MixBytes()

ARAGON ONE

SMART CONTRACT

AUDIT REPORT

JANUARY 13

2020

FOREWORD
TO REPORT

A small bug can cost you millions. **MixBytes** is a team of experienced blockchain engineers that reviews your codebase and helps you avoid potential heavy losses. More than 10 years of expertise in information security and high-load services and 18 000+ lines of audited code speak for themselves. This document outlines our methodology, scope of work, and results. We would like to thank **Aragon One** for their trust and opportunity to audit their smart contracts.

CONTENT
DISCLAIMER

This report is public upon the consent of **Aragon One**. **MixBytes** is not to be held responsible for any damage arising from or connected with the report. Smart contract security audit does not guarantee an inclusive analysis disclosing all possible errors and vulnerabilities but covers the majority of issues that represent threat to smart contract operation, have been overlooked or should be fixed.

TABLE OF CONTENTS

01 INTRODUCTION TO THE AUDIT

GENERAL PROVISIONS

Aragon is a project creating software allowing to freely organize and collaborate without borders or intermediaries.

Aragon One is a Swiss company formed by the founders of the Aragon project, building the tools and community necessary for the project to succeed.

Voting Connectors are apps that serve as bridges to Aragon Voting apps requiring checkpointed balances (or any other app that requires checkpointed balances).

* Token Wrapper: wrap external tokens to a checkpointed token.
* Voting Aggregator: aggregate voting power over multiple sources.

With this in mind, **MixBytes** team was willing to contribute to Aragon ecosystem development by providing security assessment of the Voting Connectors smart contracts.

SCOPE OF THE AUDIT

The scope of the audit included:

* **Contract utils version ae01814** (except for the `test` subdirectory)
* **TokenWrapper.sol version ae01814**
* **VotingAggregator.sol version ae01814**

02 SECURITY ASSESSMENT PRINCIPLES

CLASSIFICATION OF ISSUES

CRITICAL

Bugs leading to Ether or token theft, fund access locking or any other loss of Ether/tokens to be transferred to any party (for example, dividends).

MAJOR

Bugs that can trigger a contract failure. Further recovery is possible only by manual modification of the contract state or replacement.

WARNINGS

Bugs that can break the intended contract logic or expose it to DoS attacks.

COMMENTS

Other issues and recommendations reported to/acknowledged by the team.

SECURITY ASSESSMENT METHODOLOGY

The audit was performed by 2 auditors. Stages of the audit were as follows:

1. “Blind” manual check of the code and its model
2. “Guided” manual code review
3. Checking the code compliance with customer requirements
4. Automated security analysis using the internal solidity security checker
5. Automated security analysis using public analyzers
6. Manual checklist system inspection
7. Discussion of independent audit results
8. Report preparation

03 DETECTED ISSUES

DETECTED ISSUES

CRITICAL

Not found.

MAJOR

1. VotingAggregator.sol#L299

Power source weight is not checkpointed, that makes vote manipulation possible. The issue was identified by the client after examining the intermediary audit report.

Status:

FIXED at **c25f24f**

WARNINGS

1. VotingAggregator.sol#L291

An unbound loop with external calls can have high gas consumption. As a result, block gas limit may prevent some transactions from being executed. We recommend adding a limit to the source number.

Status:

FIXED at **39c6cca**

2. VotingAggregator.sol#L131

`_weight` can be set to zero. **This check** implies that such behavior is unfavourable. We suggest adding a similar check to the `changeSourceWeight` function.

Status:

FIXED at **f31c35f**

COMMENTS

1. ActivePeriod.sol#L78

We suggest adding a check that a period with a given index exists.

Status:

DELETED - `ActivePeriod` was removed

2. Checkpointing.sol#L33
ActivePeriod.sol#L36
ActivePeriod.sol#L56

APIs of the `Checkpointing` and `ActivePeriod` libraries can be made more explicit in terms of the supported data types (`uint64` for time-like values and `uint192` for numeric values). We suggest using exact data types and forcing users of the libraries to acknowledge that by using type casts. Interestingly enough, there is a ready-made `getBlockNumber64` function, which perfectly fits into the picture.

Status:

FIXED at 935259d

3. TokenWrapper.sol#L87

We recommend adding a warning to the documentation of the `TokenWrapper` contract, stating that neither totalSupply nor any balance of the token can exceed the `MAX_UINT192` value.

Status:

FIXED at 8d0506c

4. VotingAggregator.sol#L271

Typo in the word `activation`.

Status:

DELETED - the method was removed

5. VotingAggregator.sol#L103

Many power sources with the same address can be added. Make sure that this is the expected scenario.

Status:

FIXED at be88283

6. VotingAggregator.sol#L131

The function can be executed even for a disabled power source. Make sure that this is the desired behavior.

Status:

ACKNOWLEDGED

7. VotingAggregator.sol#L297

The `_aggregateAt` function can be temporarily blocked by a malicious power source.

Status:

CHECKS ADDED at 4d9da90

8. VotingAggregator.sol#L325
ActivePeriod.sol#L128

We recommend using `assert` instead of `revert` here, since it is a better way to check the code consistency.

Status:

ACKNOWLEDGED

04 CONCLUSION AND RESULTS

Overall code quality is high. In the course of our analysis we found only a couple of minor slips, several comments and suggestions were made.

The client identified a major issue after examining the intermediary audit report. The issue was addressed and fixed properly.

The **fixed contracts** don't have any vulnerabilities according to our analysis.

ABOUT MIXBYTES

MixBytes is a team of blockchain developers, auditors and analysts keen on decentralized systems. We build open-source solutions, smart contracts and blockchain protocols, perform security audits, work on benchmarking and software testing solutions, consult universities and enterprises, do research, publish articles and documentation.

Stack

Blockchains

JOIN US