SMART CONTRACT AUDIT REPORT

for

RoofStacks Protocol

Prepared By: Patrick Lou

PeckShield
March 21, 2022

Document Properties

Client	RoofStacks
Title	Smart Contract Audit Report
Target	RoofStacks
Version	1.0
Author	Patrick Lou
Auditors	Patrick Lou, Xuxian Jiang
Reviewed by	Xiaotao Wu
Approved by	Xuxian Jiang
Classification	Public

Version Info

Version	Date	Author(s)	Description
1.0	March 21, 2022	Patrick Lou	Final Release
1.0-rc1	March 6, 2022	Patrick Lou	Release Candidate #1

Contact

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

Name	Patrick Lou
Phone	+86 156 0639 2692
Email	contact@peckshield.com

Contents

1 Introduction

Given the opportunity to review the design document and related smart contract source code of the RoofStacks 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 RoofStacks Protocol

RoofStacks protocol aims users to collect Move To Earn (MTE) points in real world with their phones by using the AR technology. After collecting the activity, users will be able to swap MTE points to Matic in the coin distribution web page. The basic information of the audited protocol is as follows:

Table 1.1: Basic Information of RoofStacks

Item	Description
Name	RoofStacks
Type	Ethereum Smart Contract
Platform	Solidity
Audit Method	Whitebox
Latest Audit Report	March 21, 2022

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

- https://github.com/roofstacks/move-to-earn-event-smart-contracts (229d56f)

And here is the commit ID after all fixes for the issues found in the audit have been checked in.

- https://github.com/roofstacks/move-to-earn-event-smart-contracts (85011b0)

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 the 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 checklist of 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

Table 1.3: The Full Audit Checklist

Category	Checklist Items
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

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 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 Logic	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 implementation of the `RoofStacks` 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 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	1	■
Low	0	
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 medium-severity vulnerability and 1 informational recommendation.

Table 2.1: Key RoofStacks Audit Findings

ID	Severity	Title	Category	Status
PVE-001	Medium	Trust Issue of Admin Keys	Security Features	Confirmed
PVE-002	Informational	Meaningful Events For Important States Change	Coding Practices	Fixed

Besides 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 Trust Issue of Admin Keys

- ID: PVE-001
- Severity: Medium
- Likelihood: Low
- Impact: High
- Target: GoArtCampaign
- Category: Security Features [3]
- CWE subcategory: CWE-287 [1]

Description

In the RoofStacks protocol, there is a privileged admin account that plays a critical role in governing and regulating the system-wide operations (e.g., system parameters setting and token withdraw). It 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.

To elaborate, we show below example privileged routines in the GoArtCampaign contract. These routines allow the admin account to add/remove admins, set contract state, swap collectible items to MATIC, etc.

```
// register a new admin with the given wallet address
function addAdmin(address _adminAddress) external onlyAdmin {
  // Can't add 0x address as an admin
  require(_adminAddress != address(0x0), '[RBAC] : Admin must be != than 0x0 address');
  // Can't add existing admin
  require(!isAdmin[_adminAddress], '[RBAC] : Admin already exists.');
  // Add admin to array of admins
  admins.push(_adminAddress);
  // Set mapping
  isAdmin[_adminAddress] = true;
}

// remove an existing admin address
function removeAdmin(address _adminAddress) external onlyAdmin {
```

```
        ...
    }

    // Set contract State as Active
    function setStateActive() external onlyAdmin {
      state = State.Active;
    }

    // Set contract State as Closed
    function setStateClosed() external onlyAdmin {
      state = State.Closed;
    }

    // Change the contract's max reward amount
    function changeMaxReward(uint256 _maxReward) external onlyAdmin {
      maxRewardTotal = _maxReward;
    }

    // change award ration
    function changeRatio(uint256 _ratio) external onlyAdmin {
      ratio = _ratio;
    }

    // register a user's wallet address if the contract is in Active state.
    function registerWallet(address payable walletAddress, string memory userId)
      external
      onlyAdmin
    {
        ...
    }

    // A user's collectible items can be swapped to MATIC through this function.
    function swapCollectibleItemsToMatic(uint256 _collectibleItemAmount, uint256
        _participantIndex)
      external
      onlyAdmin
    {
        ...
    }

    function withdrawMaticTokens(uint256 _participantIndex) external payable onlyAdmin {
        ...
    }

    // set service fee
    function setServiceFee(uint256 _fee) external onlyAdmin {
      fee = _fee;
    }

    // set minimumAmount
    function setMinimumAmount(uint256 _minimumAmount) external onlyAdmin {
      minimumAmountToWithdraw = _minimumAmount;
```

```
}
```

Listing 3.1: PresaleContract::Multiple Functions

It is worrisome if the privileged admin 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. 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 confirmed.

3.2 Meaningful Events For Important States Change

- ID: PVE-002
- Severity: Informational
- Likelihood: N/A
- Impact: N/A
- Target: GoArtCampaign
- Category: Coding Practices [4]
- CWE subcategory: CWE-563 [2]

Description

In Ethereum, the event is an indispensable part of a contract and is mainly used to record a variety of runtime dynamics. In particular, when an event is emitted, it stores the arguments passed in transaction logs and these logs are made accessible to external analytics and reporting tools. Events can be emitted in a number of scenarios. One particular case is when system-wide parameters or settings are being changed. Another case is when tokens are being minted, transferred, or burned.

In the following, we use the GoArtCampaign contract as an example. While examining the events that reflect the GoArtCampaign dynamics, we notice there is a lack of emitting related events that reflect important state changes. Specifically, when a new admin is added or removed, when the contract state is set or the the system parameters are changed, there are no respective events being emitted to reflect the changes of the related parameters.

```
// register a new admin with the given wallet address
function addAdmin(address _adminAddress) external onlyAdmin {
  // Can't add 0x address as an admin
  require(_adminAddress != address(0x0), '[RBAC] : Admin must be != than 0x0 address')
      ;
```

```
    // Can't add existing admin
    require(!isAdmin[_adminAddress], '[RBAC] : Admin already exists.');
    // Add admin to array of admins
    admins.push(_adminAddress);
    // Set mapping
    isAdmin[_adminAddress] = true;
  }

  // remove an existing admin address
  function removeAdmin(address _adminAddress) external onlyAdmin {
    // Admin has to exist
    require(isAdmin[_adminAddress]);
    require(admins.length > 1, 'Can not remove all admins since contract becomes
        unusable.');
    uint256 i = 0;

    while (admins[i] != _adminAddress) {
      if (i == admins.length) {
        revert('Passed admin address does not exist');
      }
      i++;
    }

    // Copy the last admin position to the current index
    admins[i] = admins[admins.length - 1];

    isAdmin[_adminAddress] = false;

    // Remove the last admin, since it's double present
    admins.pop();
  }

  // Set contract State as Active
  function setStateActive() external onlyAdmin {
    state = State.Active;
  }

  // Set contract State as Closed
  function setStateClosed() external onlyAdmin {
    state = State.Closed;
  }

  // Change the contract's max reward amount
  function changeMaxReward(uint256 _maxReward) external onlyAdmin {
    maxRewardTotal = _maxReward;
  }

  // change award ration
  function changeRatio(uint256 _ratio) external onlyAdmin {
    ratio = _ratio;
  }

```

```
// set service fee
function setServiceFee(uint256 _fee) external onlyAdmin {
  fee = _fee;
}

// set minimumAmount
function setMinimumAmount(uint256 _minimumAmount) external onlyAdmin {
  minimumAmountToWithdraw = _minimumAmount;
}
```

Listing 3.2: `PresaleContract`

Recommendation Properly emit the event when the related parameters are being updated.

Status This issue has been fixed in the following commit: 85011b0.

4 Conclusion

In this audit, we have analyzed the design and implementation of the `RoofStacks` protocol, which allow users to swap `MTE` points to `Matic` in the coin distribution web page. The current code base is well structured and neatly organized. Those identified issues are promptly confirmed and addressed.

Moreover, 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-563: Assignment to Variable without Use. https://cwe.mitre.org/data/definitions/563.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.