decurity

Smart Contract Security Audit Report

1inch

1. Contents

2. General Information

This report contains information about the results of the security audit of the 1inch (hereafter referred to as "Customer") smart contracts, conducted by Decurity in the period from 02/05/2024 to 02/08/2024.

2.1. Introduction

Tasks solved during the work are:

- Review the protocol design and the usage of 3rd party dependencies,
- Audit the contracts implementation,
- Develop the recommendations and suggestions to improve the security of the contracts.

2.2. Scope of Work

The audit scope included the changes in the following pull requests:

- https://github.com/1inch/limit-order-protocol/pull/303 (commit 3169ea46932ef44114a215a60d1d91ef022b416d)
- https://github.com/1inch/1inch-contract/pull/281 (commit 40fec29d681799b9dc2603c5751157a226099a35)

2.3. Threat Model

The assessment presumes the actions of an intruder who might have the capabilities of any role (an external user, token owner, token service owner, or a contract). The risks of centralization were not taken into account at the Customer's request.

The main possible threat actors are:

- Users (takers and makers),
- Protocol owners,
- Executors,

- Token contracts, etc.

2.4. Weakness Scoring

An expert evaluation scores the findings in this report, and the impact of each vulnerability is calculated based on its ease of exploitation (based on the industry practice and our experience) and severity (for the considered threats).

2.5. Disclaimer

Due to the intrinsic nature of the software and vulnerabilities and the changing threat landscape, it cannot be generally guaranteed that a certain security property of a program holds.

Therefore, this report is provided “as is” and is not a guarantee that the analyzed system does not contain any other security weaknesses or vulnerabilities. Furthermore, this report is not an endorsement of the Customer’s project, nor is it an investment advice.

That being said, Decurity exercises the best effort to perform its contractual obligations and follow the industry methodologies to discover as many weaknesses as possible and maximize the audit coverage using limited resources.

3. Summary

As a result of this work, we haven’t discovered any exploitable security issues.

The 1inch team has given feedback for the suggested changes and an explanation for the underlying code.

3.1. Suggestions

The table below contains the discovered issues, their risk level, and their status as of February 5, 2024.

Table. Discovered weaknesses

Issue	Contract	Risk Level	Status
One instance of SELFDESTRUCT left	https://github.com/1inch/1inch-contract/blob/cb472e7d0919918195ff3f14d463743a2738a1eb/contracts/executors/AggregationExecutorBase.sol	**Info**	Acknowledged

4. General Recommendations

This section contains general recommendations on how to improve the overall security level.

The Findings section contains technical recommendations for each discovered issue.

4.1. Security Process Improvement

The following is a brief long-term action plan to mitigate further weaknesses and bring the product security to a higher level:

- Keep the whitepaper and documentation updated to make it consistent with the implementation and the intended use cases of the system,
- Perform regular audits for all the new contracts and updates,
- Ensure the secure off-chain storage and processing of the credentials (e.g. the privileged private keys),
- Launch a public bug bounty campaign for the contracts.

5. Findings

5.1. One instance of SELFDESTRUCT left

Risk Level: **Info**

Status: The team commented that this is intentional.

Description:

There's one call to `selfdestruct` still present in one of the executors: https://github.com/1inch/1inch-contract/blob/cb472e7d0919918195ff3f14d463743a2738a1eb/contracts/executors/AggregationExecutorBase.sol#L62

Remediation:

Review the code and decide whether this executor needs to be refactored.

6. Appendix

6.1. About us

The Decurity team consists of experienced hackers who have been doing application security assessments and penetration testing for over a decade.

During the recent years, we've gained expertise in the blockchain field and have conducted numerous audits for both centralized and decentralized projects: exchanges, protocols, and blockchain nodes.

Our efforts have helped to protect hundreds of millions of dollars and make web3 a safer place.