SMART CONTRACT AUDIT REPORT

for

RhinoFi Protocol

Prepared By: Xiaomi Huang

PeckShield

August 26, 2023

Document Properties

Client	RhinoFi
Title	Smart Contract Audit Report
Target	RhinoFi
Version	1.0
Author	Xuxian Jiang
Auditors	Patrick Liu, Xuxian Jiang
Reviewed by	Xiaomi Huang
Approved by	Xuxian Jiang
Classification	Public

Version Info

Version	Date	Author(s)	Description
1.0	August 26, 2023	Xuxian Jiang	Final Release
1.0-rc	August 23, 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 source code of the RhinoFi 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 RhinoFi

RhinoFi is a fast, liquid, and private non-custodial trading portal built on Ethereum, leveraging StarkWare's Layer-2 scaling technology (ZK-Rollup/Validium). This audit covers an extended wallet that can hold user funds and swap them on user's behalf when they sign meta transactions to authorize a swap. The recently added SwapV3 function enables swapping via any aggregator or third party contract, whereas the original SwapV1 was limited to only swapping via Paraswap. The basic information of the audited protocol is as follows:

Table 1.1: Basic Information of RhinoFi

Item	Description
Name	RhinoFi
Type	EVM Smart Contract
Platform	Solidity
Audit Method	Whitebox
Latest Audit Report	August 26, 2023

In the following, we show the Git repository of reviewed files and the commit hash value used in this audit. Note this repository has a number of files and directories and this audit focuses on the following PR: https://github.com/rhinofi/contracts_public/pull/12.

- https://github.com/rhinofi/contracts_public.git (731647c)

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

- https://github.com/rhinofi/contracts_public.git (e75396b)

1.2 About PeckShield

PeckShield Inc. [11] 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 [10]:

- 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

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

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) [9], 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 implementation of the RhinoFi 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	1	■
Low	2	■ ■
Informational	1	■
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 medium-severity vulnerability, 2 low-severity vulnerabilities, and 1 informational recommendation.

Table 2.1: Key Audit Findings of RhinoFi Protocol

ID	Severity	Title	Category	Status
PVE-001	Low	Revisited Logic in TransferableAccessControl::transferRole()	Coding Practices	Resolved
PVE-002	Low	Reentrancy Risk in UserWallet/DVFDepositContract	Time And State	Resolved
PVE-003	Medium	Trust on Admin Keys	Security Features	Mitigated
PVE-004	Informational	Incorrect emitBalanceUpdated Events For Important State Changes	Coding Practices	Resolved

Besides recommending specific countermeasures to mitigate these issues, we also emphasize that 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 need to kick in at the very moment when the contracts are being deployed in mainnet. Please refer to Section 3 for details.

3 | Detailed Results

3.1 Revisited Logic in TransferableAccessControl::transferRole()

- ID: PVE-001
- Severity: Low
- Likelihood: Low
- Impact: Low
- Target: `TransferableAccessControl`
- Category: Business Logic [7]
- CWE subcategory: CWE-841 [4]

Description

The `RhinoFi` protocol has a role-assignment contract `TransferableAccessControl` that is directly inherited from the `OpenZeppelin`'s `AccessControl` contract. We notice the role-assignment contract adds a new function `transferRole()`, which can be improved to rigorously validate the given arguments.

To elaborate, we show below the implementation of the `transferRole()` routine. As the name indicates, this routine is used to transfer the role to another account. It comes to our attention that it does not explicitly validate whether the given account is `msg.sender`. In fact, it only makes sense to tranfer the role when the recipient is different from the sender. The same validation can also apply to another routine `DVFDepositContact::transferOwner()`.

```
    function transferRole(bytes32 role, address account) public virtual {
        require(hasRole(role, _msgSender()), 'TransferableAccessControl: sender must
            have role to transfer');
        grantRole(role, account);
        revokeRole(role, _msgSender());
    }
```

Listing 3.1: `TransferableAccessControl::transferRole()`

Recommendation Revise the above-mentioned routines, i.e., `transferRole()` and `transferOwner()` to ensure the recipient is different from the sender.

Status This issue has been resolved in the following commit hash: `c436320`.

3.2 Reentrancy Risk in UserWallet/DVFDepositContract

- ID: PVE-002
- Severity: Low
- Likelihood: Low
- Impact: Low
- Target: UserWallet, DVFDepositContract
- Category: Time and State [8]
- CWE subcategory: CWE-663 [3]

Description

A common coding best practice in Solidity is the adherence of checks-effects-interactions principle. This principle is effective in mitigating a serious attack vector known as re-entrancy. Via this particular attack vector, a malicious contract can be reentering a vulnerable contract in a nested manner. Specifically, it first calls a function in the vulnerable contract, but before the first instance of the function call is finished, second call can be arranged to re-enter the vulnerable contract by invoking functions that should only be executed once. This attack was part of several most prominent hacks in Ethereum history, including the DAO [13] exploit, and the Uniswap/Lendf.Me hack [12].

We notice there are occasions where the checks-effects-interactions principle is violated. Using the DVFDepositContract as an example, the withdraw() function (see the code snippet below) is provided to externally call a token contract to transfer assets. However, the invocation of an external contract requires extra care in avoiding the above re-entrancy. For example, the interaction with the external contract (line 90) start before effecting the update on the internal state (lines 105), hence violating the principle. In this particular case, if the external contract has certain hidden logic that may be capable of launching re-entrancy via the same entry function.

```
86  function withdraw(address token, address to, uint256 amount, string calldata
        withdrawalId) external
87    _isAuthorized
88    _withUniqueWithdrawalId(withdrawalId)
89  {
90    IERC20Upgradeable(token).safeTransfer(to, amount);
91    emit BridgedWithdrawal(to, token, amount, withdrawalId);
92  }
93
94  modifier _withUniqueWithdrawalId(string calldata withdrawalId) {
95    require(
96      bytes(withdrawalId).length > 0,
97      "Withdrawal ID is required"
98    );
99    require(
100     !processedWithdrawalIds[withdrawalId],
101     "Withdrawal ID Already processed"
102   );
103   _;
```

```

  processedWithdrawalIds[withdrawalId] = true;
}
```

Listing 3.2: `DVFDepositContract::withdraw()`

While the supported tokens in the protocol do implement rather standard ERC20 interfaces and their related token contracts are not vulnerable or exploitable for `re-entrancy`, it is important to take precautions to thwart possible `re-entrancy`. The same suggestion is also applicable to another routine `UserWallet::depositTo()`.

Recommendation Apply necessary reentrancy prevention by following the `checks-effects-interactions` principle and utilizing the necessary `nonReentrant` modifier to block possible `re-entrancy`.

Status This issue has been resolved in the following commits: `feb3bfe` and `bf48aa4`.

3.3 Trust Issue of Admin Keys

- ID: PVE-003
- Severity: Medium
- Likelihood: Medium
- Impact: Medium
- Target: `Multiple Contracts`
- Category: Security Features [5]
- CWE subcategory: CWE-287 [2]

Description

In the `RhinoFi` protocol, there is a privileged `operator` account that plays a critical role in governing and regulating the system-wide operations (e.g., parameter setting and role assignment). 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 their related privileged accesses in current contracts.

```
function removeFunds(address token, address to, uint256 amount) external
  _isAuthorized
{
  IERC20Upgradeable(token).safeTransfer(to, amount);
}

/**
  * @dev withdraw native chain currency from the contract address
  * NOTE: only for authorized users for rebalancing
  */
function removeFundsNative(address payable to, uint256 amount) public
  _isAuthorized
{
```

```
    require(address(this).balance >= amount, "INSUFFICIENT_BALANCE");
    to.call{value: amount}("");
  }

  /**
    * @dev add or remove authorized users
    * NOTE: only owner
    */
  function authorize(address user, bool value) external onlyOwner {
    authorized[user] = value;
  }

  function transferOwner(address newOwner) external onlyOwner {
    authorized[newOwner] = true;
    authorized[owner()] = false;
    transferOwnership(newOwner);
  }
```

Listing 3.3: Example Privileged Operations in the DVFDepositContract Contract

Notice that the privilege assignment is necessary and consistent with the protocol design. In the meantime, the extra power to the owner may also be a counter-party risk to the protocol users. Therefore, we list this concern as an issue here from the audit perspective and highly recommend making these privileges explicit or raising necessary awareness among protocol users.

Recommendation Making the above privileges explicit among protocol users.

Status This issue has been confirmed with the team. For the time being, the team needs to have the owner (for upgrades) and operators to secure access to various contract functions. The owner keys will be multisig and eventually the governance contracts.

3.4 Incorrect emitBalanceUpdated Events For Important State Changes

- ID: PVE-004
- Severity: Informational
- Likelihood: N/A
- Impact: N/A
- Target: UserWallet
- Category: Coding Practices [6]
- CWE subcategory: CWE-1126 [1]

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 `UserWallet` contract as an example. This contract has public functions that are used to perform emergency transfer.. While examining the events that reflect the fund changes, we notice the emitted important event `emitBalanceUpdated` needs to reflect important state changes. Specifically, when the change should reflect `sender`, not the contract itself (line 283).

```
272 function settleEmergencyWithdrawal(address token) external {
273   address sender = msg.sender;
274   {
275     uint256 requestTimestamp = emergencyWithdrawalRequests[sender][token];
276     emergencyWithdrawalRequests[sender][token] = 0;
277     require(requestTimestamp > 0, "EMERGENCY_WITHDRAWAL_NOT_REQUESTED");
278     require(requestTimestamp + withdrawalDelay < block.timestamp, "
          EMERGENCY_WITHDRAWAL_STILL_IN_PROGRESS");
279   }
280   {
281     uint256 balance = userBalances[sender][token];
282     _withdraw(sender, token, balance, sender);
283     emitBalanceUpdated(address(this), token);
284   }
285   emit LogEmergencyWithdrawalSettled(sender, token);
286 }
```

Listing 3.4: `UserWallet::settleEmergencyWithdrawal()`

Recommendation Properly emit the respective event when an user updates its balance.

Status This issue has been resolved in the following commits: `5ca5d7e` and `c1faca1`.

4 | Conclusion

In this audit, we have analyzed the design and implementation of the `RhinoFi` protocol, which is a fast, liquid, and private non-custodial trading portal built on Ethereum by leveraging `StarkWare`'s Layer-2 scaling technology (`ZK-Rollup`/`Validium`). This audit covers an extended wallet that can hold user funds and swap them on user's behalf when they sign meta transactions to authorize a swap. 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-1126: Declaration of Variable with Unnecessarily Wide Scope. https://cwe.mitre.org/data/definitions/1126.html.

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

[3] MITRE. CWE-663: Use of a Non-reentrant Function in a Concurrent Context. https://cwe.mitre.org/data/definitions/663.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 CATEGORY: Concurrency. https://cwe.mitre.org/data/definitions/557.html.

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

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

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

[12] PeckShield. Uniswap/Lendf.Me Hacks: Root Cause and Loss Analysis. https://medium.com/@peckshield/uniswap-lendf-me-hacks-root-cause-and-loss-analysis-50f3263dcc09.

[13] David Siegel. Understanding The DAO Attack. https://www.coindesk.com/understanding-dao-hack-journalists.