SMART CONTRACT AUDIT REPORT

for

YOLO

Prepared By: Xiaomi Huang

PeckShield

July 23, 2023

Document Properties

Client	LooksRare
Title	Smart Contract Audit Report
Target	YOLO
Version	1.0
Author	Xuxian Jiang
Auditors	Stephen Bie, Patrick Lou, Xuxian Jiang
Reviewed by	Xiaomi Huang
Approved by	Xuxian Jiang
Classification	Public

Version Info

Version	Date	Author(s)	Description
1.0	July 23, 2023	Xuxian Jiang	Final Release
1.0-rc	July 16, 2023	Xuxian Jiang	Release Candidate

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 LooksRare's YOLO protocol, 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 YOLO

The YOLO protocol allows users to deposit their ETH/ERC-20/ERC-721 to receive entries for the current open round. When the round's time runs out, the YOLO protocol requests for randomness from Chainlink to draw the winner. The winner can take all the deposits of that round. There is always an open round at any time as long as a closeable round is transitioned on time. The basic information of the audited protocol is as follows:

Table 1.1: Basic Information of YOLO

Item	Description
Name	YOLO
Type	Solidity Smart Contract
Platform	Solidity
Audit Method	Whitebox
Latest Audit Report	July 23, 2023

In the following, we show the Git repository of reviewed files and the commit hash value used in this audit. Note this protocol assumes a trusted external oracle, which is not part of the audit.

- https://github.com/LooksRare/contracts-yolo.git (17c23c1)

And this is the Git repository and commit ID after all fixes for the issues found in the audit have been checked in:

- https://github.com/LooksRare/contracts-yolo.git (cb9d01e)

1.2 About PeckShield

PeckShield Inc. [9] 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 [8]:

- 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.

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

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) [7], 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 YOLO 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 logic, 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	4	■■■■
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 4 low-severity vulnerabilities.

Table 2.1: Key YOLO Audit Findings

ID	Severity	Title	Category	Status
PVE-001	Low	Inconsistent TokenType Enum Between YOLO And TransferManager	Coding Practices	Resolved
PVE-002	Low	Revisited YOLO Cancellation Logic	Business Logic	Resolved
PVE-003	Low	Possible Miscalculation of Owned Protocol Fee	Business Logic	Resolved
PVE-004	Low	Trust Issue of Admin Keys	Security Features	Mitigatd

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 Inconsistent TokenType Enum Between YOLO And TransferManager

- ID: PVE-001
- Severity: Low
- Likelihood: Low
- Impact: Low
- Target: YOLO
- Category: Coding Practices [5]
- CWE subcategory: CWE-563 [2]

Description

Each YOLO has a cutoff time and users need to participate before the cutoff time. In particular, it allows users to deposit their ETH/ERC-20/ERC-721 to receive entries for the current open round. In the process of analyzing the deposit logic, we notice the current implementation has an inconsistency that needs to be resolved.

In the following, we show the definitions of the TokenType enum in YOLO and TransferManager. While they may be observed as two different enum types, the use of the same name indicates the present of possible inconsistency. This inconsistency may unnecessarily introduce confusion and is better resolved.

```
interface IYolo {
    enum RoundStatus {
        None,
        Open,
        Drawing,
        Drawn,
        Cancelled
    }

    enum TokenType {
        ERC721,
        ETH,
        ERC20
```

```
    }
    ...
}
```

Listing 3.1: The `TokenType` Enum in `IYolo`

```
enum TokenType {
    ERC20,
    ERC721,
    ERC1155
}
```

Listing 3.2: The `TokenType` Enum in `TransferManager`

Recommendation Revise the above `TokenType` enum to ensure they are consistent in both `YOLO` and `TransferManager`

Status The issue has been fixed by this commit: `74021f5`.

3.2 Revisited YOLO Cancellation Logic

- ID: PVE-002
- Severity: Low
- Likelihood: Low
- Impact: Low
- Target: `YOLO`
- Category: Business Logic [6]
- CWE subcategory: CWE-841 [3]

Description

By design, each `YOLO` round has different states in its lifecycle. While examining the state-transition logic, we notice the use of a specific cutoff time. In particular, users need to participate before the cutoff time and if there is no enough participating users before the cutoff time, the current round may be cancelled.

In the following, we show below the use of the cutoff time in two related routines, i.e., `_deposit()` and `_cancel()`. It comes to our attention that the deposit is allowed no later than the cutoff time (line 726) while the cancellation needs to be no earlier than the cutoff time (line 924). With that, we suggest to ensure no conflict regarding the cutoff time. In other words, we suggest to ensure the cancellation can only occur after the cutoff time.

```
724     function _deposit(uint256 roundId, DepositCalldata[] calldata deposits) private {
725         Round storage round = rounds[roundId];
726         if (round.status != RoundStatus.Open  block.timestamp > round.cutoffTime) {
727             revert InvalidStatus();
728         }
```

```
        uint256 userDepositCount = depositCount[roundId][msg.sender];
        if (userDepositCount == 0) {
            unchecked {
                ++round.numberOfParticipants;
            }
        }
        ...
    }
```

Listing 3.3: `Yolo::_deposit()`

```
    function _cancel(uint256 roundId) private {
        Round storage round = rounds[roundId];

        _validateRoundStatus(round, RoundStatus.Open);

        if (block.timestamp < round.cutoffTime) {
            revert CutoffTimeNotReached();
        }

        if (round.numberOfParticipants > 1) {
            revert RoundCannotBeClosed();
        }
        ...
    }
```

Listing 3.4: `Yolo::_cancel()`

Recommendation Ensure the use of the cutoff time has no conflict in terms of the deposit and cancellation.

Status The issue has been fixed by this commit: `96dd7b2`.

3.3 Possible Miscalculation of Owned Protocol Fee

- ID: PVE-003
- Severity: Low
- Likelihood: Low
- Impact: Low
- Target: `YOLO`
- Category: Business Logic [6]
- CWE subcategory: CWE-841 [3]

Description

The `YOLO` protocol supports a number of token types to deposit, including `ERC20`, `ERC721`, and `ETH`. And the protocol will charge certain fee for each successful draw of an open round. The owned protocol fee is calculated in a helper routine, which has an implicit assumption. And there is a need for improved clarification regarding the implicit assumption.

To elaborate, we show below this helper routine `getClaimPrizesPaymentRequired()`, which has a rather straightforward logic in computing the required payment to claim the prizes. However, our analysis shows this routine does not validate whether the given arguments have any duplicate rounds or prize indexes. As a result, the calculated payment amount may be miscalculated when there is a duplicate round (or prize index). Fortunately, this routine has a very specific purpose and is defined as a view-only routine. With that, we can consider it has an implicit assumption that the given arguments do not have any duplicate rounds or prize indexs. With that, we strongly suggest to make the implicit assumption explicit with additional `NatSpec` comment as part of the function summary.

```
    function getClaimPrizesPaymentRequired(
        ClaimPrizesCalldata[] calldata claimPrizesCalldata
    ) external view returns (uint256 protocolFeeOwed) {
        uint256 ethAmount;

        for (uint256 i; i < claimPrizesCalldata.length; ) {
            ClaimPrizesCalldata calldata perRoundClaimPrizesCalldata =
                claimPrizesCalldata[i];
            Round storage round = rounds[perRoundClaimPrizesCalldata.roundId];

            _validateRoundStatus(round, RoundStatus.Drawn);

            uint256[] calldata prizeIndices = perRoundClaimPrizesCalldata.prizeIndices;
            uint256 numberOfPrizes = prizeIndices.length;
            uint256 prizesCount = round.deposits.length;

            for (uint256 j; j < numberOfPrizes; ) {
                uint256 index = prizeIndices[j];
                if (index >= prizesCount) {
                    revert InvalidIndex();
                }

                Deposit storage prize = round.deposits[index];
                if (prize.tokenType == TokenType.ETH) {
                    ethAmount += prize.tokenAmount;
                }

                unchecked {
                    ++j;
                }
            }

            protocolFeeOwed += round.protocolFeeOwed;

            unchecked {
                ++i;
            }
        }
```

```
        if (protocolFeeOwed < ethAmount) {
            protocolFeeOwed = 0;
        } else {
            unchecked {
                protocolFeeOwed -= ethAmount;
            }
        }
    }
```

Listing 3.5: `YOLO::getClaimPrizesPaymentRequired()`

Recommendation Add additional comment to the above routine to document the implicit assumption without any duplicate rounds/prize indexes.

Status The issue has been fixed by this commit: `db4d00d`.

3.4 Trust Issue of Admin Keys

- ID: PVE-004
- Severity: Low
- Likelihood: Low
- Impact: Low
- Target: `YOLO`
- Category: Security Features [4]
- CWE subcategory: CWE-287 [1]

Description

In the `YOLO` protocol, there is a privileged `owner` account that plays a critical role in governing and regulating the protocol-wide operations (e.g., configure various system parameters, collect protocol fees, and pause/resume protocols). In the following, we show the representative functions potentially affected by the privilege of the account.

```
    function updateProtocolFeeRecipient(address _protocolFeeRecipient) external {
        _validateIsOwner();
        _updateProtocolFeeRecipient(_protocolFeeRecipient);
    }

    /**
     * @inheritdoc IYolo
     */
    function updateProtocolFeeBp(uint16 _protocolFeeBp) external {
        _validateIsOwner();
        _updateProtocolFeeBp(_protocolFeeBp);
    }

    /**
     * @inheritdoc IYolo
```

```
    */
    function updateMaximumNumberOfDepositsPerRound(uint40
        _maximumNumberOfDepositsPerRound) external {
        _validateIsOwner();
        _updateMaximumNumberOfDepositsPerRound(_maximumNumberOfDepositsPerRound);
    }

    /**
     * @inheritdoc IYolo
     */
    function updateMaximumNumberOfParticipantsPerRound(uint40
        _maximumNumberOfParticipantsPerRound) external {
        _validateIsOwner();
        _updateMaximumNumberOfParticipantsPerRound(_maximumNumberOfParticipantsPerRound)
            ;
    }

    /**
     * @inheritdoc IYolo
     */
    function updateReservoirOracle(address _reservoirOracle) external {
        _validateIsOwner();
        _updateReservoirOracle(_reservoirOracle);
    }

    /**
     * @inheritdoc IYolo
     */
    function updateERC20Oracle(address _erc20Oracle) external {
        _validateIsOwner();
        _updateERC20Oracle(_erc20Oracle);
    }
```

Listing 3.6: Example Privileged Operations in YOLO

We emphasize that the privilege assignment may be necessary and consistent with the protocol design. However, it would be better if the privileged account is governed by a DAO-like structure. Note that a compromised account would allow the attacker to modify a number of sensitive system parameters, which directly undermines the assumption of the protocol design.

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 The issue has been confirmed by the team. The team intends to manage the admin keys with a multi-sig account.

4 Conclusion

In this audit, we have analyzed the design and implementation of the `YOLO` protocol, which allows users to deposit their `ETH/ERC-20/ERC-721` to receive entries for the current open round. When the round's time runs out, the `YOLO` protocol requests for randomness from `Chainlink` to draw the winner. The winner can take all the deposits of that round. There is always an open round at any time as long as a closeable round is transitioned on time. The current code base is well organized and 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-287: Improper Authentication. https://cwe.mitre.org/data/definitions/287.html.

[2] MITRE. CWE-563: Assignment to Variable without Use. https://cwe.mitre.org/data/definitions/563.html.

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

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

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

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

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

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

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