

TechRate
September, 2022



SMART CONTRACTS SECURITY AUDIT REPORT



Techrate_audits



Techrate



Techrate1

Audit Details



Audited project

WSCMasterChef



Deployer address

0x5e76f735f5b9bfce423649116397f870247457f5



Client contacts:

https://twitter.com/WSecrets_WSC



Blockchain

Binance Smart Chain



Project website:

<https://staking.wealthsecrets.io>

Disclaimer

This is a limited report on our findings based on our analysis, in accordance with good industry practice as at the date of this report, in relation to cybersecurity vulnerabilities and issues in the framework and algorithms based on smart contracts, the details of which are set out in this report. In order to get a full view of our analysis, it is crucial for you to read the full report. While we have done our best in conducting our analysis and producing this report, it is important to note that you should not rely on this report and cannot claim against us on the basis of what it says or doesn't say, or how we produced it, and it is important for you to conduct your own independent investigations before making any decisions. We go into more detail on this in the disclaimer below – please make sure to read it in full.

DISCLAIMER: By reading this report or any part of it, you agree to the terms of this disclaimer. If you do not agree to the terms, then please immediately cease reading this report, and delete and destroy any and all copies of this report downloaded and/or printed by you. This report is provided for information purposes only and on a non-reliance basis, and does not constitute investment advice. No one shall have any right to rely on the report or its contents, and TechRate and its affiliates (including holding companies, shareholders, subsidiaries, employees, directors, officers and other representatives) (TechRate) owe no duty of care towards you or any other person, nor does TechRate make any warranty or representation to any person on the accuracy or completeness of the report. The report is provided "as is", without any conditions, warranties or other terms of any kind except as set out in this disclaimer, and TechRate hereby excludes all representations, warranties, conditions and other terms (including, without limitation, the warranties implied by law of satisfactory quality, fitness for purpose and the use of reasonable care and skill) which, but for this clause, might have effect in relation to the report. Except and only to the extent that it is prohibited by law, TechRate hereby excludes all liability and responsibility, and neither you nor any other person shall have any claim against TechRate, for any amount or kind of loss or damage that may result to you or any other person (including without limitation, any direct, indirect, special, punitive, consequential or pure economic loss or damages, or any loss of income, profits, goodwill, data, contracts, use of money, or business interruption, and whether in delict, tort (including without limitation negligence), contract, breach of statutory duty, misrepresentation (whether innocent or negligent) or otherwise under any claim of any nature whatsoever in any jurisdiction) in any way arising from or connected with this report and the use, inability to use or the results of use of this report, and any reliance on this report.

The analysis of the security is purely based on the smart contracts alone. No applications or operations were reviewed for security. No product code has been reviewed.

Background

TechRate was commissioned by WSCMasterChef to perform an audit of smart contracts:

<https://bscscan.com/address/0xf4d815aF311C3A83E3e274a61C4d5f16395bD604#code>

The purpose of the audit was to achieve the following:

- Ensure that the smart contract functions as intended.
- Identify potential security issues with the smart contract.

The information in this report should be used to understand the risk exposure of the smart contract, and as a guide to improve the security posture of the smart contract by remediating the issues that were identified.

Contracts Details

Token contract details for 30.08.2022

Contract name WSCMasterChef

Contract address 0xf4d815aF311C3A83E3e274a61C4d5f16395bD604

Token per block 1000000000

Total Alloc point 130

Token 0xb7dacf54a54bfea818f21472d3e71a89287841a7

Fee address 0xd0a4ff684e59aec77b2b6bec77b2a91add36fabb

Dev address 0xcf1d1f54ef1b15b042ca70b508e384aad35f120f

Contract deployer address 0x5e76f735f5b9bfce423649116397f870247457f5

Owner address 0xcf1d1f54ef1b15b042ca70b508e384aad35f120f

Contract functions details

+ [Lib] SafeMath

- [Int] tryAdd
- [Int] trySub
- [Int] tryMul
- [Int] tryDiv
- [Int] tryMod
- [Int] add
- [Int] sub
- [Int] mul
- [Int] div
- [Int] mod
- [Int] sub
- [Int] div
- [Int] mod

+ [Int] IBEP20

- [Ext] totalSupply
- [Ext] decimals
- [Ext] symbol
- [Ext] name
- [Ext] getOwner
- [Ext] balanceOf
- [Ext] transfer #
- [Ext] allowance
- [Ext] approve #
- [Ext] transferFrom #

+ [Lib] Address

- [Int] isContract
- [Int] sendValue #
- [Int] functionCall #
- [Int] functionCall #
- [Int] functionCallWithValue #
- [Int] functionCallWithValue #
- [Int] functionStaticCall
- [Int] functionStaticCall
- [Int] functionDelegateCall #
- [Int] functionDelegateCall #
- [Priv] _verifyCallResult

+ [Lib] SafeBEP20

- [Int] safeTransfer #

- [Int] safeTransferFrom #
- [Int] safeApprove #
- [Int] safeIncreaseAllowance #
- [Int] safeDecreaseAllowance #
- [Prv] _callOptionalReturn #

+ [Int] ITokenReferral

- [Ext] recordReferral #
- [Ext] recordReferralCommission #
- [Ext] getReferrer

+ Context

- [Int] _msgSender
- [Int] _msgData

+ Ownable (Context)

- [Int] <Constructor> #
- [Pub] owner
- [Pub] renounceOwnership #
 - modifiers: onlyOwner
- [Pub] transferOwnership #
 - modifiers: onlyOwner

+ ReentrancyGuard

- [Int] <Constructor> #

+ WSCMasterChef (Ownable, ReentrancyGuard)

- [Pub] <Constructor> #
- [Ext] poolLength
- [Ext] add #
 - modifiers: onlyOwner
- [Ext] set #
 - modifiers: onlyOwner
- [Pub] getMultiplier
- [Pub] pendingToken
- [Pub] canHarvest
- [Ext] deposit #
 - modifiers: nonReentrant
- [Ext] withdraw #
 - modifiers: nonReentrant
- [Ext] emergencyWithdraw #
 - modifiers: nonReentrant
- [Ext] setEmergencyWithdrawFee #
 - modifiers: onlyOwner
- [Int] payOrLockupPendingToken #

- [Ext] setDevAddress #
 - modifiers: onlyOwner
- [Ext] setFeeAddress #
 - modifiers: onlyOwner
- [Ext] setTokenReferral #
 - modifiers: onlyOwner
- [Ext] setTokenPerblock #
 - modifiers: onlyOwner
- [Ext] setReferralCommissionRate #
 - modifiers: onlyOwner
- [Int] payReferralCommission #
- [Ext] addBalance #
 - modifiers: onlyOwner
- [Int] mint #
- [Int] safeTokenTransfer #
- [Pub] getBlock
- [Ext] recoverTokens #
 - modifiers: onlyOwner
- [Ext] recoverTreasure #
 - modifiers: onlyOwner

(\$)= payable function

= non-constant function

Issues Checking Status

Issue description	Checking status
1. Compiler errors.	Passed
2. Race conditions and Reentrancy. Cross-function race conditions.	Passed
3. Possible delays in data delivery.	Passed
4. Oracle calls.	Passed
5. Front running.	Passed
6. Timestamp dependence.	Passed
7. Integer Overflow and Underflow.	Passed
8. DoS with Revert.	Passed
9. DoS with block gas limit.	Passed
10. Methods execution permissions.	Passed
11. Economy model of the contract.	Passed
12. The impact of the exchange rate on the logic.	Passed
13. Private user data leaks.	Passed
14. Malicious Event log.	Passed
15. Scoping and Declarations.	Passed
16. Uninitialized storage pointers.	Passed
17. Arithmetic accuracy.	Passed
18. Design Logic.	Passed
19. Cross-function race conditions.	Passed
20. Safe Open Zeppelin contracts implementation and usage.	Passed
21. Fallback function security.	Passed

Security Issues

✓ High Severity Issues

No high severity issues found.

✓ Medium Severity Issues

No medium severity issues found.

✓ Low Severity Issues

No low severity issues found.

Notes:







- Contract has withdrawal & emergency withdrawal fee.
- Mint function do not actually mint, but reduces treasure and allocated amounts.

Owner privileges (In the period when the owner is not renounced)



- Owner can change tokenReferral.
- Owner can change tokenPerBlock.
- Owner can change referralCommissionRate.
- Owner can change dev and fee addresses.
- Owner can increase contract balance.
- Owner can withdraw BEP20 tokens.

Testnet deployment

Contracts Description Table

Contract	Type	Bases	Mutability	Modifiers
L	Function Name	Visibility		
WSCMasterChef	Implementation	Ownable, ReentrancyGuard		
L	add	External !		onlyOwner
L	set	External !		onlyOwner
L	deposit	External !		nonReentrant
L	withdraw	External !		nonReentrant
L	emergencyWithdraw	External !		nonReentrant
L	addBalance	External !		onlyOwner

Legend

Symbol	Meaning
	Function can modify state
	Function is payable

Conclusion

Smart contracts do not contain high severity issues! The further transfers and operations with the funds raise are not related to this particular contract.

Security score: 90.

TechRate note:

Please check the disclaimer above and note, the audit makes no statements or warranties on business model, investment attractiveness or code sustainability. The report is provided for the only contract mentioned in the report and does not include any other potential contracts deployed by Owner.