SMART CONTRACT AUDIT REPORT

for

Randomizer

Prepared By: Xiaomi Huang

PeckShield

August 2, 2022

Document Properties

Client	Randomizer
Title	Smart Contract Audit Report
Target	Randomizer
Version	1.0
Author	Shulin Bie
Auditors	Shulin Bie, Xuxian Jiang
Reviewed by	Xiaomi Huang
Approved by	Xuxian Jiang
Classification	Public

Version Info

Version	Date	Author(s)	Description
1.0	August 2, 2022	Shulin Bie	Final Release
1.0-rc	July 29, 2022	Shulin Bie	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 Randomizer 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 Randomizer

Randomizer is a Verifiable Random Function (VRF) protocol that enables smart contracts to access random values without compromising security or usability. This is useful for various scenarios, e.g., NFT generation, item drop rates, gaming, etc. The basic information of the audited protocol is as follows:

Table 1.1: Basic Information of Randomizer

Item	Description
Target	Randomizer
Type	EVM Smart Contract
Language	Solidity
Audit Method	Whitebox
Latest Audit Report	August 2, 2022

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

- https://github.com/RandomizerAi/randomizer-contract.git (22be2dc)

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

- https://github.com/RandomizerAi/randomizer-contract.git (bc9d693)

1.2 About PeckShield

PeckShield Inc. [10] 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 [9]:

- 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) [8], 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 `Randomizer` 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	1	🟦
Medium	1	🟦
Low	0	
Informational	2	🟦 🟦
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 1 high-severity vulnerability, 1 medium-severity vulnerability, and 2 informational recommendations.

Table 2.1: Key Randomizer Audit Findings

ID	Severity	Title	Category	Status
PVE-001	High	Revisited Logic Of Beacon::registerBeacon()	Business Logic	Fixed
PVE-002	Informational	Redundant State/Code Removal	Coding Practices	Confirmed
PVE-003	Informational	Suggested Event Generation For Key Operations	Coding Practices	Confirmed
PVE-004	Medium	Trust Issue Of Admin Keys	Security Features	Confirmed

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 Revisited Logic Of Beacon::registerBeacon()

- ID: PVE-001
- Severity: High
- Likelihood: High
- Impact: Medium
- Target: Beacon
- Category: Business Logic [7]
- CWE subcategory: CWE-841 [4]

Description

The Randomizer protocol is a provably fair and verifiable random number generator. In the protocol, the privileged Beacon accounts are in charge of signing the user requested data and submit the signature (which will be used to generate the final random number). The Beacon contract is the main entry for interaction with them. In particular, the registerBeacon() routine is used by the privileged owner to add the new privileged Beacon account. While examining its logic, we observe there is an improper implementation that needs to be improved.

To elaborate, we show below the related code snippet of the Beacon contract. By design, only when the amount of the address's collateral is larger than minStakeEth, it is allowed as Beacon. However, we notice there is a lack of validating the collateral amount inside the registerBeacon() routine. Meanwhile, we observe the new Beacon account is not correctly stored in the beacons storage variable, which directly undermines the assumption of the design. Given this, we suggest to revisit its current implementation.

```
    function registerBeacon(address _beacon) external onlyOwner {
        if (beaconIndex[_beacon] != 0) revert BeaconExists();

        uint256 index = beacons.length - 1;
        // beacons[index] = beacons[beacons.length - 1];
        if (!sBeacon[_beacon].exists) sBeacon[_beacon] = SBeacon(true, 0, 0, 0);
        beaconIndex[_beacon] = index;
        // beacons[index] = _beacon;
        // beaconToStrikeCount[_beacon] = 0;
        emit RegisterBeacon(_beacon);
    }
```

Listing 3.1: `Beacon::registerBeacon()`

Recommendation Correct the implementation of the `registerBeacon()` routine as above-mentioned.

Status The issue has been addressed in this commit: `ad2a801`.

3.2 Redundant State/Code Removal

- ID: PVE-002
- Severity: Informational
- Likelihood: Low
- Impact: N/A
- Target: `Store`
- Category: Coding Practices [6]
- CWE subcategory: CWE-1041 [1]

Description

In the `Store` contract, we observe the inclusion of certain unused code or the presence of unnecessary redundancies that can be safely removed. For example, we notice the `strikeBurn` private state variable is not used anywhere.

To elaborate, we show below the related code snippet of the `Store` contract. The private `strikeBurn` storage variable is declared at line 71, but is not used anywhere in the contract. Given this, we suggest to remove it safely to keep the `Store` implementation clean.

```
69    contract Store {
70        address[] beacons;
71        uint256 strikeBurn;
72        uint256 minToken;
73        ...
74        mapping(address => uint256) tokenCollateral;
75    }
```

Listing 3.2: `Store`

Note that the private `minToken` and `tokenCollateral` storage variables can be similarly improved.

Recommendation Consider the removal of the redundant code with a simplified, consistent implementation.

Status The issue has been confirmed by the team.

3.3 Suggested Event Generation For Key Operations

- ID: PVE-003
- Severity: Informational
- Likelihood: N/A
- Impact: N/A
- Target: Admin
- Category: Coding Practices [6]
- CWE subcategory: CWE-563 [3]

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.

While examining the events that reflect the protocol dynamics, we notice there are several key operations that lack meaningful events to reflect their changes. In the following, we show several representative routines.

```
    function setBeaconFee(uint256 _amount) external onlyOwner {
        beaconFee = _amount;
    }

    function setMinStakeEth(uint256 _amount) external onlyOwner {
        minStakeEth = _amount;
    }

    function setExpirationBlocks(uint256 _expirationBlocks) external onlyOwner {
        expirationBlocks = _expirationBlocks;
    }

    function setExpirationSeconds(uint256 _expirationSeconds)
        external
        onlyOwner
    {
        expirationSeconds = _expirationSeconds;
    }
```

Listing 3.3: Admin

With that, we suggest to emit meaningful events for these key operations. Also, the key event information is better indexed. Note each emitted event is represented as a topic that usually consists of the signature (from a keccak256 hash) of the event name and the types (uint256, string, etc.) of its parameters. Each indexed type will be treated like an additional topic. If an argument is not indexed, it will be attached as data (instead of a separate topic). Considering that the key information is typically queried, it is better treated as a topic, hence the need of being `indexed`.

Recommendation Properly emit the above-mentioned events with accurate information to timely reflect state changes. This is very helpful for external analytics and reporting tools.

Status The issue has been confirmed by the team.

3.4 Trust Issue Of Admin Keys

- ID: PVE-004
- Severity: Medium
- Likelihood: Medium
- Impact: Medium
- Target: `Multiple Contracts`
- Category: Security Features [5]
- CWE subcategory: CWE-287 [2]

Description

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

```
    function setBeaconFee(uint256 _amount) external onlyOwner {
        beaconFee = _amount;
    }
```

Listing 3.4: `Admin::setBeaconFee()`

```
    function registerBeacon(address _beacon) external onlyOwner {
        if (beaconIndex[_beacon] != 0) revert BeaconExists();

        uint256 index = beacons.length - 1;
        // beacons[index] = beacons[beacons.length - 1];
        if (!sBeacon[_beacon].exists) sBeacon[_beacon] = SBeacon(true, 0, 0, 0);
        beaconIndex[_beacon] = index;
        // beacons[index] = _beacon;
        // beaconToStrikeCount[_beacon] = 0;
        emit RegisterBeacon(_beacon);
    }

    ...

    function unregisterBeacon(address _beacon) public {
        if (msg.sender != _beacon && msg.sender != owner())
            revert NotOwnerOrBeacon();

        if (beaconIndex[_beacon] == 0) revert NotABeacon();
        if (sBeacon[_beacon].pending != 0)
            revert BeaconHasPending(sBeacon[_beacon].pending);

        uint256 collateral = ethCollateral[_beacon];

        _removeBeacon(_beacon);
        emit UnregisterBeacon(_beacon, sBeacon[_beacon].strikes);

        if (collateral > 0) {
            // Remove collateral
            ethCollateral[_beacon] = 0;
            // tokenCollateral[_beacon] = 0;

            // Refund ETH
            _transferEth(_beacon, collateral);
        }
    }
```

Listing 3.5: `Beacon::registerBeacon()&&unregisterBeacon()`

We emphasize that the privilege assignment is indeed necessary and consistent with the protocol design. However, it is worrisome if the privileged account is a plain EOA account. A multi-sig account could greatly alleviate this concern, though it is still far from perfect. Note that a compromised privileged account would allow the attacker to modify a number of sensitive system parameters, which directly undermines the assumption of the protocol design.

Recommendation Suggest a multi-sig account plays the privileged `owner` account to mitigate this issue. Additionally, all changes to privileged operations may need to be mediated with necessary timelocks.

Status The issue has been confirmed by the team. The team intends to transfer the privileged account to the intended `DAO`-like governance contract.

4 Conclusion

In this audit, we have analyzed the `Randomizer` design and implementation. `Randomizer` is a `Verifiable Random Function` (`VRF`) protocol that enables smart contracts to access random values without compromising security or usability. This is useful for various scenarios, e.g., `NFT generation`, `item drop rates`, `gaming`, etc. The current code base is well structured and neatly organized. Those identified issues are promptly confirmed and addressed.

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-1041: Use of Redundant Code. https://cwe.mitre.org/data/definitions/1041.html.

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

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

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

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

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

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

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

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

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