Choise Token Security Analysis

by Pessimistic

This report is public

February 24, 2022

Abstract

In this report, we consider the security of smart contracts of Choise Token project. Our task is to find and describe security issues in the smart contracts of the platform.

Disclaimer

The audit does not give any warranties on the security of the code. A single audit cannot be considered enough. We always recommend proceeding with several independent audits and a public bug bounty program to ensure the security of smart contracts. Besides, a security audit is not investment advice.

Summary

In this report, we considered the security of Choise Token smart contracts. We performed our audit according to the procedure described below.

The audited project is an ERC20 token which is based on OpenZeppelin implementation.

The audit did not reveal any issues.

General recommendations

We recommend improving NatSpec coverage.

Project overview

Project description

For the audit, we were provided with Choise Token project on Etherscan, address 0xBBa39Fd2935d5769116ce38d46a71bde9cf03099.

The project is based on OpenZeppelin ERC20 token standard.

The project has documentation with a description.

The project has no tests.

The total LOC of audited sources is 3.

Token details

Name:	choise.com Token
Symbol:	CHO
Decimals:	18
Total Supply:	1 000 000 000

Procedure

In our audit, we consider the following crucial features of the code:

1. Whether the code is secure.
2. Whether the code corresponds to the documentation (including whitepaper).
3. Whether the code meets best practices.

We perform our audit according to the following procedure:

- Automated analysis
    - We scan the project's codebase with the automated tool: Slither.
    - We manually verify (reject or confirm) all the issues found by the tools.
- Manual audit
    - We manually analyze the codebase for security vulnerabilities.
    - We assess the overall project structure and quality.
- Report
    - We reflect all the gathered information in the report.

Manual analysis

The contracts were completely manually analyzed, their logic was checked. Besides, the results of the automated analysis were manually verified. All the confirmed issues are described below.

Critical issues

Critical issues seriously endanger project security. They can lead to loss of funds or other catastrophic consequences. The contracts should not be deployed before these issues are fixed.

The audit showed no critical issues.

Medium severity issues

Medium issues can influence project operation in the current implementation. Bugs, loss of potential income, and other non-critical failures fall into this category, as well as potential problems related to incorrect system management. We highly recommend addressing them.

The audit showed no issues of medium severity.

Low severity issues

Low severity issues do not directly affect project operation. However, they might lead to various problems in future versions of the code. We recommend fixing them or explaining why the team has chosen a particular option.

The audit showed no issues of low severity.

This analysis was performed by Pessimistic:

Vladimir Tarasov, Security Engineer
Nikita Kirillov, Junior Security Engineer
Irina Vikhareva, Project Manager

February 24, 2022