AstraSec

1inch Protocol Fees Security Audit Report

April 19, 2025

Contents

1 Introduction

1.1 About 1inch Protocol Fees

The protocol fees feature introduces fees taken from resolvers and from the exchange price that is above market price. The resolver fees consist of two components: integrator fees and resolver fees, which are configured sequentially by the backend during order creation. The surplus fee is calculated based on the positive difference between the filling price and the reference price..

1.2 Source Code

The following source code was reviewed during the audit:

- https://github.com/1inch/fusion-protocol
- CommitID: c0197a5

  contracts/SimpleSettlement.sol
- https://github.com/1inch/limit-order-protocol
- CommitID: cf8e50e

  contracts/extensions/FeeTaker.sol
  contracts/extensions/AmountGetterWithFee.sol
  contracts/extensions/AmountGetterBase.sol

2 Overall Assessment

This report has been compiled to identify issues and vulnerabilities within the 1inch protocol fees feature. During this audit, we utilized auxiliary tool techniques to complement our thorough manual code review. The code is well-designed and engineered, demonstrating adherence to best practices in security and functionality. No issues, vulnerabilities, or inefficiencies were identified during the audit.

Severity	Count	Acknowledged	Won't Do	Addressed
Critical	–	–	–	–
High	–	–	–	–
Medium	–	–	–	–
Low	–	–	–	–
Informational	–	–	–	–
Undetermined	–	–	–	–

3 Vulnerability Summary

3.1 Overview

After completing the audit, we conclude that the implementation of the 1inch protocol fees feature is well-structured and expertly engineered, with no vulnerability identified.

3.2 Security Level Reference

In web3 smart contract audits, vulnerabilities are typically classified into different severity levels based on the potential impact they can have on the security and functionality of the contract. Here are the definitions for critical-severity, high-severity, medium-severity, and low-severity vulnerabilities:

Severity	Acknowledged
C-X (Critical)	A severe security flaw with immediate and significant negative consequences. It poses high risks, such as unauthorized access, financial losses, or complete disruption of functionality. Requires immediate attention and remediation.
H-X (High)	Significant security issues that can lead to substantial risks. Although not as severe as critical vulnerabilities, they can still result in unauthorized access, manipulation of contract state, or financial losses. Prompt remediation is necessary.
M-X (Medium)	Moderately impactful security weaknesses that require attention and re-mediation. They may lead to limited unauthorized access, minor financial losses, or potential disruptions to functionality.
L-X (Low)	Minor security issues with limited impact. While they may not pose significant risks, it is still recommended to address them to maintain a robust and secure smart contract.
I-X (Informational)	Warnings and things to keep in mind when operating the protocol. No immediate action required.
U-X (Undetermined)	Identified security flaw requiring further investigation. Severity and impact need to be determined. Additional assessment and analysis are necessary.

4 Appendix

4.1 About AstraSec

AstraSec is a blockchain security company that serves to provide high-quality auditing services for blockchain-based protocols. With a team of blockchain specialists, AstraSec maintains a strong commitment to excellence and client satisfaction. The audit team members have extensive audit experience for various famous DeFi projects. AstraSec's comprehensive approach and deep blockchain understanding make it a trusted partner for the clients.

4.2 Disclaimer

The information provided in this audit report is for reference only and does not constitute any legal, financial, or investment advice. Any views, suggestions, or conclusions in the audit report are based on the limited information and conditions obtained during the audit process and may be subject to unknown risks and uncertainties. While we make every effort to ensure the accuracy and completeness of the audit report, we are not responsible for any errors or omissions in the report.

We recommend users to carefully consider the information in the audit report based on their own independent judgment and professional advice before making any decisions. We are not responsible for the consequences of the use of the audit report, including but not limited to any losses or damages resulting from reliance on the audit report.

This audit report is for reference only and should not be considered a substitute for legal documents or contracts.

4.3 Contact

Phone	+86 156 0639 2692
Email	contact@astrasec.ai
Twitter	https://twitter.com/AstraSecAI