1inch Farming 1.1.2 Smart Contracts Review And Verification

By: ChainSafe Systems

November 2022

1inch Farming 1.1.2 Smart Contracts Review And Verification

Auditors: Tanya Bushenyova, Anderson Lee, Oleksii Matiiasevych

WARRANTY

This Code Review is provided on an “as is” basis, without warranty of any kind, express or implied. It is not intended to provide legal advice, and any information, assessments, summaries, or recommendations are provided only for convenience (each, and collectively a “recommendation”). Recommendations are not intended to be comprehensive or applicable in all situations. ChainSafe Systems does not guarantee that the Code Review will identify all instances of security vulnerabilities or other related issues.

Introduction

1inch Network requested ChainSafe Systems to perform a review of the Farming smart contracts update. The contracts can be identified by the following git commit hash:

`8403ce63df903db66c5c8fd7958470c6827df7e6`

There are 6 contracts in scope, excluding contracts from other repositories.
After the initial review, the 1inch team applied a number of updates which can be identified by the following git commit hash:

`6b140d74cc751360e6f72d4ea68d8f3caea09bce`

Additional verification was performed after that.

Disclaimer

The review makes no statements or warranties about the utility of the code, safety of the code, suitability of the business model, regulatory regime for the business model, or any other statements about the fitness of the contracts for any specific purpose, or their bug free status.

Executive Summary

There are no known compiler bugs for the specified compiler version (0.8.12), that might affect the contracts' logic.

There were 0 critical, 0 major, 0 minor, 2 informational/optimizational issues identified in the initial version of the contracts. The issues found were not present in the final version of the contracts. They are described below for historical purposes. The code uses manual memory pointers management in some cases. The goal, as explained by the 1inch team, is to not introduce additional dependencies in the UserAccounting library, because it is used in multiple projects.

Critical Bugs and Vulnerabilities

No critical issues were identified.

Line by Line Review. Fixed Issues

1. FarmAccounting, line 38. Optimization, the condition `period == 0` could be checked at the beginning of the `startFarming()` function to implement early exit and save gas on failed transactions.

2. FarmAccounting, line 39. Optimization, the condition `period > type(uint32).max` could be checked at the beginning of the `startFarming()` function to implement early exit and save gas on failed transactions.

Tanya Bushenyova

Anderson Lee

Oleksii Matiiasevych