

TechRate
September, 2022



SMART CONTRACTS SECURITY AUDIT REPORT



Techrate_audits



Techrate



Techrate1

Audit Details



Audited project

Risu



Deployer address

0xbbc56b7cc37f792221ac048e5baa99fdd3ccd765



Client contacts:

Risu team



Blockchain

Binance Smart Chain



Project website:

<https://risutoken.com>

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 Risu to perform an audit of smart contracts:

<https://bscscan.com/address/0x8163100460d2186de4e700c479d5e87283426d27#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 08.09.2022

Contract name Risu

Contract address 0x8163100460d2186DE4e700C479D5e87283426D27

Total supply 1,000,000,000

Token ticker RISU

Decimals 9

Token holders 2,088

Transactions count 19,782

Top 100 holders dominance 79.13%

Min buy limit 1000000000000000000

Max holding amount 200000000000000000

Total holders distribution 25388182858035575

Uniswap V2 pair 0x26793a1dfb68502d7aba66bf38056f7a115b6942

Contract deployer address 0xbbc56b7cc37f792221ac048e5baa99fdd3ccd765

Owner address 0x00

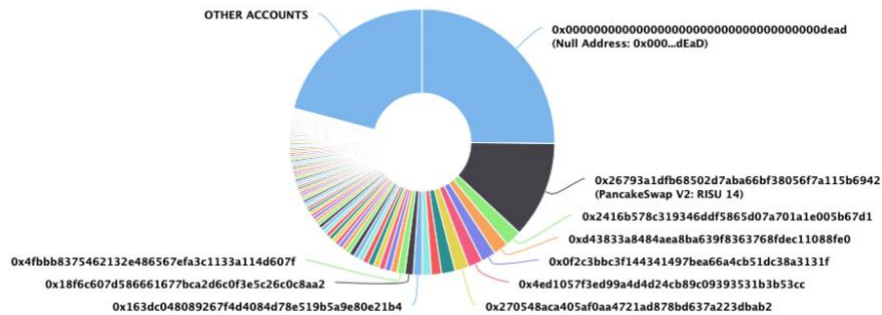
Risu Token Distribution

The top 100 holders collectively own 79.13% (791,269,184.39 Tokens) of Risu

Token Total Supply: 1,000,000,000.00 Token | Total Token Holders: 2,088

Risu Top 100 Token Holders

Source: BscScan.com



(A total of 791,269,184.39 tokens held by the top 100 accounts from the total supply of 1,000,000,000.00 token)

Risu Contract Interaction Details

Time Series: Token Contract Overview

Sun 4, Sept 2022 - Wed 7, Sept 2022

Token Contract 0x8163100460d2186de4e700c479d5e87283426d27 (Risu)
Source: BscScan.com



Risu Top 10 Token Holders

Rank	Address	Quantity (Token)	Percentage
1	Null Address: 0x000...dEaD	251,730,676.042919461	25.1731%
2	PancakeSwap V2: RISU 14	117,533,725.015644519	11.7534%
3	0x2416b578c319346ddf5865d07a701a1e005b67d1	20,000,000	2.0000%
4	0xd43833a8484aea8ba639f8363768fdec11088fe0	18,105,139.548272479	1.8105%
5	0x0f2c3bbc3f144341497bea66a4cb51dc38a3131f	17,891,775.469583832	1.7892%
6	0x4ed1057f3ed99a4d4d24cb89c09393531b3b53cc	17,434,359.796192955	1.7434%
7	0x270548aca405af0aa4721ad878bd637a223dbab2	17,298,675.02494521	1.7299%
8	0x376d8277bc84ab477130456dd939d26775579d9c	16,554,061.09444732	1.6554%
9	0x2f65d8f9ef83097d26277aabea0631be77cb25b5	12,236,493.418533646	1.2236%
10	0xffaa26f715162224071d6991ca85f0b04cebb1de	11,161,153.619186893	1.1161%

Risu LP Token Holders

Rank	Address	Quantity	Percentage
1	Pinksale: PinkLock V2	3.060958674464409282	87.6179%
2	0x163dc048089267f4d4084d78e519b5a9e80e21b4	0.334554266689331676	9.5764%
3	Null Address: 0x000...000	0.063645751427420713	1.8218%
4	0x0ed943ce24baebf257488771759f9b482c39706	0.034370606644245433	0.9838%

Contract functions details

+ [Int] IBEP20

- [Ext] totalSupply
- [Ext] balanceOf
- [Ext] transfer #
- [Ext] allowance
- [Ext] approve #
- [Ext] transferFrom #

+ [Int] IDexFactory

- [Ext] createPair #

+ [Int] IDexRouter

- [Ext] factory
- [Ext] WETH
- [Ext] addLiquidityETH (\$)
- [Ext] swapExactTokensForETHSupportingFeeOnTransferTokens #

+ Context

- [Int] _msgSender
- [Int] _msgData

+ Ownable (Context)

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

+ [Lib] SafeMath

- [Int] add
- [Int] sub
- [Int] sub
- [Int] mul
- [Int] div
- [Int] div
- [Int] mod
- [Int] mod

+ RISU (Context, IBEP20, Ownable)

- [Pub] <Constructor> #
- [Pub] name
- [Pub] symbol
- [Pub] decimals
- [Pub] totalSupply
- [Pub] balanceOf
- [Pub] allowance
- [Pub] transfer #
- [Pub] approve #
- [Pub] transferFrom #
- [Pub] increaseAllowance #
- [Pub] decreaseAllowance #
- [Pub] isExcludedFromReward
- [Pub] totalHolderDistribution
- [Pub] isExcludedFromFee
- [Pub] isExcludedFromMaxHoldLimit
- [Pub] isExcludedFromMaxTxnLimit
- [Pub] deliver #
- [Pub] reflectionFromToken
- [Pub] tokenFromReflection
- [Pub] includeOrExcludeFromMaxHoldLimit #
 - modifiers: onlyOwner
- [Pub] includeOrExcludeFromMaxTxnLimit #
 - modifiers: onlyOwner
- [Pub] setAntiBotStopEnabled #
 - modifiers: onlyOwner
- [Pub] setMaxHoldingAmount #
 - modifiers: onlyOwner
- [Pub] setMinBuyLimit #
 - modifiers: onlyOwner
- [Ext] removeStuckToken #
 - modifiers: onlyOwner
- [Ext] setSellFeePercent #
 - modifiers: onlyOwner
- [Pub] includeOrExcludeFromFee #
 - modifiers: onlyOwner
- [Pub] setMinTokenToSwap #
 - modifiers: onlyOwner
- [Ext] setBuyFeePercent #
 - modifiers: onlyOwner
- [Pub] enableOrDisableSwapAndLiquify #
 - modifiers: onlyOwner
- [Ext] enableOrDisableFees #
 - modifiers: onlyOwner
- [Ext] setmarketWalletAddress #

- modifiers: onlyOwner
 - [Ext] <Fallback> (\$)
 - [Int] totalFeePerTx
 - [Prv] _checkMaxWalletAmount
 - [Prv] _getRate
 - [Prv] setBuyFee #
 - [Prv] _getCurrentSupply
 - [Prv] removeAllFee #
 - [Prv] setSellFee #
 - [Ext] addSniperInList #
 - modifiers: onlyOwner
 - [Ext] removeSniperFromList #
 - modifiers: onlyOwner
 - [Prv] _approve #
 - [Prv] _transfer #
 - [Prv] _tokenTransfer #
 - [Prv] _transferStandard #
 - [Prv] _transferFromExcluded #
 - [Prv] _transferBothExcluded #
 - [Prv] _transferToExcluded #
 - [Prv] _reflectFee #
 - [Int] _takeAllFee #
 - [Int] _takeBurnFee #
 - [Prv] swapAndLiquify #
- + [Lib] Utils
- [Int] swapTokensForEth #
 - [Int] addLiquidity #

(\$) = 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:





















- Exclusion from reward is not realized, so using this logic for transfer is unused.
- transferFrom() function include sniper restriction, that is also included in internal transfer function.
- Contract can receive BNB, but there is no logic to withdraw it.
- Owner can pause transfers.
- Comments don't match the condition – *"require(amount <= minBuyLimit, "Amount must be greater than minimum buy Limit")"*
- Fees are taking only in DEX transactions.

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



- Owner can include/exclude from max hold limit.
- Owner can enable/disable antiBotStopEnabled.
- Owner can change maxHoldingAmount and minBuyLimit.
- Owner can withdraw BEP20 tokens.
- Owner can change fees.
- Owner can change minTokenToSwap.
- Owner can exclude from the fees.
- Owner can enable/disable swap and liquify.
- Owner can enable/disable fees.
- Owner can change marketWallet.
- Owner can add/remove snipers.

Testnet deployment

Contracts Description Table

Contract	Type	Bases		
L	Function Name	Visibility	Mutability	Modifiers
RISU	Implementation	Context, IBEP20, Ownable		
L	transfer	Public !		NO !
L	approve	Public !		NO !
L	transferFrom	Public !		NO !
L	increaseAllowance	Public !		NO !
L	decreaseAllowance	Public !		NO !
L	deliver	Public !		NO !
L	includeOrExcludeFromMaxHoldLimit	Public !		onlyOwner
L	includeOrExcludeFromMaxTxnLimit	Public !		onlyOwner
L	setAntiBotStopEnabled	Public !		onlyOwner
L	setMaxHoldingAmount	Public !		onlyOwner
L	setMinBuyLimit	Public !		onlyOwner
L	removeStuckToken	External !		onlyOwner
L	setSellFeePercent	External !		onlyOwner
L	includeOrExcludeFromFee	Public !		onlyOwner
L	setMinTokenToSwap	Public !		onlyOwner
L	setBuyFeePercent	External !		onlyOwner
L	enableOrDisableSwapAndLiquify	Public !		onlyOwner
L	enableOrDisableFees	External !		onlyOwner
L	setmarketWalletAddress	External !		onlyOwner
L	addSniperInList	External !		onlyOwner
L	removeSniperFromList	External !		onlyOwner

Legend

Symbol	Meaning
	Function can modify state
	Function is payable

Conclusion

Smart contracts do not contain high severity issues! Liquidity pair contract's security is not checked due to out of scope. The further transfers and operations with the funds raise are not related to this particular contract.

Liquidity locking details are provided by the team:

<https://www.pinksale.finance/pinklock/record/1035212?chain=BSC>

Security score: 85.

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.