THE FOREGOING, NEITHER CERTIK NOR ANY OF CERTIK’S AGENTS MAKES ANY REPRESENTATION OR WARRANTY OF ANY KIND, EXPRESS OR IMPLIED AS TO THE ACCURACY, RELIABILITY, OR CURRENCY OF ANY INFORMATION OR CONTENT PROVIDED THROUGH THE SERVICE. CERTIK WILL ASSUME NO LIABILITY OR RESPONSIBILITY FOR (I) ANY ERRORS, MISTAKES, OR INACCURACIES OF CONTENT AND MATERIALS OR FOR ANY LOSS OR DAMAGE OF ANY KIND INCURRED AS A RESULT OF THE USE OF ANY CONTENT, OR (II) ANY PERSONAL INJURY OR PROPERTY DAMAGE, OF ANY NATURE WHATSOEVER, RESULTING FROM CUSTOMER’S ACCESS TO OR USE OF THE SERVICES, ASSESSMENT REPORT, OR OTHER MATERIALS.

ALL THIRD-PARTY MATERIALS ARE PROVIDED “AS IS” AND ANY REPRESENTATION OR WARRANTY OF OR CONCERNING ANY THIRD-PARTY MATERIALS IS STRICTLY BETWEEN CUSTOMER AND THE THIRD-PARTY OWNER OR DISTRIBUTOR OF THE THIRD-PARTY MATERIALS.

THE SERVICES, ASSESSMENT REPORT, AND ANY OTHER MATERIALS HEREUNDER ARE SOLELY PROVIDED TO CUSTOMER AND MAY NOT BE RELIED ON BY ANY OTHER PERSON OR FOR ANY PURPOSE NOT SPECIFICALLY IDENTIFIED IN THIS AGREEMENT, NOR MAY COPIES BE DELIVERED TO, ANY OTHER PERSON WITHOUT CERTIK’S PRIOR WRITTEN CONSENT IN EACH INSTANCE.

NO THIRD PARTY OR ANYONE ACTING ON BEHALF OF ANY THEREOF, SHALL BE A THIRD PARTY OR OTHER BENEFICIARY OF SUCH SERVICES, ASSESSMENT REPORT, AND ANY ACCOMPANYING

MATERIALS AND NO SUCH THIRD PARTY SHALL HAVE ANY RIGHTS OF CONTRIBUTION AGAINST CERTIK WITH RESPECT TO SUCH SERVICES, ASSESSMENT REPORT, AND ANY ACCOMPANYING MATERIALS.

THE REPRESENTATIONS AND WARRANTIES OF CERTIK CONTAINED IN THIS AGREEMENT ARE SOLELY FOR THE BENEFIT OF CUSTOMER. ACCORDINGLY, NO THIRD PARTY OR ANYONE ACTING ON BEHALF OF ANY THEREOF, SHALL BE A THIRD PARTY OR OTHER BENEFICIARY OF SUCH REPRESENTATIONS AND WARRANTIES AND NO SUCH THIRD PARTY SHALL HAVE ANY RIGHTS OF CONTRIBUTION AGAINST CERTIK WITH RESPECT TO SUCH REPRESENTATIONS OR WARRANTIES OR ANY MATTER SUBJECT TO OR RESULTING IN INDEMNIFICATION UNDER THIS AGREEMENT OR OTHERWISE.

FOR AVOIDANCE OF DOUBT, THE SERVICES, INCLUDING ANY ASSOCIATED ASSESSMENT REPORTS OR MATERIALS, SHALL NOT BE CONSIDERED OR RELIED UPON AS ANY FORM OF FINANCIAL, TAX, LEGAL, REGULATORY, OR OTHER ADVICE.

About

Founded in 2017 by leading academics in the field of Computer Science from both Yale and Columbia University, CertiK is a leading blockchain security company that serves to verify the security and correctness of smart contracts and blockchain-based protocols. Through the utilization of our world-class technical expertise, alongside our proprietary, innovative tech, we're able to support the success of our clients with best-in-class security, all whilst realizing our overarching vision; provable trust for all throughout all facets of blockchain.

CERTIK