SMART CONTRACT AUDIT REPORT

for

StoryHunt

Prepared By: Xiaomi Huang

PeckShield

February 3, 2025

Document Properties

Client	StoryHunt
Title	Smart Contract Audit Report
Target	StoryHunt
Version	1.0
Author	Xuxian Jiang
Auditors	Daisy Cao, Xuxian Jiang
Reviewed by	Xiaomi Huang
Approved by	Xuxian Jiang
Classification	Public

Version Info

Version	Date	Author(s)	Description
1.0	February 3, 2025	Xuxian Jiang	Final Release
1.0-rc	January 14, 2025	Xuxian Jiang	Release Candidate #1

Contact

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

Name	Xiaomi Huang
Email	contact@peckshield.com

Contents

1 | Introduction

Given the opportunity to review the design document and related source code of the StoryHunt 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 StoryHunt

StoryHunt is the native DEX on the Story protocol, powering IPFi by enabling the trading of IP assets represented as ERC20 tokens. It combines the Uniswap V3 model with farming features inspired by PancakeSwap, with a new extension allowing multiple rewards tokens for liquidity providers. Users can stake their positions to earn yields from various IP asset pools, enabling new mechanics to earn yields generated from IP licenses and monetization in Story protocol. he basic information of audited contracts is as follows:

Table 1.1: Basic Information of StoryHunt

Item	Description
Name	StoryHunt
Type	Smart Contract
Language	Solidity
Audit Method	Whitebox
Latest Audit Report	February 3, 2025

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

- https://github.com/0xstoryhunt/v3-core.git (ee518ae)
- https://github.com/0xstoryhunt/v3-periphery.git (d34506c)

- https://github.com/0xstoryhunt/v3-lm-pool.git (81b1d88)

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

- https://github.com/0xstoryhunt/v3-core.git (5bcc238)
- https://github.com/0xstoryhunt/v3-periphery.git (37f74df)
- https://github.com/0xstoryhunt/v3-lm-pool.git (8d84b0a)

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 accordingly classified into four categories, 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. Moreover, in case there is an issue that may affect an active protocol that has been deployed, the public version of this report may omit such issue, but will be amended with full details right after the affected protocol is upgraded with respective fixes.

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

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.

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.

2 Findings

2.1 Summary

Here is a summary of our findings after analyzing the implementation of the `StoryHunt` protocol. 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	0	
Informational	1	■
Total	3	

We have so far identified a list of potential issues: some of them involve subtle corner cases that might not be previously thought of. 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, this smart contract is 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 1 informational issue.

Table 2.1: Key StoryHunt Audit Findings

ID	Severity	Title	Category	Status
PVE-001	Medium	Improper refund() Logic in AlphaHunterV3	Business Logic	Resolved
PVE-002	Informational	Revisited Flashloan Protocol Fee Distribution Logic	Business Logic	Resolved
PVE-003	Medium	Trust Issue of Admin Keys	Security Features	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 contract is being deployed on mainnet. Please refer to Section 3 for details.

3 Detailed Results

3.1 Improper refund() Logic in AlphaHunterV3

- ID: PVE-001
- Severity: Medium
- Likelihood: Medium
- Impact: Medium
- Target: AlphaHunterV3
- Category: Business Logic [4]
- CWE subcategory: CWE-841 [2]

Description

To incentivize protocol users, the StoryHunt protocol has a core AlphaHunterV3 contract that is inspired by the popular MasterChef to manage and reward multiple LP pools. While reviewing an internal helper routine to refund LP users, we notice current implementation should be revised.

To elaborate, we show below the related refund() routine. It has a rather straightforward logic in refunding the remaining tokens back to the user. When the token being refunded is WETH, there is a refundETH() call to nonfungiblePositionManager. However, the nonfungiblePositionManager contract does not have the refundETH() function, which should be revised as refundIP(). Note it also affects other related files, including INonfungiblePositionManager.sol and INonfungiblePositionManager.ts

```
    function refund(address _token, uint256 _amount) internal {
        if (_token == WETH && msg.value > 0) {
            nonfungiblePositionManager.refundETH();
            safeTransferETH(msg.sender, address(this).balance);
        } else {
            IERC20(_token).safeTransfer(msg.sender, _amount);
        }
    }
```

Listing 3.1: AlphaHunterV3::refund()

Recommendation Revisit the above routine to properly refund user assets.

Status This issue has been resolved in the following commit: b4c6414.

3.2 Revisited Flashloan Protocol Fee Distribution Logic

- ID: PVE-002
- Severity: Informational
- Likelihood: N/A
- Impact: N/A
- Target: StoryHuntV3Pool
- Category: Business Logic [4]
- CWE subcategory: CWE-841 [2]

Description

As mentioned earlier, the StoryHunt protocol is in essence a DEX engine that facilitates the swaps between tokens. It also supports the flashloan feature that allows users to borrow assets without having to provide collateral or a credit score. This type of loan has to be paid back within the same blockchain transaction block. While reviewing the flashloan logic, we notice the way to distribute flashloan fee may need to be revisited.

To elaborate, we show below the related flash() routine. It has a rather straightforward logic in making the liquidity available to flashloaners and collecting the flashloan fee accordingly. Note the flashloan funds are pooled together from all liquidity providers. However, the flashloan fee is only credited to in-range liquidity providers, not all liquidity providers. This design may need to be revisited.

```
    function flash(
        address recipient,
        uint256 amount0,
        uint256 amount1,
        bytes calldata data
    ) external override lock noDelegateCall {
        uint128 _liquidity = liquidity;
        require(_liquidity > 0, 'L');

        uint256 fee0 = FullMath.mulDivRoundingUp(amount0, fee, 1e6);
        uint256 fee1 = FullMath.mulDivRoundingUp(amount1, fee, 1e6);
        uint256 balance0Before = balance0();
        uint256 balance1Before = balance1();

        if (amount0 > 0) TransferHelper.safeTransfer(token0, recipient, amount0);
        if (amount1 > 0) TransferHelper.safeTransfer(token1, recipient, amount1);

        IStoryHuntV3FlashCallback(msg.sender).storyHuntV3FlashCallback(fee0, fee1, data)
            ;

        uint256 balance0After = balance0();
        uint256 balance1After = balance1();

        require(balance0Before.add(fee0) <= balance0After, 'F0');
        require(balance1Before.add(fee1) <= balance1After, 'F1');
```

```

        // sub is safe because we know balanceAfter is gt balanceBefore by at least fee
        uint256 paid0 = balance0After - balance0Before;
        uint256 paid1 = balance1After - balance1Before;

        if (paid0 > 0) {
            uint8 feeProtocol0 = slot0.feeProtocol % 16;
            uint256 fees0 = feeProtocol0 == 0 ? 0 : paid0 / feeProtocol0;
            if (uint128(fees0) > 0) protocolFees.token0 += uint128(fees0);
            feeGrowthGlobal0X128 += FullMath.mulDiv(paid0 - fees0, FixedPoint128.Q128,
                _liquidity);
        }
        if (paid1 > 0) {
            uint8 feeProtocol1 = slot0.feeProtocol >> 4;
            uint256 fees1 = feeProtocol1 == 0 ? 0 : paid1 / feeProtocol1;
            if (uint128(fees1) > 0) protocolFees.token1 += uint128(fees1);
            feeGrowthGlobal1X128 += FullMath.mulDiv(paid1 - fees1, FixedPoint128.Q128,
                _liquidity);
        }

        emit Flash(msg.sender, recipient, amount0, amount1, paid0, paid1);
    }
```

Listing 3.2: `StoryHuntV3Pool::flash()`

Recommendation Revisit the above routine to properly credit the flashloan fee to all liquidity providers.

Status This issue has been confirmed as the team clarifies the need of maintaining the code consistency with the original `UniswapV3` codebase.

3.3 Trust Issue of Admin Keys

- ID: PVE-003
- Severity: Medium
- Likelihood: Medium
- Impact: Medium
- Target: `Multiple Contracts`
- Category: Security Features [3]
- CWE subcategory: CWE-287 [1]

Description

In the `StoryHunt` protocol, there is a privileged account `owner` that plays a critical role in governing and regulating the system-wide operations (e.g., configure the fee-related parameters, collect protocol fee, and manage reward pools). The account also has the privilege to control or govern the flow of assets managed by this protocol. Our analysis shows that the privileged account needs to be scrutinized.

In the following, we examine the privileged account and the related privileged accesses in current contracts.

```
    function setEmergency(bool _emergency) external onlyOwner {
        emergency = _emergency;
        emit SetEmergency(emergency);
    }

    function setReceiver(address _receiver) external onlyOwner {
        if (_receiver == address(0)) revert ZeroAddress();
        for (uint i = 0; i < rewardTokens.length; i++) {
            if (IERC20(rewardTokens[i]).allowance(_receiver, address(this)) != type(
                uint256).max) revert();
        }
        receiver = _receiver;
        emit NewReceiver(_receiver);
    }

    function setLMPoolDeployer(ILMPoolDeployer _LMPoolDeployer) external onlyOwner {
        if (address(_LMPoolDeployer) == address(0)) revert ZeroAddress();
        LMPoolDeployer = _LMPoolDeployer;
        emit NewLMPoolDeployerAddress(address(_LMPoolDeployer));
    }

    function setRewardTokens(address[] memory _tokens) external onlyOwner {
        if (_tokens.length == 0) revert NotEmpty();
        rewardTokens = _tokens;
    }
```

Listing 3.3: Example Privileged Functions in `AlphaHunterV3`

Note that if these privileged accounts are plain EOA accounts, this may be worrisome and pose counter-party risk to the exchange users. 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. In the meantime, a timelock-based mechanism can also be considered as mitigation.

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 resolved as the team is going to have a short `genesis phase` using a secure multisig until the mainnet token launches. After that, the ownership will be passed over to the `DAO`.

4 Conclusion

In this audit, we have analyzed the design and implementation of the StoryHunt protocol, which is the native DEX on the Story protocol, powering IPFi by enabling the trading of IP assets represented as ERC20 tokens. It combines the Uniswap V3 model with farming features inspired by PancakeSwap, with a new extension allowing multiple rewards tokens for liquidity providers. Users can stake their positions to earn yields from various IP asset pools, enabling new mechanics to earn yields generated from IP licenses and monetization in Story protocol. 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-287: Improper Authentication. https://cwe.mitre.org/data/definitions/287.html.

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

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