1inch FixedRateSwap Security Analysis

by Pessimistic

This report is public.

Published: August 27, 2021

Abstract

In this report, we consider the security of smart contracts of 1inch network 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 network smart contracts. We performed our audit according to the procedure described below.

The audit showed two issues of low severity.

However, the project has no documentation, and the code is lacking NatSpecs.

General recommendations

We recommend adding the documentation to the project and adding a check to ensure that tokens with same decimals are used.

Project overview

Project description

For the audit, we were provided with 1inch Fixed Rate Swap project on a private GitHub repository, commit c79226adf79ce85ef1dc2f5d62e52947e6bcda23.

The project has no documentation, the code is lacking NatSpecs. For the audit, we were provided with comments on the logic of choosing the constants.

The project compiles successfully. All nine tests pass, the coverage is 87.8%.

The total LOC of audited sources is 119.

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 the issues found by tools.
- Manual audit
  - We manually analyze code base for security vulnerabilities.
  - We assess 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 smart contracts security. We highly recommend fixing them.

The audit showed no critical issues.

Medium severity issues

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

Insufficient documentation

For the audit, we were provided with a few comments that describe the logic of fee calculation and choosing the constants. However, the project has no documentation, and the code is lacking NatSpecs. As a result, it is sometimes unclear what the intention of the code is, and whether its behavior is correct, and the architecture of the project is appropriate.

Considering the complexity of the project, the documentation is critically important not only for the audit but also for development process. It should explicitly explain the purpose and behavior of the contract and main design choices.

Low severity issues

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

Code quality

Consider declaring functions `decimals()`, `swap0To1For()`, and `swap1To0For()` functions as `external` instead of `public`.

Code logic

The contract will not work correctly when swapping tokens with different values (e.g. stablecoins pegged to the same currency or wrappers of the same asset) or different `decimals` values. It is not restricted though. Consider adding appropriate checks or explicitly declaring these requirements in the documentation.

This analysis was performed by Pessimistic:

Daria Korepanova, Security Engineer
Evgeny Marchenko, Senior Security Engineer
Boris Nikashin, Analyst
Irina Vikhareva, Project Manager

August 27, 2021