MixBytes()

OPEN ENTERPRISE TEMPLATE
SMART CONTRACT
AUDIT REPORT

NOVEMBER 20
2019

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 15 000+ lines of audited code speak for themselves. This document outlines our methodology, scope of work, and results. We would like to thank **Autark** for their trust and opportunity to audit their smart contracts.

CONTENT
DISCLAIMER

This report is public upon the consent of **Autark**. **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 software allowing to freely organize and collaborate without borders or intermediaries. Create global, bureaucracy-free organizations, companies, and communities.

Autark is an Aragon Network organization building open source tools that serve digital cooperatives and aims to revolutionize work by leveraging the corresponding challenges.

With this in mind, **MixBytes** team is willing to contribute to **Autark** development initiatives by providing security assessment of the Open Enterprise Template smart contract and its dependencies.

SCOPE OF THE AUDIT*

Audited code:

1. **BaseTemplate.sol version 0e0df6e**
2. **TokenCache.sol version 297a950**
3. **BaseOEApps version 1502373**
4. **OpenEnterpriseTemplate version 1502373**

* **The initial commits for the contracts were reviewed by MixBytes while they were in a work-in-progress stage.**

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*

CRITICAL

Not found.

MAJOR

1. OpenEnterpriseTemplate.sol#L177
   BaseTemplate.sol#L305

We advise to prohibit the burning of tokens, otherwise Rewards will not function properly. As it has not been done since the previous Rewards contract audit, we still recommend doing so.

Status:

ACKNOWLEDGED

> Acknowledged. We can't change this with respect to the template we have here, but will look into providing warnings in the frontend UI when creating merit rewards.

2. OpenEnterpriseTemplate.sol#L114
   OpenEnterpriseTemplate.sol#L143

A repeated attempt to get the token from the cache will fail, because the token is removed from the cache during the first call. We recommend abandoning the caches altogether and passing the token in function arguments.

Status:

FIXED at OpenEnterpriseTemplate.sol#L143

Client:

> The contract was in a work-in-progress state, as the review occurred in parallel to finalizing the development.

3. OpenEnterpriseTemplate.sol#L160

This call will not be valid because the current contract is not the `_vault.TRANSFER_ROLE()` permission manager (Voting has already been assigned here **OpenEnterpriseTemplate.sol#L172**). You can initially set the template as a permission manager, then call `_grantVaultPermissions` and then pass the control to Voting.

Status:

FIXED at **OpenEnterpriseTemplate.sol#L197**

Client:

> The contract was in a work-in-progress state, as the review occurred in parallel to finalizing the development.

WARNINGS

1. BaseOEApps.sol#L72

The parameters of the `Allocations.initialize` call do not match those in the `Allocations` from the npm-repository as of September 27th. We suggest using the versioning mechanics to ensure that these parameters are consistent.

Status:

FIXED at **BaseOEApps.sol#L69**

2. OpenEnterpriseTemplate.sol#L78
BaseOEApps.sol#L93
DotVoting.sol#L97-L98

There is a type mismatch. It seems that the settings were copied from the Voting initialization. We advise checking the code and making explicit type casts.

Status:

FIXED at **OpenEnterpriseTemplate.sol#L57**

3. OpenEnterpriseTemplate.sol#L193

Only the Voting app is able to create DotVoting vote, i.e. DAO members will first have to vote for creating a DotVoting vote. We recommend making sure that this is the desired behavior. As an alternative, any DAO members may be granted a permission to create a DotVoting vote (as it is done in Voting).

Status:

FIXED at OpenEnterpriseTemplate.sol#L219

COMMENTS

1. OpenEnterpriseTemplate.sol#L13

As DAO participants are given one token and the `decimals` equals 0, the token as such turns into a boolean flag of the address that belongs to the DAO. In this case, a DotVoting vote is senseless, because there is no way to distribute a vote (i.e. tokens) between several candidates. Additional tokens can be generated, but this will require the DAO to vote. We recommend making sure that this is the desired behavior.

Status:

ACKNOWLEDGED

2. BaseOEApps.sol#L64

The `UPDATE_ENTRY_ROLE` permission is not configured.

Status:

ACKNOWLEDGED

3. BaseOEApps.sol#L76

The `EXECUTE_ALLOCATION_ROLE`, `EXECUTE_PAYOUT_ROLE`, `CHANGE_PERIOD_ROLE`, and `CHANGE_BUDGETS_ROLE` permissions are not configured.

Status:

ACKNOWLEDGED

4. BaseOEApps.sol#L138

The `REMOVE_ISSUES_ROLE`, `FUND_OPEN_ISSUES_ROLE`, and `UPDATE_BOUNTIES_ROLE` permissions are not configured.

Status:

ACKNOWLEDGED

5. BaseOEApps.sol#L109

The `ROLE_MODIFY_QUORUM` and `ROLE_MODIFY_CANDIDATE_SUPPORT` permissions are not configured.

Status:

ACKNOWLEDGED

6. OpenEnterpriseTemplate.sol#L173-L174 BaseTemplate.sol#L270-L277

The `CHANGE_PERIOD_ROLE`, `CHANGE_BUDGETS_ROLE` permissions are not configured.

Status:

ACKNOWLEDGED

7. OpenEnterpriseTemplate.sol#L207-L208

The checks are redundant as they always return the `true` value.

Status:

ACKNOWLEDGED

8. BaseOEApps.sol#L41 OpenEnterpriseTemplate.sol#L33

To increase the code readability, you can set individual parameters instead of an array.

Status:

ACKNOWLEDGED

04 CONCLUSION AND RESULTS

In case DAO tokens are burned, Rewards app may issue rewards equal to 0. The client regards this as expected behaviour.

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

* The contracts were passed for MixBytes review at a work-in progress stage.

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