SMART CONTRACT AUDIT REPORT

for

1inch Aggregation Router (V5)

Prepared By: Xiaomi Huang

PeckShield

July 28, 2022

Document Properties

Client	1inch Network
Title	Smart Contract Audit Report
Target	1inch
Version	1.0
Author	Xuxian Jiang
Auditors	Xiaotao Wu, Xuxian Jiang
Reviewed by	Xiaomi Huang
Approved by	Xuxian Jiang
Classification	Public

Version Info

Version	Date	Author(s)	Description
1.0	July 28, 2022	Xuxian Jiang	Final Release
1.0-rc1	July 26, 2022	Xuxian Jiang	Release Candidate #1

Contact

For more information about this document and its contents, please contact PeckShield Inc.

Name	Xiaomi Huang
Phone	+86 183 5897 7782
Email	contact@peckshield.com

Contents

1 Introduction

Given the opportunity to review the design document and related smart contract source code of the 1inch Aggregation Router protocol (v5), we outline in the report our systematic approach to evaluate potential security issues in the smart contract implementation, expose possible semantic inconsistencies between smart contract code and design document, and provide additional suggestions or recommendations for improvement. Our results show that the given version of smart contracts can be further improved due to the presence of several issues related to either security or performance. This document outlines our audit results.

1.1 About 1inch

1inch is a DeFi aggregator and a decentralized exchange with smart routing. The core protocol connects a large number of decentralized and centralized platforms in order to minimize price slippage and find the optimal trade for the users. The smart contracts reviewed are designed to create a universal exchange for tokens. Major changes within the scope are numerous gas optimization, the support of ClipperV2, as well as custom errors support. The basic information of the audited protocol is as follows:

Table 1.1: Basic Information of The 1inch

Item	Description
Issuer	1inch Network
Website	https://app.1inch.io/
Type	EVM Smart Contract
Platform	Solidity
Audit Method	Whitebox
Latest Audit Report	July 28, 2022

In the following, we show the Git repository of reviewed files and the commit hash value used in this audit.

- https://github.com/1inch/1inch-contract/compare/v4-release...v5-audit-pre-release-v2 (47f1bc6b)

1.2 About PeckShield

PeckShield Inc. [7] is a leading blockchain security company with the goal of elevating the security, privacy, and usability of current blockchain ecosystems by offering top-notch, industry-leading services and products (including the service of smart contract auditing). We are reachable at Telegram (https://t.me/peckshield), Twitter (http://twitter.com/peckshield), or Email (contact@peckshield.com).

Table 1.2: Vulnerability Severity Classification

Impact \ Likelihood	*High*	*Medium*	*Low*
High	Critical	High	Medium
Medium	High	Medium	Low
Low	Medium	Low	Low

1.3 Methodology

To standardize the evaluation, we define the following terminology based on OWASP Risk Rating Methodology [6]:

- Likelihood represents how likely a particular vulnerability is to be uncovered and exploited in the wild;
- Impact measures the technical loss and business damage of a successful attack;
- Severity demonstrates the overall criticality of the risk.

Likelihood and impact are categorized into three ratings: *H*, *M* and *L*, i.e., *high*, *medium* and *low* respectively. Severity is determined by likelihood and impact and can be classified into four categories accordingly, i.e., *Critical*, *High*, *Medium*, *Low* shown in Table 1.2.

To evaluate the risk, we go through a list of check items and each would be labeled with a severity category. For one check item, if our tool or analysis does not identify any issue, the contract is considered safe regarding the check item. For any discovered issue, we might further

Table 1.3: The Full List of Check Items

Category	Check Item
Basic Coding Bugs	Constructor Mismatch
	Ownership Takeover
	Redundant Fallback Function
	Overflows & Underflows
	Reentrancy
	Money-Giving Bug
	Blackhole
	Unauthorized Self-Destruct
	Revert DoS
	Unchecked External Call
	Gasless Send
	Send Instead Of Transfer
	Costly Loop
	(Unsafe) Use Of Untrusted Libraries
	(Unsafe) Use Of Predictable Variables
	Transaction Ordering Dependence
	Deprecated Uses
Semantic Consistency Checks	Semantic Consistency Checks
Advanced DeFi Scrutiny	Business Logics Review
	Functionality Checks
	Authentication Management
	Access Control & Authorization
	Oracle Security
	Digital Asset Escrow
	Kill-Switch Mechanism
	Operation Trails & Event Generation
	ERC20 Idiosyncrasies Handling
	Frontend-Contract Integration
	Deployment Consistency
	Holistic Risk Management
Additional Recommendations	Avoiding Use of Variadic Byte Array
	Using Fixed Compiler Version
	Making Visibility Level Explicit
	Making Type Inference Explicit
	Adhering To Function Declaration Strictly
	Following Other Best Practices

deploy contracts on our private testnet and run tests to confirm the findings. If necessary, we would additionally build a PoC to demonstrate the possibility of exploitation. The concrete list of check items is shown in Table 1.3.

In particular, we perform the audit according to the following procedure:

- Basic Coding Bugs: We first statically analyze given smart contracts with our proprietary static code analyzer for known coding bugs, and then manually verify (reject or confirm) all the issues found by our tool.

- Semantic Consistency Checks: We then manually check the logic of implemented smart contracts and compare with the description in the white paper.

- Advanced DeFi Scrutiny: We further review business logics, examine system operations, and place DeFi-related aspects under scrutiny to uncover possible pitfalls and/or bugs.

- Additional Recommendations: We also provide additional suggestions regarding the coding and development of smart contracts from the perspective of proven programming practices.

To better describe each issue we identified, we categorize the findings with Common Weakness Enumeration (CWE-699) [5], which is a community-developed list of software weakness types to better delineate and organize weaknesses around concepts frequently encountered in software development. Though some categories used in CWE-699 may not be relevant in smart contracts, we use the CWE categories in Table 1.4 to classify our findings.

1.4 Disclaimer

Note that this security audit is not designed to replace functional tests required before any software release, and does not give any warranties on finding all possible security issues of the given smart contract(s) or blockchain software, i.e., the evaluation result does not guarantee the nonexistence of any further findings of security issues. As one audit-based assessment cannot be considered comprehensive, we always recommend proceeding with several independent audits and a public bug bounty program to ensure the security of smart contract(s). Last but not least, this security audit should not be used as investment advice.

Table 1.4: Common Weakness Enumeration (CWE) Classifications Used in This Audit

Category	Summary
Configuration	Weaknesses in this category are typically introduced during the configuration of the software.
Data Processing Issues	Weaknesses in this category are typically found in functionality that processes data.
Numeric Errors	Weaknesses in this category are related to improper calculation or conversion of numbers.
Security Features	Weaknesses in this category are concerned with topics like authentication, access control, confidentiality, cryptography, and privilege management. (Software security is not security software.)
Time and State	Weaknesses in this category are related to the improper management of time and state in an environment that supports simultaneous or near-simultaneous computation by multiple systems, processes, or threads.
Error Conditions, Return Values, Status Codes	Weaknesses in this category include weaknesses that occur if a function does not generate the correct return/status code, or if the application does not handle all possible return/status codes that could be generated by a function.
Resource Management	Weaknesses in this category are related to improper management of system resources.
Behavioral Issues	Weaknesses in this category are related to unexpected behaviors from code that an application uses.
Business Logics	Weaknesses in this category identify some of the underlying problems that commonly allow attackers to manipulate the business logic of an application. Errors in business logic can be devastating to an entire application.
Initialization and Cleanup	Weaknesses in this category occur in behaviors that are used for initialization and breakdown.
Arguments and Parameters	Weaknesses in this category are related to improper use of arguments or parameters within function calls.
Expression Issues	Weaknesses in this category are related to incorrectly written expressions within code.
Coding Practices	Weaknesses in this category are related to coding practices that are deemed unsafe and increase the chances that an exploitable vulnerability will be present in the application. They may not directly introduce a vulnerability, but indicate the product has not been carefully developed or maintained.

2 Findings

2.1 Summary

Here is a summary of our findings after analyzing the `1inch` protocol implementation. During the first phase of our audit, we study the smart contract source code and run our in-house static code analyzer through the codebase. The purpose here is to statically identify known coding bugs, and then manually verify (reject or confirm) issues reported by our tool. We further manually review business logics, examine system operations, and place DeFi-related aspects under scrutiny to uncover possible pitfalls and/or bugs.

Severity	# of Findings	
Critical	0	
High	0	
Medium	2	🟦🟦
Low	2	🟦🟦
Informational	0	
Total	4	

We have so far identified a list of potential issues: some of them involve subtle corner cases that might not be previously thought of, while others refer to unusual interactions among multiple contracts. For each uncovered issue, we have therefore developed test cases for reasoning, reproduction, and/or verification. After further analysis and internal discussion, we determined a few issues of varying severities that need to be brought up and paid more attention to, which are categorized in the above table. More information can be found in the next subsection, and the detailed discussions of each of them are in Section 3.

2.2 Key Findings

Overall, these smart contracts are well-designed and engineered, though the implementation can be improved by resolving the identified issues (shown in Table 2.1), including 2 medium-severity vulnerabilities and 2 low-severity vulnerabilities.

Table 2.1: Key 1inch Audit Findings

ID	Severity	Title	Category	Status
PVE-001	Medium	Revisited Logic in LimitedAmountExtension	Coding Practices	Resolved
PVE-002	Low	Improved Logic in LeftoversExtension::_processLeftovers()	Coding Practices	Confirmed
PVE-003	Low	Improved Logic in UniswapV2Extension::swapUniV2()	Coding Practices	Resolved
PVE-004	Medium	Trust Issue of Admin Keys	Security Features	Mitigated

Besides recommending specific countermeasures to mitigate these issues, we also emphasize that it is always important to develop necessary risk-control mechanisms and make contingency plans, which may need to be exercised before the mainnet deployment. The risk-control mechanisms need to kick in at the very moment when the contracts are being deployed in mainnet. Please refer to Section 3 for details.

3 | Detailed Results

3.1 Revisited Logic in LimitedAmountExtension

- ID: PVE-001
- Severity: Low
- Likelihood: Low
- Impact: Low
- Target: `LimitedAmountExtension`
- Category: Coding Practices [4]
- CWE subcategory: CWE-1126 [1]

Description

The `AggregationRouterV5` contract in `1inch` supports a number of extensions. Among the supported extensions, `LimitedAmountExtension` is patch-friendly one with the customized support of at most two calls. While reviewing the implementation of this extension, we notice that the current implementation needs to be improved.

To elaborate, we show below the related code snippet of the `_limited()` function. Specifically, this function is designed to make at most two external calls (lines 26 and 29). These two calls are indicated by the given arguments `offsets`. The current logic relies on the initial requirement statement, i.e., `offsets >> 16 != 0 && offsets >> 32 == 0`, which needs to be adjusted as follows: `require( offsets&0xffff !=0 && offsets>>32 == 0);` and `require(amount<=limit || ((offsets>>16)> offsets&0xffff));`.

```
23      function _limited(uint256 amount, uint256 limit, uint256 offsets, bytes calldata
            data) private returns (uint256 result) {
24          if (offsets >> 16 != 0 && offsets >> 32 == 0) revert ShouldHaveExactlyTwoCalls()
                ;
25
26          result = _slice(data, 0, offsets & 0xffff).makeCall(Math.min(amount, limit));
27          if (amount > limit) {
28              unchecked {
29                  _slice(data, offsets & 0xffff, (offsets >> 16) & 0xffff).makeCall(amount
                        - limit);
30              }
31          }
32     }
```

Listing 3.1: `LimitedAmountExtension::_limited()`

Recommendation Validate the input arguments of the above `_limited()` routine by ensuring the given offsets are valid.

Status This issue has been fixed in the following commit: `5fc5af9`.

3.2 Improved Logic in LeftoversExtension::_processLeftovers()

- ID: PVE-002
- Severity: Low
- Likelihood: Low
- Impact: Low
- Target: `LeftoversExtension`
- Category: Coding Practices [4]
- CWE subcategory: CWE-1126 [1]

Description

As mentioned earlier, the `AggregationRouterV5` contract in `1inch` supports a number of extensions. In this section, we examine the `LeftoversExtension` that is designed to process leftovers. While reviewing the current implementation, we notice the core handling routine can be improved.

To elaborate, we show below the related code snippet of the `_processLeftovers()` function. This function supports the handling of the so-called referrer fee,which is computed as `referrerFee = (referrer != address(0))? leftovers * numerator / denominator : 0` (lines 80). Since the variable `denominator` is used as the divisor, it is better to ensure it is not 0. In other words, we can improve the current computation as follows: `referrerFee = (referrer != address(0)&& denominator != 0)? leftovers * numerator / denominator : 0`.

```
64     function _processLeftovers(
65         IERC20 token,
66         uint256 guaranteedAmount,
67         uint256 threshold,
68         uint256 numerator,
69         uint256 denominator,
70         address payable referrer,
71         uint256 amount
72     ) private returns(uint256) {
73         if (amount <= guaranteedAmount) {
74             return amount;
75         }
76 
77         unchecked {
78             uint256 leftovers = amount - guaranteedAmount;
```

```
            if (leftovers > threshold) {
                uint256 referrerFee = (referrer != address(0)) ? leftovers * numerator / denominator : 0;
                uint256 adminFee = leftovers - referrerFee;

                if (adminFee > threshold) {
                    token.uniTransfer(_feeReceiver, adminFee);
                    amount -= adminFee;
                }

                if (referrerFee > threshold) {
                    token.uniTransfer(referrer, referrerFee);
                    amount -= referrerFee;
                }
            }

            return amount;
        }
    }
```

Listing 3.2: `LeftoversExtension::_processLeftovers()`

Recommendation Improve the above `_processLeftovers()` routine to ensure 0 will not be as the divisor.

Status This issue has been confirmed and the team will exercise extra care in never generating `denominator == 0` on the backend.

3.3 Improved Logic in UniswapV2Extension::swapUniV2()

- ID: PVE-003
- Severity: Low
- Likelihood: Low
- Impact: Low
- Target: `UniswapV2Extension`
- Category: Coding Practices [4]
- CWE subcategory: CWE-1126 [1]

Description

Among the supported extensions in `AggregationRouterV5`, `UniswapV2Extension` allows for the interaction with `UniswapV2`-based DEX engines. The associated support makes heavy use of assembly for gas optimization. While reviewing the implementation of this extension, we notice a possibility to improve the current implementation.

To elaborate, we show below the related code snippet of the `swapUniV2()` function. In particular, at the end of `swapUniV2()`, there is an external actual `swap()` call which requires proper preparation of arguments. So far, it takes four ending call of four arguments: `uint256 amount0Out`, `uint256 amount1Out`, `address to`, and `bytes calldata data`. While the first three arguments are properly prepared, the last one `bytes calldata data` can be improved. Specifically, its current logic of `mstore(add(ptr, 0x64), 0x80)` only initializes the offset of `bytes calldata data`, but not the length. In other words, we can explicitly initialize the length by the following statement: `mstore(add(ptr, 0x84), 0)`.

```
    function swapUniV2() external returns (uint256 result) {
        bytes4 getReservesSelector = IUniswapV2Pair.getReserves.selector;
        bytes4 swapSelector = IUniswapV2Pair.swap.selector;
        bytes4 swapBrokenSelector = IUniswapV2BrokenPair.swap.selector;
        bytes4 exceptionReturnAmountIsNotEnough = Errors.ReturnAmountIsNotEnough.
            selector;
        assembly {  // solhint-disable-line no-inline-assembly
            let ptr := mload(0x40)

            let firstBytes := byte(0, calldataload(4))
            let flip := shr(_FLIP_BIT, firstBytes)
            let broken := and(1, shr(_BROKEN_BIT, firstBytes))
            let fee := shr(224, calldataload(5))
            let pair := shr(96, calldataload(9))

            let offset := 29
            let destination
            if and(_HAS_DESTINATION_FLAG, firstBytes) {
                destination := shr(96, calldataload(offset))
                offset := add(offset, 20)
            }
            if iszero(destination) {
                destination := address()
            }
            let minReturn
            if and(_HAS_MIN_RETURN_FLAG, firstBytes) {
                minReturn := calldataload(offset)
                offset := add(offset, 32)
            }
            let amount := calldataload(offset)

            {  // Stack too deeep
                let reserve0
                let reserve1
                mstore(0, getReservesSelector)
                if iszero(staticcall(gas(), pair, 0, 0x04, 0, 0x40)) {
                    returndatacopy(ptr, 0, returndatasize())
                    revert(ptr, returndatasize())
                }

                switch flip
                case 1 {
                    reserve1 := mload(0x00)
                    reserve0 := mload(0x20)
                }
                case 0 {
                    reserve0 := mload(0x00)
                    reserve1 := mload(0x20)
                }

                let feeDenom := _DENOMINATOR
                if gt(fee, _DENOMINATOR) {
                    feeDenom := _SCALED_DENOMINATOR
                }

                let amountInWithFee := mul(amount, sub(feeDenom, fee))
                let numerator := mul(amountInWithFee, reserve1)
                let denominator := add(mul(reserve0, feeDenom), amountInWithFee)
                amount := div(numerator, denominator)  // we use amount instead of result here due to stack too deep error
            }

            result := amount  // put result where it should be
            if lt(result, minReturn) {
                mstore(0, exceptionReturnAmountIsNotEnough)
                revert(0, 4)
            }

            switch broken
            case 1 {
                mstore(ptr, swapBrokenSelector)
            }
            case 0 {
                mstore(ptr, swapSelector)
            }
            mstore(add(ptr, 0x04), mul(result, flip))
            mstore(add(ptr, 0x24), mul(result, iszero(flip)))
            mstore(add(ptr, 0x44), destination)
            mstore(add(ptr, 0x64), 0x80)

            if iszero(call(gas(), pair, 0, ptr, sub(0xa4, mul(broken, 0x40)), 0, 0)) {
                returndatacopy(ptr, 0, returndatasize())
                revert(ptr, returndatasize())
            }
        }
```

Listing 3.3: `UniswapV2Extension::swapUniV2()`

Recommendation Improve the above `swapUniV2()` routine by also initializing the required length of the last argument.

Status This issue has been fixed in the following commit: `8e7d5cf`.

3.4 Trust Issue of Admin Keys

- ID: PVE-004
- Severity: Medium
- Likelihood: Medium
- Impact: Medium
- Target: AggregationRouterV5
- Category: Security Features [3]
- CWE subcategory: CWE-287 [2]

Description

In the 1inch protocol, there is a privileged account, i.e., owner. The owner account can be used to recover the funds or even destroy the AggregationRouterV5 contract. Our analysis shows that this privileged account needs to be scrutinized. In the following, we show the representative function potentially affected by the privileges of the owner account.

```
    function rescueFunds(IERC20 token, uint256 amount) external onlyOwner {
        token.uniTransfer(payable(msg.sender), amount);
    }

    function destroy() external onlyOwner {
        selfdestruct(payable(msg.sender));
    }
```

Listing 3.4: AggregationRouterV5::rescueFunds()/destroy()

We understand the need of the privileged functions for contract maintenance, but at the same time the extra power to the owner may also be a counter-party risk to the protocol users. It is worrisome if the privileged owner account is a plain EOA account. Note that a multi-sig account could greatly alleviate this concern, though it is still far from perfect. Specifically, a better approach is to eliminate the administration key concern by transferring the role to a community-governed DAO.

Recommendation Promptly transfer the privileged account to the intended DAO-like governance contract. All changed to privileged operations may need to be mediated with necessary timelocks. Eventually, activate the normal on-chain community-based governance life-cycle and ensure the intended trustless nature and high-quality distributed governance.

Status This issue has been mitigated as the team confirms that multi-sig will be adopted for the privileged account.

4 Conclusion

In this audit, we have analyzed the design and implementation of the `1inch Aggregation Router` protocol (v5). `1inch` is a `DeFi` aggregator and a decentralized exchange with smart routing. The core protocol connects a large number of decentralized and centralized platforms in order to minimize price slippage and find the optimal trade for the users. The current code base is well structured and neatly organized. Those identified issues are promptly confirmed and addressed.

Meanwhile, we need to emphasize that `Solidity`-based smart contracts as a whole are still in an early, but exciting stage of development. To improve this report, we greatly appreciate any constructive feedbacks or suggestions, on our methodology, audit findings, or potential gaps in scope/coverage.

References

[1] MITRE. CWE-1126: Declaration of Variable with Unnecessarily Wide Scope. https://cwe.mitre.org/data/definitions/1126.html.

[2] MITRE. CWE-287: Improper Authentication. https://cwe.mitre.org/data/definitions/287.html.

[3] MITRE. CWE CATEGORY: 7PK - Security Features. https://cwe.mitre.org/data/definitions/254.html.

[4] MITRE. CWE CATEGORY: Bad Coding Practices. https://cwe.mitre.org/data/definitions/1006.html.

[5] MITRE. CWE VIEW: Development Concepts. https://cwe.mitre.org/data/definitions/699.html.

[6] OWASP. Risk Rating Methodology. https://www.owasp.org/index.php/OWASP_Risk_Rating_Methodology.

[7] PeckShield. PeckShield Inc. https://www.peckshield.com.