Smart Contract Audit Report

Author: Web3 Technology Solutions

Dated: 1st August, 2022

Contents

Purpose of this report

Web3 Technologies Solutions has been engaged to performed an audit of [redacted] smart contract. The purpose of this engagement has been to review the codebase for quality, security, and correctness and to report any findings.

This audit report contains details of any and all findings made during the audit process. A detailed examination of the codebase has been performed, utilizing Automated and Manual Review techniques.

The primary objectives of the audit have been to:

- Determine whether the codebase meets industry standard best practices.
- Assess the codebase to the documentation and comments match the logic and expected behavior.
- Ensure the token distribution and calculations are as per the intended behavior mentioned in the whitepaper.
- Determine ERC-721 token standards are implemented.
- Assess for efficient use of gas.
- Assess to ensure the codebase is safe from reentrancy and other vulnerabilities.

Scope of Audit

The scope of this audit was to audit [redacted] smart contract smart contract's codebase for quality, security, and correctness.

Project Name	[redacted] – Audit
Platform	Polygon (MATIC)
Language	Solidity
Codebase	[redacted]
Commit ID	20f5123945d2b24f86cfdff83ee1433a0593286f

Methodology

We have audited the smart contract both automatic and manual line by line for commonly known vulnerabilities and best practices. Here are some of the items we have audited for:

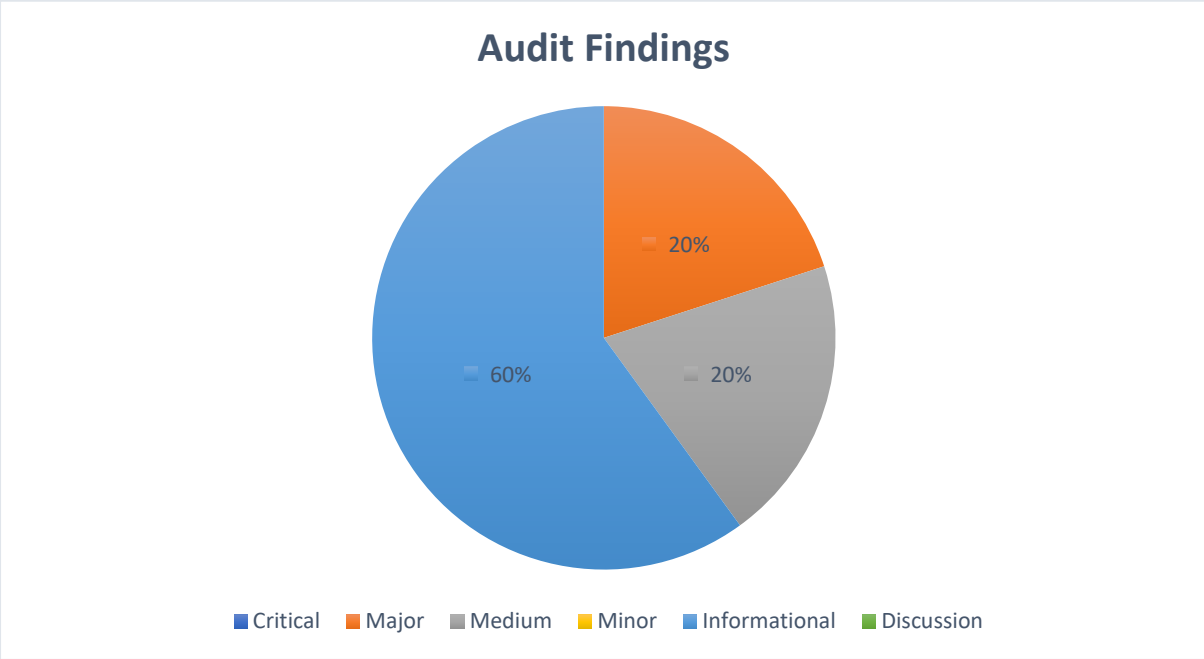
- Re-entrancy
- Timestamp Dependence
- Gas Limit and Loops
- Exception Disorder
- Gasless Send
- Use of tx.origin
- Malicious libraries
- Compiler version not fixed
- Address hardcoded
- Divide before multiply
- Integer overflow/underflow
- Using throw
- Using inline assembly

Audit Summary

We have audited the contract based on the described methodology. We have found the code quality to be Good. The contract has been found free of any known severe vulnerability and precautions to have been optimized for Gas consumption. The found issue are of Major (1), Medium (1), and Informational (3).

Audit Findings

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



ID	Title	Category	Severity	Status
W3T 01	Centralization Risks in [redacted].sol	Centralization/ Privilege	Major	Open
W3T 02	Potential Re-entrancy Attack	Logical Issue	Medium	Open
W3T 03	Missing Emit Events	Coding Style	Informational	Open
W3T 04	Missing Error Messages	Coding Style	Informational	Open
W3T 05	Short Error Message	Coding Style	Informational	Open

W3T 01 | Centralization Risk

Category	Severity	Location	Status
Centralization / Privilege	Major	A[redacted].sol: 704, 731, 736, 741, 746, 751, 757, 778, 785, 792, 847	Open

Description

[redacted]'s Contract has multiple function which has role _owner to one address. Any compromise to the _owner account may allow the hacker to take advantages of this authority.

Recommendation

We advise the client to carefully manage the privileged account's private key to avoid any potential risk. In general, we strongly recommended centralized privileges or roles in the protocol be improved. For example; multi-signature wallets, Time lock, Role Based Contract.

W3T 02 | Reentrancy Attack

Category	Severity	Location	Status
Logical Issue	Medium	[redacted].sol: 797~845, 799, 815, 847	Open

Description

We recommend applying OpenZeppelin ReentrancyGuard library - nonReentrant modifier for mentioned functions to prevent reentrancy attack.

Recommendation

We recommend applying OpenZeppelin ReentrancyGuard library - nonReentrant modifier for the aforementioned functions to prevent reentrancy attack.

W3T 03 | Missing Emit Events

Category	Severity	Location	Status
Coding Style	Informational	A[redacted].sol: 627, 704, 731, 736, 741, 746, 751, 757, 778, 785, 792, 847	Open

Description

There should always be events emitted in the sensitive functions that are controlled by centralization roles.

Recommendation

It is recommended emitting events for the sensitive functions that are controlled by centralization roles.

W3T 04 | Missing Error Messages

Category	Severity	Location	Status
Coding Style	Informational	[redacted].sol: 689, 694, 699	Open

Description

The require can be used to check for conditions and throw an exception if the condition is not met. It is better to provide a string message containing details about the error that will be passed back to the caller.

Recommendation

We advise adding error messages to the linked require statements.

W3T 05 | Short Error Messages

Category	Severity	Location	Status
Coding Style	Informational	A[redacted].sol:802,818, 835, 848, 849	Open

Description:

Use Short error message when any error message trigger less gas need to consume.

Recommendation:

Mention in Comments the error message error and use short name in the message. Like ISF in require condition and Insufficient fund in comment.

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.

Logical Issue

Logical Issue findings detail a fault in the logic of the linked code, such as an incorrect notion on how block.timestamp works.

Coding Style

Coding Style findings usually do not affect the generated byte-code but rather comment on how to make the codebase more legible and, as a result, easily maintainable.

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 Web3 Technology Solution's prior written consent in each instance.

This report does not provide any warranty or guarantee regarding the absolute bug, issues, and vulnerability -free nature of the technology and/or code analyzed. The scope of the audit neither includes nor verifies any indication of the technologies ownership, business, business model viability or legal compliance. The sole scope of this audit is to provide an assessment of the code for known vulnerabilities and compliance with industry best coding practices.

The purpose of this audit is not to provide any advice on any decision other than to help our customers increase quality of code and to reduce the risk presented by the blockchain technology.

THE CONTENT OF THIS AUDIT REPORT IS PROVIDED "AS IS" WITHOUT REPRESENTATIONS AND WARRANTIES ON THE SECURITY OF THE CODE. THOUGH WE (WEB3 TECHNOLOGY SOLUTIONS) HAVE COVERED MOST OF THE COMMON VULNERABILITIES OF SMART CONTRACT DEVELOPMENT, IT MAY NOT COVER ALL OF THE SECURITY ISSUES RELATED TO SMART CONTRACT. ONE AUDIT CANNOT BE CONSIDERED ENOUGH, WE RECOMMEND PROCEEDING WITH MULTIPLE INDEPENDENT AUDITS TO ENSURE THE SECURITY OF SMART CONTRACTS. THE AUTHOR AND HIS/HER EMPLOYER (us) DISCLAIM ANY LIABILITY FOR DAMAGES ARISING OUT OF, OR IN CONNECTION WITH, THIS REPORT. COPYRIGHT OF THIS REPORT REMAINS WITH THE AUTHOR.

WE HEREBY DISCLAIMS ALL WARRANTIES, WHETHER EXPRESS, IMPLIED, STATUTORY, OR OTHERWISE WITH RESPECT TO THE SERVICES, ASSESSMENT REPORT, OR OTHER MATERIALS. WITHOUT LIMITING THE FOREGOING, WE 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, WE 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, WE 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 US NOR ANY OF OUR 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. WE 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.