SMART CONTRACT AUDIT REPORT

for

Tokenlon (Multicall)

Prepared By: Patrick Lou

PeckShield

July 6, 2022

Document Properties

Client	Tokenlon
Title	Smart Contract Audit Report
Target	Tokenlon (Multicall)
Version	1.0
Author	Xuxian Jiang
Auditors	Jing Wang, Patrick Lou, Xuxian Jiang
Reviewed by	Patrick Lou
Approved by	Xuxian Jiang
Classification	Public

Version Info

Version	Date	Author(s)	Description
1.0	July 6, 2022	Xuxian Jiang	Final Release
1.0-rc	July 2, 2022	Xuxian Jiang	Release Candidate #1

Contact

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

Name	Patrick Lou
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 `multicall` support in `Tokenlon`, 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 Tokenlon

`Tokenlon` is originally based on the `0x` protocol for decentralized atomic currency exchange, which provides users with faster speed, better price decentralized currency exchange services. It is different from other decentralized exchanges in being neither an `Automated Market Maker (AMM)` nor an order book exchange. Instead, It adopts an exchange methodology called `Request For Quotation (RFQ)` so that trading on `Tokenlon` looks like trading with an automated `Over-The-Counter (OTC)` desk. As a result, `Tokenlon` achieves extremely low failure of trading transaction execution with competitive, zero-slippage prices. The `multicall` feature allows to batch together multiple trading orders in a single call. The basic information of the audited protocol is as follows:

Table 1.1: Basic Information of Tokenlon (Multicall)

Item	Description
Name	Tokenlon
Website	https://tokenlon.im/
Type	EVM Smart Contract
Platform	Solidity
Audit Method	Whitebox
Latest Audit Report	July 6, 2022

In the following, we show the Git repository of reviewed files and the commit hash value used in this audit. This audit mainly covers the `multicall` support in `Tokenlon`.

- https://github.com/consenlabs/tokenlon-contracts.git (eeb8f5b)

And here are the commit IDs after all fixes for the issues found in the audit have been checked in:

- https://github.com/consenlabs/tokenlon-contracts.git (a401718)

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 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), 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 1.3: 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

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 design and implementation of the `multicall` support in `Tokenlon`. 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	0	
Low	1	■
Informational	1	■
Total	2	

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 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 1 low-severity vulnerability and 1 informational recommendation.

Table 2.1: Key Audit Findings

ID	Severity	Title	Category	Status
PVE-001	Informational	Consistent Ether Support with Multicall	Business Logic	Resolved
PVE-002	Low	Improved Logic in LimitOrder::cancelLimitOrder()	Coding Practices	Resolved

Beside the identified issues, we emphasize that for any user-facing applications and services, 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 should kick in at the very moment when the contracts are being deployed on mainnet. Please refer to Section 3 for details.

3 Detailed Results

3.1 Consistent Ether Support with Multicall

- ID: PVE-001
- Severity: Informational
- Likelihood: N/A
- Impact: N/A
- Target: UserProxy
- Category: Business Logic [4]
- CWE subcategory: CWE-841 [2]

Description

The TokenLon protocol has the UserProxy contract as the main entrance for interaction with various features in supporting low-cost, reliable market making to fulfill user trading requests. The audited feature of multicall supports to batch together multiple trading orders in a single call. While examining the current implementation, we notice the dispatcher routine from the UserProxy contract supports the use of Ether for PMM/AMM/RFQ-related orders, but not the LimitOrder.

To elaborate, we show below its toRFQ()/toLimitOrder() routines, which are invoked to call the actual RFQ and Limit Order functionalities. Note the Limit Order functionality is supported by three public functions: fillLimitOrderByTrader(), fillLimitOrderByProtocol(), and cancelLimitOrder(). While none of these three functions has the payable support, the use of batched calls with RFQ orders may require the payable modifier in the top-level toLimitOrder() function.

```
    function toRFQ(bytes calldata _payload) external payable {
        require(isRFQEnabled(), "UserProxy: RFQ is disabled");
        require(msg.sender == tx.origin, "UserProxy: only EOA");

        (bool callSucceed, ) = rfqAddr().call{ value: msg.value }(_payload);
        if (callSucceed == false) {
            // Get the error message returned
            assembly {
                let ptr := mload(0x40)
                let size := returndatasize()
                returndatacopy(ptr, 0, size)
                revert(ptr, size)
```

```
            }
        }
    }

    function toLimitOrder(bytes calldata _payload) external {
        require(isLimitOrderEnabled(), "UserProxy: Limit Order is disabled");
        require(msg.sender == tx.origin, "UserProxy: only EOA");

        (bool callSucceed, ) = limitOrderAddr().call(_payload);
        if (callSucceed == false) {
            // Get the error message returned
            assembly {
                let ptr := mload(0x40)
                let size := returndatasize()
                returndatacopy(ptr, 0, size)
                revert(ptr, size)
            }
        }
    }
```

Listing 3.1: `UserProxy::toRFQ()/toLimitOrder()`

Recommendation Be consistent in the batched support of multiple types of trade orders.

Status The issue has been resolved as the team confirms the design choince in not supporting the `ether` with `multicall`.

3.2 Improved Logic in LimitOrder::cancelLimitOrder()

- ID: PVE-002
- Severity: Low
- Likelihood: Low
- Impact: Low
- Target: `LimitOrder`
- Category: Coding Practices [3]
- CWE subcategory: CWE-563 [1]

Description

As mentioned earlier, `Tokenlon` supports multiple types of trade orders, i.e., `AMM`, `PMM`, `RFQ`, and `Limit Order`. While examining the support of `Limit Order`, we notice the order cancellation logic can be improved.

In the following, we show below the implementation of the related `cancelLimitOrder()` function. This function has a rather straightforward logic in nullifying the intended maker order. However, our analysis shows that the current implementation does not validate whether the given order has been already expired or canceled before. Therefore, we suggest to validate the cancellation order thoroughly in also validating its `expiry` as well as the related cancellation status.

```
    function cancelLimitOrder(LimitOrderLibEIP712.Order calldata _order, bytes calldata _cancelOrderMakerSig) external override onlyUserProxy nonReentrant {
        {
            LimitOrderLibEIP712.Order memory cancelledOrder = _order;
            cancelledOrder.takerTokenAmount = 0;

            bytes32 cancelledOrderHash = getEIP712Hash(LimitOrderLibEIP712._getOrderStructHash(cancelledOrder));
            require(isValidSignature(_order.maker, cancelledOrderHash, bytes(""), _cancelOrderMakerSig), "LimitOrder: Cancel request is not signed by maker");
        }

        // Set cancelled state to storage
        bytes32 orderHash = getEIP712Hash(LimitOrderLibEIP712._getOrderStructHash(_order));
        LibOrderStorage.getStorage().orderHashToCancelled[orderHash] = true;

        emit OrderCancelled(orderHash, _order.maker);
    }
```

Listing 3.2: `LimitOrder::cancelLimitOrder()`

Recommendation Be thorough in validating the cancellation order.

Status The issue has been fixed by this commit hash: `a401718`.

4 Conclusion

In this audit, we have analyzed the documentation and implementation of the `multicall` support in `Tokenlon`. The audited feature allows to batch together multiple trading orders in a single call. The current code base is well structured and neatly organized. Those identified issues are promptly confirmed and fixed.

Meanwhile, we need to emphasize that 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-563: Assignment to Variable without Use. https://cwe.mitre.org/data/definitions/563.html.

[2] MITRE. CWE-841: Improper Enforcement of Behavioral Workflow. https://cwe.mitre.org/data/definitions/841.html.

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

[4] MITRE. CWE CATEGORY: Business Logic Errors. https://cwe.mitre.org/data/definitions/840.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.