Security Assessment

WOOFi

Dec 16th, 2021

Table of Contents

Summary

This report has been prepared for WOOFi to discover issues and vulnerabilities in the source code of the WOOFi project as well as any contract dependencies that were not part of an officially recognized library. A comprehensive examination has been performed, utilizing Static Analysis and Manual Review techniques.

The auditing process pays special attention to the following considerations:

- Testing the smart contracts against both common and uncommon attack vectors.
- Assessing the codebase to ensure compliance with current best practices and industry standards.
- Ensuring contract logic meets the specifications and intentions of the client.
- Cross referencing contract structure and implementation against similar smart contracts produced by industry leaders.
- Thorough line-by-line manual review of the entire codebase by industry experts.

Addtionally, this audit is based on a premise that all external contracts and calculation formula were implemented safely.

The scope of this audit does not include the contracts referenced in the contract:
* @openzeppelin/contracts/utils/EnumerableSet.sol

- @openzeppelin/contracts/utils/ReentrancyGuard.sol
- @openzeppelin/contracts/math/SafeMath.sol
- @openzeppelin/contracts/token/ERC20/SafeERC20.sol
- @openzeppelin/contracts/token/ERC20/IERC20.sol
- @openzeppelin/contracts/token/ERC20/ERC20.sol
- @uniswap/lib/contracts/libraries/TransferHelper.sol
- ./libraries/InitializableOwnable.sol
- ./libraries/DecimalMath.sol
- /interfaces/IWooAccessManager.sol

The security assessment resulted in findings that ranged from critical to informational. We recommend addressing these findings to ensure a high level of security standards and industry practices. We suggest recommendations that could better serve the project from the security perspective:

- Enhance general coding practices for better structures of source codes;
- Add enough unit tests to cover the possible use cases;
- Provide more comments per each function for readability, especially contracts that are verified in public;
- Provide more transparency on privileged activities once the protocol is live.

Overview

Project Summary

Project Name	WOOFi
Platform	BSC
Language	Solidity
Codebase	https://github.com/woonetwork/woofi_swap_smart_contracts
Commit	08cdcaa333ca90a6dfbf6813c817ce6c3394ecfb 36d5040ae36b062583ebf787b493770e00a05209

Audit Summary

Delivery Date	Dec 16, 2021
Audit Methodology	Static Analysis, Manual Review
Key Components	

Vulnerability Summary

Vulnerability Level	Total	Pending	Declined	Acknowledged	Partially Resolved	Resolved
Critical	0	0	0	0	0	0
Major	1	0	0	1	0	0
Medium	0	0	0	0	0	0
Minor	0	0	0	0	0	0
Informational	2	0	0	0	0	2
Discussion	0	0	0	0	0	0

Audit Scope

ID	File	SHA256 Checksum
WRM	WooRebateManager.sol	230368872a040c8e31974e15e33352f114b58904448342ba879564730317c8a8
WSV	WooStakingVault.sol	ac2dc0829dd6a6d4b49f2a9e35b717defb04bb58c427b28297d51e80ac08cff8
WVM	WooVaultManager.sol	eb2b310c6015ea249b3693f458f5d246bf22cc5e83b9e49c5ed891f156766e45

Understandings

Overview

This audit includes `WooRebateManager`, `WooStakingVault` and `WooVaultManager` contracts.

In the `WooRebateManager`, the user can deposit USDT. When the user withdraws, the contract will transfer `USDT` to the `WooPP` contract and swap `USDT` to `WOO`. It should be noted that the owner can withdraw any token in the contract urgently.

In the `WooVaultManager` contract, everyone can transfer `USDT` to the contract as the reward. The owner can add new vaults and assign their weight. When assigning the weight of the vault, if the USDT in the contract exceeds 100, the contract will transfer `USDT` to the `WooPP` contract and swap `USDT` to `WOO`. After the swap is completed, the contract will transfer `WOO` to each vault according to the weight as reward. It should be noted that the owner can withdraw any token in the contract urgently.

In the `WooStakingVault` contract, the user can deposit `WOO` to the contract and obtain `x` tokens. When the user withdraws, `x` tokens will be burned. It should be noted that when the user withdraws, if the deposit time is less than `withdrawFeePeriod` (up to 7 days) or emergency withdrawal, the contract will charge `withdrawFee` (up to 5%).

Privileged Functions

The contract contains the following privileged functions that are restricted by some modifiers. They are used to modify the contract configurations and address attributes. We grouped these functions below:

The `onlyOwner` modifier:

Contract `WooRebateManager`:

- setAccessManager(address newAccessManager)
- emergencyWithdraw(address token, address to)

Contract `WooVaultManager`:

- setAccessManager(address newAccessManager)
- emergencyWithdraw(address token, address to)

Contract `WooStakingVault`:

- setWithdrawFeePeriod(uint256 newWithdrawFeePeriod)

- setWithdrawFee(uint256 newWithdrawFee)
- setTreasury(address newTreasury)
- setWooAccessManager(address newWooAccessManager)
- pause()
- unpause()

The `whenNotPaused` modifier:

Contract `WooStakingVault`:

- deposit(uint256 amount)
- reserveWithdraw(uint256 shares)
- withdraw()
- instantWithdraw(uint256 shares)
- addReward(uint256 amount)
- getPricePerFullShare()
- balance()

The `onlyAdmin` modifier:

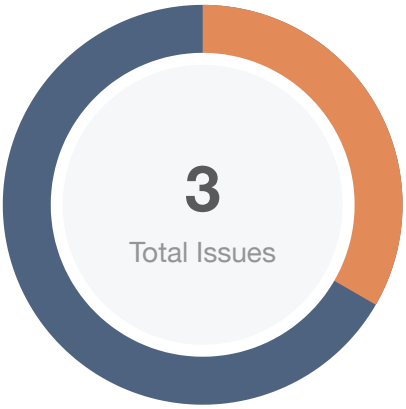
Contract `WooRebateManager`:

- setRebateRate(address brokerAddr, uint256 rate)
- setWooPP(address newWooPP)

Contract `WooVaultManager`:

- setVaultWeight(address vaultAddr, uint256 weight)
- distributeAllReward()
- setWooPP(address newWooPP)

Findings



Critical	0 (0.00%)
Major	1 (33.33%)
Medium	0 (0.00%)
Minor	0 (0.00%)
Informational	2 (66.67%)
Discussion	0 (0.00%)

ID	Title	Category	Severity	Status
GLOBAL-01	Centralization Risk	**Centralization / Privilege**	**Major**	Acknowledged
WRM-01	Check Effect Interaction Pattern Violated	Logical Issue	Informational	Resolved
WSV-01	Missing Input Validation	Logical Issue	Informational	Resolved

GLOBAL-01 | Centralization Risk

Category	Severity	Location	Status
Centralization / Privilege	Major	Global	Acknowledged

Description

The role `owner` has the authority over the following function:
Contract `WooRebateManager`:

- setAccessManager(address newAccessManager)
- emergencyWithdraw(address token, address to)

Contract `WooVaultManager`:

- setAccessManager(address newAccessManager)
- emergencyWithdraw(address token, address to)

Contract `WooStakingVault`:

- setWithdrawFeePeriod(uint256 newWithdrawFeePeriod)
- setWithdrawFee(uint256 newWithdrawFee)
- setTreasury(address newTreasury)
- setWooAccessManager(address newWooAccessManager)
- pause()
- unpause()

The role `admin` has the authority over the following function:
Contract `WooRebateManager`:

- setRebateRate(address brokerAddr, uint256 rate)
- setWooPP(address newWooPP)

Contract `WooVaultManager`:

- setVaultWeight(address vaultAddr, uint256 weight)
- distributeAllReward()
- setWooPP(address newWooPP)

without obtaining the consensus of the community.

Recommendation

We advise the client to carefully manage the owner account's private key to avoid any potential risks of being hacked. In general, we strongly recommend centralized privileges or roles in the protocol to be improved via a decentralized mechanism or smart-contract-based accounts with enhanced security practices, e.g., Multisignature wallets.

Indicatively, here is some feasible suggestions that would also mitigate the potential risk at the different level in term of short-term and long-term:

- Time-lock with reasonable latency, e.g., 48 hours, for awareness on privileged operations;
- Assignment of privileged roles to multi-signature wallets to prevent a single point of failure due to the private key;
- Introduction of a DAO/governance/voting module to increase transparency and user involvement.

Alleviation

The client response:
We’re uisng the multi-sign wallet:
https://bscscan.com/address/0xa0FA9C6fa8a5Dad6BEFF9F12EAd2e7d5e8D14E2c#code. 3/5 multi-sig gnosis wallet to ensure the security and decentralization.

WRM-01 | Check Effect Interaction Pattern Violated

Category	Severity	Location	Status
Logical Issue	Informational	WooRebateManager.sol (f89cd27): 114	Resolved

Description

The order of external call/transfer and storage manipulation must follow the check-effect-interaction pattern.

Recommendation

We advise the client to check if storage manipulation is before the external call/transfer operation.

Alleviation

The team heeded our advice and changed related codes. Code change was applied in commit 36d5040ae36b062583ebf787b493770e00a05209.

WSV-01 | Missing Input Validation

Category	Severity	Location	Status
Logical Issue	Informational	WooStakingVault.sol (f89cd27): 241, 254	Resolved

Description

The given input is missing the check for the non-zero address.

Recommendation

We advise adding the check for the passed-in values to prevent unexpected error as below:

setTreasury():

```
241 function setTreasury(address newTreasury) external onlyOwner {
242     require(newTreasury != address(0), "newTreasury can not be 0 address!");
243     treasury = newTreasury;
244 }
```

setWooAccessManager():

```
241 function setWooAccessManager(address newWooAccessManager) external onlyOwner {
242     require(newWooAccessManager != address(0), "newWooAccessManager can not be 0
address!");
243     wooAccessManager = IWooAccessManager(newWooAccessManager);
244 }
```

Alleviation

The team heeded our advice and changed related codes. Code change was applied in commit 36d5040ae36b062583ebf787b493770e00a05209.

Appendix

Finding Categories

Centralization / Privilege

Centralization / Privilege findings refer to either feature logic or implementation of components that act against the nature of decentralization, such as explicit ownership or specialized access roles in combination with a mechanism to relocate funds.

Logical Issue

Logical Issue findings detail a fault in the logic of the linked code, such as an incorrect notion on how block.timestamp works.

Checksum Calculation Method

The "Checksum" field in the "Audit Scope" section is calculated as the SHA-256 (Secure Hash Algorithm 2 with digest size of 256 bits) digest of the content of each file hosted in the listed source repository under the specified commit.

The result is hexadecimal encoded and is the same as the output of the Linux "sha256sum" command against the target file.

Disclaimer

This report is subject to the terms and conditions (including without limitation, description of services, confidentiality, disclaimer and limitation of liability) set forth in the Services Agreement, or the scope of services, and terms and conditions provided to you ("Customer" or the "Company") in connection with the Agreement. This report provided in connection with the Services set forth in the Agreement shall be used by the Company only to the extent permitted under the terms and conditions set forth in the Agreement. This report may not be transmitted, disclosed, referred to or relied upon by any person for any purposes, nor may copies be delivered to any other person other than the Company, without CertiK's prior written consent in each instance.

This report is not, nor should be considered, an "endorsement" or "disapproval" of any particular project or team. This report is not, nor should be considered, an indication of the economics or value of any "product" or "asset" created by any team or project that contracts CertiK to perform a security assessment. This report does not provide any warranty or guarantee regarding the absolute bug-free nature of the technology analyzed, nor do they provide any indication of the technologies proprietors, business, business model or legal compliance.

This report should not be used in any way to make decisions around investment or involvement with any particular project. This report in no way provides investment advice, nor should be leveraged as investment advice of any sort. This report represents an extensive assessing process intending to help our customers increase the quality of their code while reducing the high level of risk presented by cryptographic tokens and blockchain technology.

Blockchain technology and cryptographic assets present a high level of ongoing risk. CertiK's position is that each company and individual are responsible for their own due diligence and continuous security. CertiK's goal is to help reduce the attack vectors and the high level of variance associated with utilizing new and consistently changing technologies, and in no way claims any guarantee of security or functionality of the technology we agree to analyze.

The assessment services provided by CertiK is subject to dependencies and under continuing development. You agree that your access and/or use, including but not limited to any services, reports, and materials, will be at your sole risk on an as-is, where-is, and as-available basis. Cryptographic tokens are emergent technologies and carry with them high levels of technical risk and uncertainty. The assessment reports could include false positives, false negatives, and other unpredictable results. The services may access, and depend upon, multiple layers of third-parties.

ALL SERVICES, THE LABELS, THE ASSESSMENT REPORT, WORK PRODUCT, OR OTHER MATERIALS, OR ANY PRODUCTS OR RESULTS OF THE USE THEREOF ARE PROVIDED "AS IS" AND "AS

AVAILABLE" AND WITH ALL FAULTS AND DEFECTS WITHOUT WARRANTY OF ANY KIND. TO THE MAXIMUM EXTENT PERMITTED UNDER APPLICABLE LAW, CERTIK HEREBY DISCLAIMS ALL WARRANTIES, WHETHER EXPRESS, IMPLIED, STATUTORY, OR OTHERWISE WITH RESPECT TO THE SERVICES, ASSESSMENT REPORT, OR OTHER MATERIALS. WITHOUT LIMITING THE FOREGOING, CERTIK SPECIFICALLY DISCLAIMS ALL IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, TITLE AND NON-INFRINGEMENT, AND ALL WARRANTIES ARISING FROM COURSE OF DEALING, USAGE, OR TRADE PRACTICE. WITHOUT LIMITING THE FOREGOING, CERTIK MAKES NO WARRANTY OF ANY KIND THAT THE SERVICES, THE LABELS, THE ASSESSMENT REPORT, WORK PRODUCT, OR OTHER MATERIALS, OR ANY PRODUCTS OR RESULTS OF THE USE THEREOF, WILL MEET CUSTOMER'S OR ANY OTHER PERSON'S REQUIREMENTS, ACHIEVE ANY INTENDED RESULT, BE COMPATIBLE OR WORK WITH ANY SOFTWARE, SYSTEM, OR OTHER SERVICES, OR BE SECURE, ACCURATE, COMPLETE, FREE OF HARMFUL CODE, OR ERROR-FREE. WITHOUT LIMITATION TO THE FOREGOING, CERTIK PROVIDES NO WARRANTY OR UNDERTAKING, AND MAKES NO REPRESENTATION OF ANY KIND THAT THE SERVICE WILL MEET CUSTOMER'S REQUIREMENTS, ACHIEVE ANY INTENDED RESULTS, BE COMPATIBLE OR WORK WITH ANY OTHER SOFTWARE, APPLICATIONS, SYSTEMS OR SERVICES, OPERATE WITHOUT INTERRUPTION, MEET ANY PERFORMANCE OR RELIABILITY STANDARDS OR BE ERROR FREE OR THAT ANY ERRORS OR DEFECTS CAN OR WILL BE CORRECTED.

WITHOUT LIMITING THE FOREGOING, NEITHER CERTIK NOR ANY OF CERTIK'S AGENTS MAKES ANY REPRESENTATION OR WARRANTY OF ANY KIND, EXPRESS OR IMPLIED AS TO THE ACCURACY, RELIABILITY, OR CURRENCY OF ANY INFORMATION OR CONTENT PROVIDED THROUGH THE SERVICE. CERTIK WILL ASSUME NO LIABILITY OR RESPONSIBILITY FOR (I) ANY ERRORS, MISTAKES, OR INACCURACIES OF CONTENT AND MATERIALS OR FOR ANY LOSS OR DAMAGE OF ANY KIND INCURRED AS A RESULT OF THE USE OF ANY CONTENT, OR (II) ANY PERSONAL INJURY OR PROPERTY DAMAGE, OF ANY NATURE WHATSOEVER, RESULTING FROM CUSTOMER'S ACCESS TO OR USE OF THE SERVICES, ASSESSMENT REPORT, OR OTHER MATERIALS.

ALL THIRD-PARTY MATERIALS ARE PROVIDED "AS IS" AND ANY REPRESENTATION OR WARRANTY OF OR CONCERNING ANY THIRD-PARTY MATERIALS IS STRICTLY BETWEEN CUSTOMER AND THE THIRD-PARTY OWNER OR DISTRIBUTOR OF THE THIRD-PARTY MATERIALS.

THE SERVICES, ASSESSMENT REPORT, AND ANY OTHER MATERIALS HEREUNDER ARE SOLELY PROVIDED TO CUSTOMER AND MAY NOT BE RELIED ON BY ANY OTHER PERSON OR FOR ANY PURPOSE NOT SPECIFICALLY IDENTIFIED IN THIS AGREEMENT, NOR MAY COPIES BE DELIVERED TO, ANY OTHER PERSON WITHOUT CERTIK'S PRIOR WRITTEN CONSENT IN EACH INSTANCE.

NO THIRD PARTY OR ANYONE ACTING ON BEHALF OF ANY THEREOF, SHALL BE A THIRD PARTY OR OTHER BENEFICIARY OF SUCH SERVICES, ASSESSMENT REPORT, AND ANY ACCOMPANYING

MATERIALS AND NO SUCH THIRD PARTY SHALL HAVE ANY RIGHTS OF CONTRIBUTION AGAINST CERTIK WITH RESPECT TO SUCH SERVICES, ASSESSMENT REPORT, AND ANY ACCOMPANYING MATERIALS.

THE REPRESENTATIONS AND WARRANTIES OF CERTIK CONTAINED IN THIS AGREEMENT ARE SOLELY FOR THE BENEFIT OF CUSTOMER. ACCORDINGLY, NO THIRD PARTY OR ANYONE ACTING ON BEHALF OF ANY THEREOF, SHALL BE A THIRD PARTY OR OTHER BENEFICIARY OF SUCH REPRESENTATIONS AND WARRANTIES AND NO SUCH THIRD PARTY SHALL HAVE ANY RIGHTS OF CONTRIBUTION AGAINST CERTIK WITH RESPECT TO SUCH REPRESENTATIONS OR WARRANTIES OR ANY MATTER SUBJECT TO OR RESULTING IN INDEMNIFICATION UNDER THIS AGREEMENT OR OTHERWISE.

FOR AVOIDANCE OF DOUBT, THE SERVICES, INCLUDING ANY ASSOCIATED ASSESSMENT REPORTS OR MATERIALS, SHALL NOT BE CONSIDERED OR RELIED UPON AS ANY FORM OF FINANCIAL, TAX, LEGAL, REGULATORY, OR OTHER ADVICE.

About

Founded in 2017 by leading academics in the field of Computer Science from both Yale and Columbia University, CertiK is a leading blockchain security company that serves to verify the security and correctness of smart contracts and blockchain-based protocols. Through the utilization of our world-class technical expertise, alongside our proprietary, innovative tech, we're able to support the success of our clients with best-in-class security, all whilst realizing our overarching vision; provable trust for all throughout all facets of blockchain.