RD AUDITORS

SMART CONTRACT CODE REVIEW AND SECURITY ANALYSIS REPORT

Customer: Typhoon Network
Prepared on: 10/04/2021
Platform: Binance Smart Chain
Language: Solidity

info@rdauditors.com

TABLE OF CONTENTS

THIS DOCUMENT MAY CONTAIN CONFIDENTIAL INFORMATION ABOUT ITS SYSTEMS AND INTELLECTUAL PROPERTY OF THE CUSTOMER AS WELL AS INFORMATION ABOUT POTENTIAL VULNERABILITIES AND METHODS OF THEIR EXPLOITATION.

THE REPORT CONTAINING CONFIDENTIAL INFORMATION CAN BE USED INTERNALLY BY THE CUSTOMER OR IT CAN BE DISCLOSED PUBLICLY AFTER ALL VULNERABILITIES ARE FIXED - UPON DECISION OF CUSTOMER.

info@rdauditors.com

Document

Name	Smart Contract Code Review and Security Analysis Report for Typhoon Network
Platform	BSC / Solidity
File 1	BEP20Typhoon.sol
MD5 hash	D41D8CD98F00B204E9800998ECF8427E
SHA256 hash	E3B0C44298FC1C149AFBF4C8996FB92427AE41E4649B934CA495991B7852B855
File 2	BNBTyphoon.sol
MD5 hash	D2A87D3CE0CD9CE40C4F7FAB5BBD70A5
SHA256 hash	F8270F39C41BB4D609DF0C759F3FFBEC71805582F12FF7C8A33B8A93A3B3462A
File 3	MarkleTreeWithHistory.sol
MD5 hash	42137EC6F8AAF52221AD1A27EB7F4EE3
SHA256 hash	D361E8F10BF447856B05C322AAC36F46C61516961EDDD3BDE6A6F88BEE92C0A5
File 4	Typhoon.sol
MD5 hash	93462E2F0BA300132691E317FEE17942
SHA256 hash	02AA6B2B05AB6879844DDA58F3DD8918B1337AFEF540774A32D888A640CFF8DC
File 5	Veifier.sol
MD5 hash	348C991B84BE3499A9FE7C0A2A671207
SHA256 hash	4F8C89D51C19838F3D0764642C2080D5B8A6F24F682A07EA9BC601FB562B177F
Date	**10/04/2021**

info@rdauditors.com

Introduction

RD Auditors (Consultant) was contracted by Typhoon Network (Customer) to conduct a Smart Contracts Code Review and Security Analysis. This report presents the findings of the security assessment of Customer`s smart contracts and its code review conducted between April 8, 2021 – April 10, 2021.

This contract consists of five files.

Project Scope

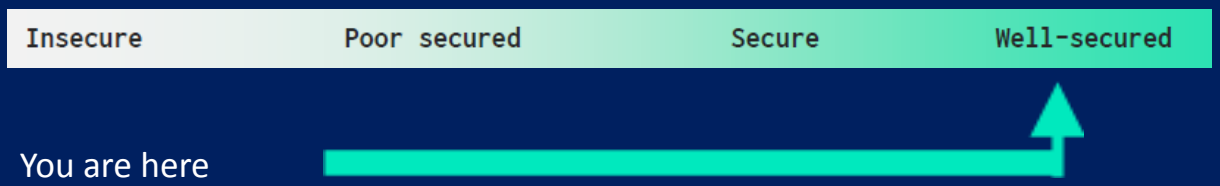
The scope of the project is a smart contract.

We have scanned this smart contract for commonly known and more specific vulnerabilities, below are those considered (the full list includes but not limited to):

- Reentrancy
- Timestamp Dependence
- Gas Limit and Loops
- DoS with (Unexpected) Throw
- DoS with Block Gas Limit
- Transaction-Ordering Dependence
- Byte array vulnerabilities
- Style guide violation
- Transfer forwards all gas
- ERC20 API violation
- Malicious libraries
- Compiler version not fixed
- Unchecked external call - Unchecked math
- Unsafe type inference
- Implicit visibility level

Executive Summary

According to the assessment, the customer`s solidity smart contract is well secured.



Automated checks are with smartDec, Mythril, Slither and remix IDE. All issues were performed by our team, which included the analysis of code functionality, manual audits found during automated analysis were manually reviewed and applicable vulnerabilities are presented in the audit overview section. The general overview is presented in the AS-IS section and all issues found are located in the audit overview section.

We found 0 critical, 0 high, 0 medium, 0 low and 0 very low level issues.

Code Quality

Typhoon Network consists of multiple smart contract files. This multiple file smart contract also contains Hasher and Pairing etc from the popular open source.

The libraries in the Typhoon 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 Typhoon.

Typhoon Network has also conducted unit tests using scripts provided through the same github link which fortify functionality and security of the contract, which also helped us to determine the integrity of the code in an automated way.

Overall, the code is well commented. Commenting provides rich documentation for functions, return variables and more and also helps auditors to quick cover the flow behind code logic. Use of Ethereum Natural Language Specification Format (NatSpec) for commenting is recommended.

Documentation

We were given a Typhoon and its supporting files in the form of the link: https://github.com/typhoonnetwork/typhoon-core/tree/master/contracts

The hash of that file is mentioned in the table. As mentioned, It's recommended to write comments in the smart contract code, 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 provides 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. Those were based on well known industry standard open source projects. And even core code blocks are written well and systematically.

AS-IS Overview

Typhoon Overview

It handles token deposit, withdrawal, pairing and tracks, using markle tree.

File And Function Level Report

File: BEP20Typhoon.sol

Contract: BEP20Typhoon
Import: typhoon
Observation: Passed
Test Report: Passed
Score: Passed
Conclusion: Passed

Sl.	Function	Type	Observation	Test Report	Conclusion	Score
1	_processDeposit	write	Passed	All Passed	No Issue	Passed
2	_processWithdraw	write	Passed	All Passed	No Issue	Passed
3	_safeBEP20TransferFrom	write	Passed	All Passed	No Issue	Passed
4	_safeBEP20Transfer	write	Passed	All Passed	No Issue	Passed

File: BNBTyphoon.sol

Contract: BNBTyphoon
Inherit: Typhoon
Import: TYphoon.sol, Initializable.sol
Observation: Passed
Test Report: Passed
Score: Passed
Conclusion: Passed

info@rdauditors.com

Sl.	Function	Type	Observation	Test Report	Conclusion	Score
1	_processDeposit	write	Passed	All Passed	No Issue	Passed
2	_processWithdraw	write	Passed	All Passed	No Issue	Passed
3	Initialize	write	Passed	All Passed	No Issue	Passed

File: MerkleTreeWithHistory.sol

Contract: MerkleTreeWithHistory
inherit: Initializable
Import: Initializable
Observation: All Passed
Test Report: Passed
Score: Passed
Conclusion: Passed

Sl.	Function	Type	Observation	Test Report	Conclusion	Score
1	initialize	write	Passed	All Passed	No Issue	Passed
2	hashLeftRight	read	Passed	All Passed	No Issue	Passed
3	_insert	write	Passed	All Passed	No Issue	Passed

File: Typhoon.sol

Contract: Typhoon
inherit: MerkleTreeWithHistory
Import: ReentrancyGuard.sol, safeMath, initializable.sol, MerkletreeWithHistory
Observation: Passed
Test Report: Passed
Score: Passed
Conclusion: Passed

Sl.	Function	Type	Observation	Test Report	Conclusion	Score
1	initialize	write	Passed	All Passed	No Issue	Passed
2	calculateFee	read	Passed	All Passed	No Issue	Passed
3	deposit	write	Passed	All Passed	No Issue	Passed
4	withdraw	write	Passed	All Passed	No Issue	Passed
5	processWithdraw	write	Passed	All Passed	No Issue	Passed
6	isSpentArray	read	Passed	All Passed	Greater array length may revert the function because of the loop	
7	IsSpent	read	Passed	All Passed	No Issue	Passed
8	Updateverifier	write	Passed	All Passed	No Issue	Passed
9	ChangeOperator	write	Passed	All Passed	No Issue	Passed
10	changeFee	write	Passed	All Passed	No Issue	Passed

NOTE: Use “for” loops wisefully so that it will not fail. These are performing core logical requirements so edit may impact workflow.

File: Verifier.sol

Contract: Verifier
Import: MerkleTreeWithHistory
Observation: Passed
Test Report: Passed
Score: Passed
Conclusion: Passed

Sl.	Function	Type	Observation	Test Report	Conclusion	Score
1	verifyingKey	read	Passed	All Passed	No Issue	Passed
2	verify	read	Passed	All Passed	No Issue	Passed
3	verifyProof	read	Passed	All Passed	No Issue	Passed
4	VerifyProof	read	Passed	All Passed	No Issue	Passed

Severity Definitions

Risk Level	Description
Critical	Critical vulnerabilities are usually straightforward to exploit and can lead to tokens lossed 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

High

No high severity vulnerabilities were found.

Medium

No Medium severity vulnerabilities were found.

Low

No Low severity vulnerabilities were found.

Very Low

No very Low severity vulnerabilities were found.

Discussion:

Kindly use loops carefully, so that it will not fail. These are performing core logical requirements, so edits may impact workflow.

info@rdauditors.com

Conclusion

We were given a contract file and have used all possible tests based on the given object. The contract is written systematically but comments were missing. We found some medium issues which have been resolved so it is ready to go for production.

Since possible test cases can be unlimited and developer level documentation (code flow diagram with function level description) not provided, for such extensive smart contract protocol, 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.

The security state of the reviewed contract is now “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

RD Auditors Disclaimer

The smart contracts given for audit have been analyzed 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).

Because 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 recommend proceeding with several independent audits and a public bug bounty program to ensure security of smart contracts.

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.

RD
AUDITORS

info@rdauditors.com