PrandomDao Audit Report

Version 1.0.0

Presented by MSB team

March 8, 2021

01. Introduction

This document contains the results of the audit of the prandomdao project conducted by the MSB team.

The audited code can be found in the public file http://prandomdao.com. this report uses the submitted version.

0x901a9DAF3F0ae17f34f6830a5de668539393D1bb

The purpose of this audit is to review the reliable implementation of prandomdao project, study potential security vulnerabilities, overal design and architecture, and identify defects that may endanger production software.

We look at specific areas of the code that have specific problems, and at possible problems in general Traversing the entire code base horizontally can improve its overall quality.

-Disclaimer

Please note that as of the date of publication, the content of this document reflects the current understanding of known security.The mode and status quo of smart contract security.

Based on the running environment of Ethereum, the implementation of solidity is audited. Regardless of the implementation The problems that may run on other blockchains or may run on other blockchains are not within the scope of this audit.

This audit does not include the risks or problems arising from the interaction between this implementation and other project contracts.

This audit does not include risks or problems arising from the use of data sources from outside the chain.

Given the size of the project, the findings detailed here are not exhaustive and require further testing and auditing It is suggested that after solving the problems involved.

-Methodology

The code base of PrandomDao is studied in detail to get a clear impression of its implementation.

Then the code base is deeply analyzed and reviewed, and a series of observations are obtained. Problems and Countermeasures. This document discusses possible solutions and, where possible, identifies common sources and solutions for such problems . There are also comments on them.

-Structure of documents

This report contains a list of issues and comments for all contract documents in the directory http://prandomdao.com And its subdirectories. Assign a severity level to each problem based on its potential impact and recommendations for resolution, If applicable. For ease of navigation, the report begins with an index by topic and by severity.

-Documents

Here's the source of the truth about how the prandomdao system should work:

http://prandomdao.com

These are considered specifications. When there is a difference with the actual code behavior, we will consult him and report a problem.

-Comments of auditee

No serious, high or moderate vulnerabilities were found in PrandomDao's code base.

All of the less serious vulnerabilities are recognized by the team, which believes they will not be discovered Will cause problems or risks and may change in future upgrades.

PrandomDao code base is audited by the MSB team.

02.About MSB

MSB is a leading technology company in the blockchain industry, providing consulting and security auditing for organizations.MSB has developed industry security standards for the design and deployment of smart contract systems.

03. severity level reference.

Each problem in this report is assigned the following severity levels:

Serious problems need to be solved as soon as possible. High severity problems may bring problems and should be solved. Problems of medium severity may cause problems and should be solved in the end.

Low severity issues are secondary details and warnings that can remain unrepaired, but are best fixed at some point in the future.

04. List of issues by severity

A. Critical

- N/A

B. High

- N/A

C. Medium

- N/A

D. Low

- FluxAggregator.sol

Shadowed Declaration

- AggregatorProxy.sol

Shadowed Declaration

Inappropriate Function Name

- interfaces/PrandomDao TokenInterface.sol

Inappropriate Parameter Names

- HECO Token Directory

Obsolete Usage

05. List of issues by contract file

- FluxAggregator.sol

Shadowed Declaration: Low

- AggregatorProxy.sol

Shadowed Declaration: Low

Inappropriate Function Name: Low

- interfaces/PrandomDaoTokenInterface.sol

Inappropriate Parameter Names: Low

- HCOToken Directory

Obsolete Usage: Low

06. Issue descriptions and recommendations by contract file.

- FluxAggregator.sol

Shadowed Declaration: Low

Source:

Line745: in the statement RoundDetails storage details = details[_queriedRoundId]; the locally declared variable details shadows the global variable details declared in the statement mapping(uint32 => RoundDetails) internal details in line 68. This causes reader confusions.

Recommendation:

Consider renaming the variable details declared in line 648 to detail and making changes in lines 617 and 630 accordingly.

Update: Acknowledged by the PrandomDao team. The team doesn't think this will cause potential issues and therefore prefers to keep it for now, and may make a change in a future upgrade.

- **AggregatorProxy.sol**

Shadowed Declaration: Low

Source:

Lines 256 and 351: the variable phaseId declared in the statement uint16 phaseId = uint16(_roundId >> PHASE_OFFSET); in line 382 and the variable phaseId defined as a function parameter in line 394 shadows the function phaseId defined in line 217.

Recommendation:

Consider renaming phaseId that appears in lines 382, 385, 394, 407 and 411 to _phaseId .

Update: Acknowledged by the PrandomDao team. The team doesn't think this will cause potential issues and therefore prefers to keep it for now, and may make a change in a future upgrade.

Inappropriate Function Name: Low

Source:

Line 373: the function addPhase implies by its name, that a "phase" will be added and some states will be updated. However it is defined as a pure function and its behavior is to compose a roundId . This function is not named in a way that describes its behavior.

This causes reader confusions.

Recommendation:

Consider renaming the function addPhase to encodeRoundId , defining it as internal and making changes in lines 134, 407 and 411 accordingly.

Update: Acknowledged by the PrandomDao team. The team doesn't think this will cause potential issues and therefore prefers to keep it for now, and may make a change in a future upgrade.

- interfaces/PrandomDaoTokenInterface.sol

Inappropriate Parameter Names: Low

Source:

Line 18: the parameter addedValue defined in the function decreaseApproval in line 18 and the parameter subtractedValue defined in the function increaseApproval in line 22 don't match their functions' behaviors respectively. This causes reader confusions.

Recommendation:

Consider swapping the two parameters.

Update: Acknowledged by the PrandomDao team. The team doesn't think this will cause potential issues and therefore prefers to keep it for now, and may make a change in a future upgrade.

- HCOToken Directory

Obsolete Usage: Low

Source: the contract files contained in this directory use older versions of Solidity compiler(as old as 0.4.24) and therefore have lots of obsolete Solidity usages.

Recommendation:

Consider rewriting the code by using a Solidity compiler with version 0.6.0 or above and replacing the obsolete usages with new usages that match the selected compiler version.

Update: Acknowledged by the PrandomDao team. The team doesn't think this will cause potential issues and therefore prefers to keep it for now, and may make a change in a future upgrade.