NCC Group
650 California St, Suite 2950
San Francisco, CA 94108
https://nccgroup.com

March 15, 2022

Algofi, Inc.
Harborside Financial Center, Office 2514
Jersey City, NJ, 07302

Introduction

During February and March 2022, Algofi engaged NCC Group to perform an implementation review of the Algofi AMM smart contract collection. The AMM collection includes a pool manager functionality, a basic Uniswap V2-like AMM implementation, together with an iterative method which computes token prices according to the StableSwap invariant. The AMM is written in PyTEAL, a Python-like language that gets compiled to Algorand's native smart contract language, TEAL.

The assessment was delivered over the course of 20 person-days by two consultants. Full source code access was provided and the Algofi Team also readily answered consultants' questions in a dedicated Slack channel. Four meetings were held in total during the project, including code walkthroughs by the Algofi Team and status updates on work progress by NCC Group consultants.

Detailed Letter of Engagement Overview

NCC Group is a global information assurance firm that, in the US, specializes in application, mobile, network, host, and product security. Security conscious companies use NCC Group's Detailed Letters of Engagement to verify product attributes in view of current security best practices, standard security functionality, and product protection. More information about the Group's processes and products can be found at https://nccgroup.com/us.

It is important to note that this document represents a point-in-time evaluation of security posture. Security threats and attacker techniques evolve rapidly, and the results of this assessment are not intended to represent an endorsement of the adequacy of current security measures against future threats. This Detailed Letter of Engagement necessarily contains information in summary form and is therefore intended for general guidance only; it is not intended as a substitute for detailed research or the exercise of professional judgment. The information presented here should not be construed as professional advice or service.

Testing Methods

The strategy used during the review was to search for general unintended behavior in contract functionalities. For each function, an intuition was built on the expected behavior of the function. Such an intuition was built based on both the function code and available documentation (source code comments). When reasonable, testing was used to confirm the intuition.

Commit `daaaf4efa6` of the https://github.com/algofiorg/algofi-amm/ repository was in scope. It contains three components:

- **Pool manager:** Pool registration, global cross-pool variables, fees and limits, etc.
- **AMM pool implementation:** Pooling, burning, swapping and flash lending, etc.
- **StableSwap invariant**: Iterative price calculation according to StableSwap.

The review focused on the following areas:

- **Teal Contract Analysis,** including:
    - Identification of dangerous code paths using manual review and automated analysis tools
    - Evaluation of security impact when encountering exceptional or unintended code paths, including multi-contract scenarios, gasless spend, or exhausted call stack
    - Review of mechanisms to safely provide liquidity without risk of loss of funds
    - Verification that user trading is completed according to an anticipated mathematical model
    - Evaluation of state management within the contract, including proper transition during successful and unsuccessful function calls
    - Evaluation of time-related functions and ensuring that an attacker is unable to gain an advantage
    - Verification of the precision for fixed-point math
    - Review of common smart contract vulnerabilities such as described on the Decentralized Application Security Project (http://dasp.co/)
- **Teal Contract Attacker Analysis,** including the ability to:
    - Compel execution of unintended code
    - Bypass contract logic or validation routines
    - Transfer assets without proper authorization
    - Compromise critical operations
- **Blockchain Structures and Algorithms Analysis**
    - Token Ownership - code and the consensus rules to ensure that ownership of tokens is correctly enforced
    - Access Control - core authorization policies used to identify authorized parties and regulate their actions on the network
    - Transaction Processing - mechanisms used to process transactions, including those used to validate transaction data and preserve transaction invariants
    - Distributed Ledger Consensus - mechanisms used to replicate and validate state changes to ensure they cannot be abused to violate guarantees.

Summary of Findings

This review did not uncover substantial security flaws. It should be noted, however, that the absence of security bugs is not guaranteed, as the review was best-effort and should not be considered as an absolute safety guarantee.

During the assessment, NCC Group identified:

- Two (2) low severity vulnerabilities
- Four (4) informational findings

These findings are briefly summarized here:

- **Temporary Early-Liquidity Pool Monopolization:** An early liquidity provider can temporarily monopolize the pool. It will be possible to de-monopolize the pool, but it will require a flash loan and induce a flash loan fee.
- **False Positives In Overflow Condition Evaluation:** The amount of LP tokens users receive can be less than users expect.
- **Amplification Factor Ramp-Up Renders Checks Unnecessary:** An implementation quirk in amplification factor ramp-up code results in a check that becomes redundant as soon as the first ramp-up is triggered.

- **Inner Flash Loan Transactions Can Self-Reference Pools:** Some edge-case transactions which would work in normal circumstances would fail if executed inside a flash loan context.
- **Fragility in Flash Loan Repay Validation:** Future contract upgrades must not add support for transaction groups that have payment-to-pool transactions as last transaction in the group. In addition, it is not possible for users to take flash loans from multiple pools atomically.

One of the informational findings was deemed a false positive, and is not included above. Upon completion of the assessment, all findings were reported to Algofi along with recommendations.

Prepared by NCC Group Security Services for AlgoFi Inc. Portions of this document and the templates used in its production are the property of NCC Group and cannot be copied (in full or in part) without NCC Group's permission. While precautions have been taken in the preparation of this document, NCC Group the publisher, and the author (s) assume no responsibility for errors, omissions, or for damages resulting from the use of the information contained herein. Use of NCC Group's services does not guarantee the security of a system, or that computer intrusions will not occur.