1inch NETWORK

1inch Vesting Security Analysis

by Pessimistic

This report is public.
Published: May 31, 2021.

Abstract

In this report, we consider the security of smart contracts of 1inch vesting 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. One 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, security audit is not an investment advice.

Summary

In this report, we considered the security of 1inch vesting smart contract. We performed our audit according to the procedure described below.

The audit showed no critical, medium or low severity issues.

General recommendations

We recommend adding tests and `NatSpec` documentation to the project.

Project overview

Project description

For the audit, we were provided with 1inch vesting smart contract on a public GitHub repository, commit 23eb29884b73e0037123e7cd3ed513a4bafb3062.

The codebase is the Solidity smart contract without documentation.

The contract has no tests.

The contract compiles successfully.

The total SLOC of audited sources is 70.

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 project's code base with automated tools: Slither and SmartCheck.
  - We manually verify (reject or confirm) all found issues.
- Manual audit
  - We manually analyze code base for security vulnerabilities.
  - We assess overall project structure and quality.
  - We check smart contracts logic and compare it with the one described in the documentation.
- Report
  - We reflect all the gathered information in the report.

Manual analysis

The contract was completely manually analyzed, its 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 smart contracts security. We highly recommend fixing them.

The audit showed no critical issues.

Medium severity issues

Medium issues can influence smart contracts operation in current implementation. We highly recommend addressing them.

The audit showed no medium severity issues.

Low severity issues

Low severity issues can influence smart contracts operation in future versions of code. We recommend taking them into account.

The audit showed no low severity issues.

Notes

Overpowered role

- The contract's owner can cancel vesting at any moment and get all vested tokens by calling **StepVesting.kill** function.

  We recommend designing contracts in a trustless manner or implementing proper key management, e.g. multisig.

- There is no check if the contract holds respective tokens.

  We advise users to check the contract's balance before calling **StepVesting.claim**.

This analysis was performed by Pessimistic.

Evgeny Marchenko, Senior Security Engineer
Daria Korepanova, Security Engineer
Vladimir Tarasov, Security Engineer
Boris Nikashin, Analyst
Alexander Seleznev, Founder

May 31, 2021