RICK FINANCE PROTOCOL SMART CONTRACT CODE REVIEW AND SECURITY ANALYSIS REPORT

Customer: Rick Finance Team (https://www.rick.finance)
Prepared on: 26/03/2021
Platform: Binance Smart Chain
Language: Solidity
Audit Type: Standard

audit@etherauthority.io

Table of contents

THIS IS SECURITY AUDIT REPORT DOCUMENT AND WHICH MAY CONTAIN INFORMATION WHICH IS CONFIDENTIAL. WHICH INCLUDES ANY POTENTIAL VULNERABILITIES AND MALICIOUS CODES WHICH CAN BE USED TO EXPLOIT THE SOFTWARE. THIS MUST BE REFERRED INTERNALLY AND ONLY SHOULD BE MADE AVAILABLE TO PUBLIC AFTER ISSUES ARE RESOLVED.

Project files

Name	Smart Contract Code Review and Security Analysis Report for Rick Finance
Platform	Binance Smart Chain / Solidity
File 1	MasterChef.sol
File 1 MD5 hash	6186FD4277E83F454493AF1B64D54C4B
File 1 BscScan Contract URL	https://bscscan.com/address/0x0e0f3247db921559abde3ef7e8fdb6651b2e2836#code
File 2	Timelock.sol
File 2 MD5 hash	FEEACF4FC7026EAFA0AAF4122936DDEB
File 2 BscScan Contract URL	https://bscscan.com/address/0xa796683a20f159db73fa48d4e0a5b00c094f4941#code
File 3	RickToken.sol
File 3 MD5 hash	2610082B3E33EAE2988E7F0E9401296E
File 3 BscScan Contract URL	https://bscscan.com/address/0x95fc8747eb0246eeb59d9c5df76ec806d77f7b2d#code

Introduction

We were contracted by the Rick Finance team to perform the Security audit of the smart contracts code. The audit has been performed using manual analysis as well as using automated software tools. This report presents all the findings regarding the audit performed on 26/03/2021.

The Audit type was Standard Audit. Which means this audit is concluded based on Standard audit scope, which is one security engineer performing audit procedure for 2 days. This document outlines all the findings as well as AS-IS overview of the smart contract codes.

Email: audit@EtherAuthority.io

Quick Stats:

Main Category	Subcategory	Result
Contract Programming	Solidity version not specified	Passed
	Solidity version too old	Moderated
	Integer overflow/underflow	Passed
	Function input parameters lack of check	Moderated
	Function input parameters check bypass	Passed
	Function access control lacks management	Passed
	Critical operation lacks event log	Moderated
	Human/contract checks bypass	Passed
	Random number generation/use vulnerability	N/A
	Fallback function misuse	Passed
	Race condition	Passed
	Logical vulnerability	Passed
	Other programming issues	Passed
Code Specification	Function visibility not explicitly declared	Passed
	Var. storage location not explicitly declared	Passed
	Use keywords/functions to be deprecated	Passed
	Other code specification issues	Passed
Gas Optimization	Assert() misuse	Passed
	High consumption ‘for/while’ loop	Moderated
	High consumption ‘storage’ storage	Passed
	“Out of Gas” Attack	Passed
Business Risk	The maximum limit for mintage not set	Moderted
	“Short Address” Attack	Passed
	“Double Spend” Attack	Passed

Overall Audit Result: PASSED

Executive Summary

According to the **standard** audit assessment, Customer`s solidity smart contract is **well secured**.

We used various tools like SmartDec, Mythril, Slither and Remix IDE. At the same time this finding is based on critical analysis of the manual audit.
All issues found during automated analysis were manually reviewed and applicable vulnerabilities are presented in the Audit overview section. General overview is presented in AS-IS section and all issues can be found in the Audit overview section.

We found 0 high, 2 medium and 1 low and some very low level issues.

Code Quality

We were given 3 smart contract files of Rick Finance Protocol. These smart contracts also contain Libraries, Smart contract inherits and Interfaces. These smart contracts are fork of goosedefi.com with minor customization.

The libraries in the Rick Finance protocol are part of its logical algorithm. A library is a different type of smart contract that contains reusable code. Once deployed on the blockchain (only once), it is assigned a specific address and its properties / methods can be reused many times by other contracts in the Rick Finance protocol.

The Rick Finance team has **not** provided scenario and unit test scripts, which would have helped to determine the integrity of the code in an automated way.

Overall, code parts are well commented. Commenting can provide rich documentation for functions, return variables and more. Ethereum Natural Language Specification Format (NatSpec) is used, which is a good thing.

Documentation

We were given Rick Finance smart contracts code in the form of BscScan web links. The hashes of those codes and their BscScan web links are mentioned above in the table.

As mentioned above, most code parts are well commented. so anyone can quickly understand the programming flow as well as complex code logic. Comments are very helpful in understanding the overall architecture of the protocol. It also provided a clear overview of the system components, including helpful details, like the lifetime of the background script.

Use of Dependencies

As per our observation, the libraries are used in this smart contract infrastructure that are based on well known industry standard open source projects. And their core code blocks are written well.

Apart from libraries, Rick Finance smart contracts depend on an interconnected set of smart contracts.

AS-IS overview

Rick Finance protocol is a decentralized exchange running on Binance Smart Chain, with other features like farming, governance tokens, etc. Following are the main components of core smart contracts.

MasterChef.sol

(1) Inherited contracts

(a) Ownable: ownership contract

(2) Usages

(a) using SafeMath for uint256
(b) using SafeBEP20 for IBEP20

(3) Structs

(a) UserInfo: Info about each user
(b) PoolInfo: Info about each pools

(4) Events

(a) event Deposit(address indexed user, uint256 indexed pid, uint256 amount);
(b) event Withdraw(address indexed user, uint256 indexed pid, uint256 amount);
(c) event EmergencyWithdraw(address indexed user, uint256 indexed pid, uint256 amount);

(5) Functions

Sl.	Function	Type	Observation	Conclusion	Score
1	constructor	write	Passed	No Issue	Passed
2	poolLength	read	Passed	No Issue	Passed
3	add	write	Input validation missing	LP Token must not be added twice	Passed with consent
4	set	write	Passed	No Issue	Passed
5	getMultiplier	read	Passed	No Issue	Passed
6	pendingRick	read	Passed	No Issue	Passed

7	massUpdatePools	write	Infinite loop possibility	Array length must be limited	Passed with consent
8	updatePool	write	Passed	No Issue	Passed
9	deposit	write	Passed	No Issue	Passed
10	withdraw	write	Passed	No Issue	Passed
11	emergencyWithdraw	write	Passed	No Issue	Passed
12	safeRickTransfer	write	Passed	No Issue	Passed
13	dev	write	Passed	No Issue	Passed
14	setFeeAddress	write	Passed	No Issue	Passed
15	updateEmissionRate	write	Passed	No Issue	Passed

Timelock.sol

(1) Usages

(a) using SafeMath for uint

(2) Events

(a) event NewAdmin(address indexed newAdmin);
(b) event NewPendingAdmin(address indexed newPendingAdmin);
(c) event NewDelay(uint indexed newDelay);
(d) event CancelTransaction(bytes32 indexed txHash, address indexed target, uint value, string signature, bytes data, uint eta);
(e) event ExecuteTransaction(bytes32 indexed txHash, address indexed target, uint value, string signature, bytes data, uint eta);
(f) event QueueTransaction(bytes32 indexed txHash, address indexed target, uint value, string signature, bytes data, uint eta);

(3) Functions

Sl.	Function	Type	Observation	Conclusion	Score
1	constructor	write	Passed	No Issue	Passed
2	fallback function	write	accepts BNB	No Issue	Passed
3	setDelay	write	caller was required to be contract itself	It should be an admin	Passed with consent
4	acceptAdmin	write	Passed	No Issue	Passed

Email: audit@EtherAuthority.io

5	setPendingAdmin	write	caller was required to be contract itself	It should be an admin	Passed with consent
6	queueTransaction	write	Passed	No Issue	Passed
7	cancelTransaction	write	Passed	No Issue	Passed
8	executeTransaction	write	Passed	No Issue	Passed
9	getBlockTimestamp	read	Passed	No Issue	Passed

RickToken.sol

(1) Inherited contracts

(a) BEP20: Standard contract for BEP20
(b) Context: Provides msg.sender and msg.value context
(c) IBEP20: unwanted inheritance. Remove this.
(d) Ownable: Ownership contract

(2) Events

(a) event DelegateChanged(address indexed delegator, address indexed fromDelegate, address indexed toDelegate);
(b) event DelegateVotesChanged(address indexed delegate, uint256 previousBalance, uint256 newBalance);

(3) Functions

Sl.	Function	Type	Observation	Conclusion	Score
1	mint	write	No max minting set	must be used carefully	Passed with consent
2	delegates	read	Passed	No Issue	Passed
3	delegate	write	Passed	No Issue	Passed
4	delegateBySig	write	Signature was used	Take extra care with handling signatures	Passed with consent
5	getCurrentVotes	read	Passed	No Issue	Passed

6	getPriorVotes	read	Infinite loop possibility	Keep array length limited	Passed with consent
7	_delegate	internal	Passed	No Issue	Passed
8	_moveDelegates	internal	Passed	No Issue	Passed
9	_writeCheckpoint	internal	Passed	No Issue	Passed
10	safe32	read	Passed	No Issue	Passed
11	getChainId	read	Passed	No Issue	Passed

Severity Definitions

Risk Level	Description
Critical	Critical vulnerabilities are usually straightforward to exploit and can lead to tokens loss etc.
High	High-level vulnerabilities are difficult to exploit; however, they also have significant impact on smart contract execution, e.g. public access to crucial functions
Medium	Medium-level vulnerabilities are important to fix; however, they can't lead to tokens lose
Low	Low-level vulnerabilities are mostly related to outdated, unused etc. code snippets, that can't have significant impact on execution
Lowest / Code Style / Best Practice	Lowest-level vulnerabilities, code style violations and info statements can't affect smart contract execution and can be ignored.

Audit Findings

Critical

No critical severity vulnerabilities were found.

High

No high severity vulnerabilities were found.

Medium

(1) Input validation missing in MasterChef.sol

```
// XXX DO NOT add the same LP token more than once. Rewards will be messed up if you do.
function add(uint256 _allocPoint, IBEP20 _lpToken, uint16 _depositFeeBP, bool _withUpdate) public onlyOwner
    require(_depositFeeBP <= 10000, "add: invalid deposit fee basis points");
    if (_withUpdate) {
        massUpdatePools();
    }
    uint256 lastRewardBlock = block.number > startBlock ? block.number : startBlock;
    totalAllocPoint = totalAllocPoint.add(_allocPoint);
    poolInfo.push(PoolInfo({
```

As mentioned in the comment, the token must never be added twice. So, there must be a condition to prevent that happening by mistake.

<u>Resolution</u>: we got confirmation from the Rick Finance team as this will be taken extra care as this is the owner function.

(2) Minting could be unlimited by owner in RickToken.sol

```
function mint(address _to, uint256 _amount) public onlyOwner {
    _mint(_to, _amount);
    _moveDelegates(address(0), _delegates[_to], _amount);
}
```

Unlimited minting is considered a bad practice for tokenomics and hence it should be discouraged.

<u>Resolution</u>: Rick Finance team confirmed that this minting would be triggered by masterChef contract only.

Low

(1) Infinite loops possibility at multiple places:

```
function massUpdatePools() public {
    uint256 length = poolInfo.length;
    for (uint256 pid = 0; pid < length; ++pid) {
        updatePool(pid);
    }
}
```

As seen in the AS-IS section, there are some places in the smart contracts, where array.length is used directly in the loops. It is recommended to put some kind of limits, so it does not go wild and create any scenario where it can hit the block gas limit.

Resolution: We got confirmation from the Rick Finance team that the array will be provided as limited length. And this will be taken care of from the client side.

Very Low

(1) Ownership transfer function:

Ownable.sol smart contract has active ownership transfer. This will be troublesome if the ownership was sent to an incorrect address by human error.

```
function _transferOwnership(address newOwner) internal {
  require(newOwner != address(0), "Ownable: new owner is the zero address");
  emit OwnershipTransferred(_owner, newOwner);
  _owner = newOwner;
}
```

so, it is a good practice to implement acceptOwnership style to prevent it. Code flow similar to below:

```
    function transferOwnership(address payable _newOwner) external onlyOwner {
        newOwner = _newOwner;
    }

    //this flow is to prevent transferring ownership to wrong wallet by mistake
    function acceptOwnership() external {
        require(msg.sender == newOwner);
        emit OwnershipTransferred(owner, newOwner);
        owner = newOwner;
        newOwner = payable(0);
    }
}
```

Resolution: Rick Finance team acknowledged this, as this should be taken care of from admin side.

(2) Use the latest solidity version while contract deployment to prevent any compiler version level bugs.
Resolution: This issue is acknowledged.

(3) Event log must be fired in the place where the stats are being changed. for example:

- dev function in MasterChef.sol
- setFeeAddress function in MasterChef.sol
- updateEmissionRate function in MasterChef.sol

Resolution: This issue is acknowledged.

(4) Signatures are used in the functions delegateBySig in RickToken.sol contract. Those signatures should be used securely by the dapps. Because users might not know that signing such a message would allow malicious dapps to do certain actions on the user's behalf.

Conclusion

We were given contract code. And we have used all possible tests based on given objects as files. The contracts are written so systematically, that we did not find any major issues. **So it is good to go for the production.**

Since possible test cases can be unlimited for such extensive smart contract protocol, so we provide no such guarantee of future outcomes. We have used all the latest static tools and manual observations to cover maximum possible test cases to scan everything.

Smart contracts within the scope were manually reviewed and analyzed with static analysis tools. Smart Contract's high level description of functionality was presented in the As-is overview section of the report.

Audit report contains all found security vulnerabilities and other issues in the reviewed code.

Security state of the reviewed contract, based on extensive audit procedure scope is "**Well Secured**".

Our Methodology

We like to work with a transparent process and make our reviews a collaborative effort. The goals of our security audits are to improve the quality of systems we review and aim for sufficient remediation to help protect users. The following is the methodology we use in our security audit process.

Manual Code Review:

In manually reviewing all of the code, we look for any potential issues with code logic, error handling, protocol and header parsing, cryptographic errors, and random number generators. We also watch for areas where more defensive programming could reduce the risk of future mistakes and speed up future audits. Although our primary focus is on the in-scope code, we examine dependency code and behavior when it is relevant to a particular line of investigation.

Vulnerability Analysis:

Our audit techniques included manual code analysis, user interface interaction, and whitebox penetration testing. We look at the project's web site to get a high level understanding of what functionality the software under review provides. We then meet with the developers to gain an appreciation of their vision of the software. We install and use the relevant software, exploring the user interactions and roles. While we do this, we brainstorm threat models and attack surfaces. We read design documentation, review other audit results, search for similar projects, examine source code dependencies, skim open issue tickets, and generally investigate details other than the implementation.

Documenting Results:

We follow a conservative, transparent process for analyzing potential security vulnerabilities and seeing them through successful remediation. Whenever a potential issue is discovered, we immediately create an Issue entry for it in this document, even though we have not yet verified the feasibility and impact of the issue. This process is conservative because we document our suspicions early even if they are later shown to not represent exploitable vulnerabilities. We generally follow a process of first documenting the suspicion with unresolved questions, then confirming the issue through code analysis, live experimentation, or automated tests. Code analysis is the most tentative, and we strive to provide test code, log captures, or screenshots demonstrating our confirmation. After this we analyze the feasibility of an attack in a live system.

Suggested Solutions:

We search for immediate mitigations that live deployments can take, and finally we suggest the requirements for remediation engineering for future releases. The mitigation and remediation recommendations should be scrutinized by the developers and deployment engineers, and successful mitigation and remediation is an ongoing collaborative process after we deliver our report, and before the details are made public.

Disclaimers

EtherAuthority.io Disclaimer

EtherAuthority team has analyzed this smart contract in accordance with the best industry practices at the date of this report, in relation to: cybersecurity vulnerabilities and issues in smart contract source code, the details of which are disclosed in this report, (Source Code); the Source Code compilation, deployment and functionality (performing the intended functions).

Due to the fact that the total number of test cases are unlimited, so the audit makes no statements or warranties on security of the code. It also cannot be considered as a sufficient assessment regarding the utility and safety of the code, bugfree status or any other statements of the contract. While we have done our best in conducting the analysis and producing this report, it is important to note that you should not rely on this report only. We also suggest to conduct a bug bounty program to confirm the high level of security of this smart contract.

Technical Disclaimer

Smart contracts are deployed and executed on blockchain platform. The platform, its programming language, and other software related to the smart contract can have their own vulnerabilities that can lead to hacks. Thus, the audit can’t guarantee explicit security of the audited smart contracts.

EtherAuthority

Email: audit@EtherAuthority.io