

TechRate
November, 2022



SMART CONTRACTS SECURITY AUDIT REPORT



Techrate_audits



Techrate



Techrate1

Audit Details



Audited project

WORLD CUP INU



Deployer address

0x6FB8Efee44784af8a0d1fb32811ef417471A5416



Client contacts:

WORLD CUP INU team



Blockchain

Ethereum



Project website:

<https://worldcupinu.app>

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 WORLD CUP INU to perform an audit of smart contracts:

<https://etherscan.io/address/0xC5a9BC46A7dbe1c6dE493E84A18f02E70E2c5A32#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 13.11.2022

Contract name WORLD CUP INU

Contract address 0xC5a9BC46A7dbe1c6dE493E84A18f02E70E2c5A32

Total supply 1,000,000,000

Token ticker WCI

Decimals 9

Token holders 5,588

Transactions count 45,037

Top 100 holders dominance 48.47%

Total fee 500

Liquidity fee receiver 0x6FB8Efee44784af8a0d1fb32811ef417471A5416

Marketing fee receiver 0x6FB8Efee44784af8a0d1fb32811ef417471A5416

pair 0xD17E88b13E53029F356D46aBa44B5640B35C8e9C

Contract deployer address 0x6FB8Efee44784af8a0d1fb32811ef417471A5416

Owner address 0x6FB8Efee44784af8a0d1fb32811ef417471A5416

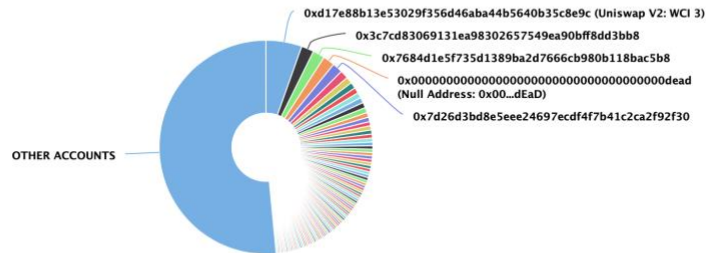
WORLD CUP INU Token Distribution

The top 100 holders collectively own 48.47% (484,723,183.99 Tokens) of WORLD CUP INU

Token Total Supply: 1,000,000,000.00 Token | Total Token Holders: 5,588

WORLD CUP INU Top 100 Token Holders

Source: Etherscan.io



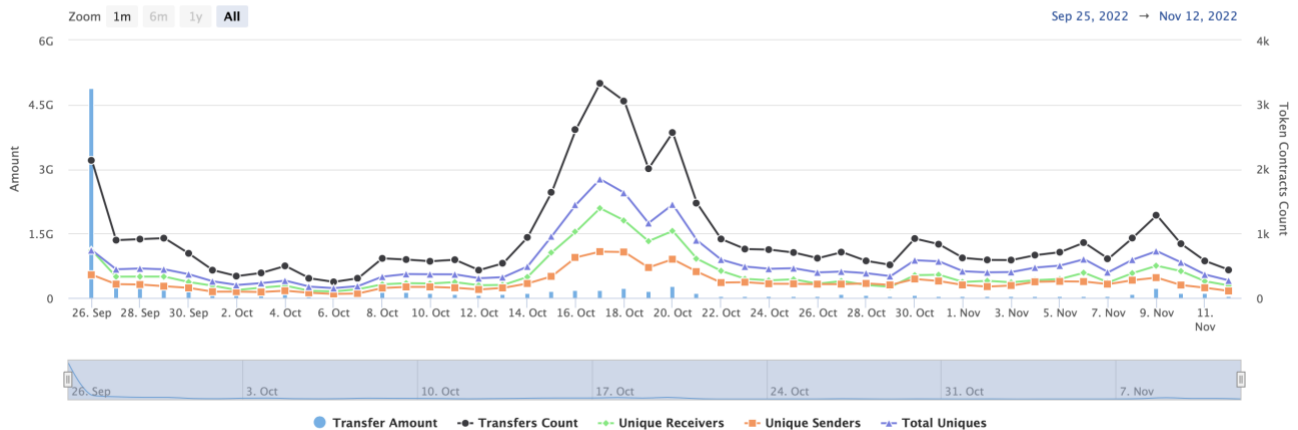
(A total of 484,723,183.99 tokens held by the top 100 accounts from the total supply of 1,000,000,000.00 token)

WORLD CUP INU Contract Interaction Details


Time Series: Token Contract Overview

Mon 26, Sept 2022 - Sat 12, Nov 2022


Token Contract 0xC5a98C46A7d8e1c6dE493E84A18f02E70E2c5A32 (WORLD CUP INU)
Source: Etherscan.io



WORLD CUP INU Top 10 Token Holders

| Rank | Address | Quantity (Token) | Percentage |
|------|---|----------------------|------------|
| 1 |  Uniswap V2: WCI 3 | 54,471,541.377069844 | 5.4472% |
| 2 | 0x3c7cd83069131ea98302657549ea90bfff8dd3bb8 | 18,854,235.511486 | 1.8854% |
| 3 | 0x7684d1e5f735d1389ba2d7666cb980b118bac5b8 | 18,204,037.240532906 | 1.8204% |
| 4 | Null Address: 0x00...dEaD | 17,640,551.88900701 | 1.7641% |
| 5 | 0x7d26d3bd8e5eee24697ecd4f7b41c2ca2f92f30 | 15,503,239.644476165 | 1.5503% |
| 6 | 0xa2091f370bf0f56d014cfd13ad86d876b434ee84 | 12,586,425.562336214 | 1.2586% |
| 7 | 0x9d8d250285de197a9a1fe6e7a22e85f949930803 | 10,000,182.28583347 | 1.0000% |
| 8 | 0xf92d1489e4ca27d7a9b69549be698616dfa7ac3c | 9,354,861.2 | 0.9355% |
| 9 | 0x7073e0e2ac3b0cd36e3e1fc682c545fd8ed64848 | 8,600,000.000000655 | 0.8600% |
| 10 | 0xad7b013f817528c6e143a8543944a4bb4b78a0c6 | 8,288,862.300146151 | 0.8289% |

WORLD CUP INU LP Token Holders

| Rank | Address | Quantity | Percentage |
|------|--|----------------------|------------|
| 1 |  TrustSwap: Team Finance Lock | 3.769326997499629331 | 88.9206% |
| 2 | World Cup Inu: Deployer | 0.329516263339543322 | 7.7735% |
| 3 | Null Address: 0x00...dEaD | 0.139547408535132508 | 3.2920% |
| 4 | 0x7fd987fb6f6bc446500c7c989bf88e5cac5e1f51 | 0.000439028496303932 | 0.0104% |
| 5 | 0xc04f8a544f49c86142df090389111d06cb9e5ef1 | 0.000151655271137255 | 0.0036% |
| 6 | Null Address: 0x000...000 | 0.0000000000000001 | 0.0000% |

Contract functions details

+ [Lib] Address

- [Int] isContract
- [Int] sendValue #
- [Int] functionCall #
- [Int] functionCall #
- [Int] functionCallWithValue #
- [Int] functionCallWithValue #
- [Prv] _functionCallWithValue #

+ Context

- [Int] _msgSender
- [Int] _msgData

+ [Int] IERC20

- [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 #

+ Ownable (Context)

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

+ WORLDCUPINU (IERC20, Ownable)

- [Pub] <Constructor> #
- [Ext] <Fallback> (\$)

- [Ext] totalSupply
- [Ext] decimals
- [Ext] symbol
- [Ext] name
- [Ext] getOwner
- [Ext] maxBuyTxTokens
- [Ext] maxSellTxTokens
- [Ext] maxWalletTokens
- [Pub] balanceOf
- [Ext] allowance
- [Pub] approve #
- [Ext] approveMax #
- [Ext] setTeamMember #
 - modifiers: onlyOwner
- [Ext] airdrop #
 - modifiers: onlyOwner
- [Ext] clearStuckBalance #
 - modifiers: onlyTeam
- [Ext] openTrading #
 - modifiers: onlyTeam
- [Ext] pauseTrading #
 - modifiers: onlyTeam
- [Ext] disablePause #
 - modifiers: onlyTeam
- [Ext] setProtection #
 - modifiers: onlyTeam
- [Ext] disableProtection #
 - modifiers: onlyTeam
- [Ext] protectWallet #
 - modifiers: onlyTeam
- [Ext] transfer #
- [Ext] transferFrom #
- [Int] _transferFrom #
- [Int] launched
- [Int] launch #
- [Int] _basicTransfer #
- [Int] checkWalletLimit
- [Int] checkTxLimit #
- [Int] shouldTakeFee
- [Pub] getTotalFee
- [Int] takeFee #
- [Int] shouldSwapBack
- [Int] swapBack #
 - modifiers: swapping
- [Ext] addLiquidityPool #

- modifiers: onlyOwner
- [Ext] setRateLimit #
 - modifiers: onlyOwner
- [Ext] setTxLimit #
 - modifiers: onlyOwner
- [Ext] setMaxWallet #
 - modifiers: onlyOwner
- [Ext] setIsFeeExempt #
 - modifiers: onlyOwner
- [Ext] setIsTxLimitExempt #
 - modifiers: onlyOwner
- [Ext] setFees #
 - modifiers: onlyOwner
- [Ext] setFeeReceivers #
 - modifiers: onlyOwner
- [Ext] setSwapBackSettings #
 - modifiers: onlyOwner
- [Pub] getCirculatingSupply

(\$) = 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. | Low issues |
| 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

1. Out of gas

Issue:

- The function `airdrop()` uses the loop to distribute amounts to multiple accounts. Function will be aborted with `OUT_OF_GAS` exception if there will be a long addresses list.

Recommendation:

Be careful about addresses array length.

Issue:

- The function `protectWallet()` uses the loop to protect/unprotect wallets. Function will be aborted with `OUT_OF_GAS` exception if there will be a long wallets list.

Recommendation:

Be careful about wallets array length.

Notes:










- Old owner is not removed from exemptions after transferring ownership.
- `"processEnabled"` is not used.
- Protection settings can restrict transfers but don't public.

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



- Owner can set team members.
- Owner can airdrop.
- Owner can add liquidity pool.
- Owner can change rate limit.
- Owner can change max buy and sell tx amount.
- Owner can change max wallet size.
- Owner can include in and exclude from fee and transaction amount.
- Owner can change fees.
- Owner can change fee receivers.
- Owner can change swapBack settings.
- Team member can withdraw contract ETHs.
- Team member can open trading.
- Team member can stop trading.
- Team member can disable pause trading.
- Team member can change protection settings.

Testnet deployment

Contracts Description Table

| Contract | Type | Bases | Mutability | Modifiers |
|---------------|-------------------------------------|-----------------|---|-----------|
| L | Function Name | Visibility | | |
| WORLD CUP INU | Implementation | IERC20, Ownable | | |
| L | approve | Public ! |  | NO ! |
| L | setTeamMember | External ! |  | onlyOwner |
| L | openTrading | External ! |  | onlyTeam |
| L | transfer | External ! |  | NO ! |
| L | transferFrom | External ! |  | NO ! |
| L | setRateLimit | External ! |  | onlyOwner |
| L | setFees | External ! |  | onlyOwner |
| L | setFeeReceivers | External ! |  | onlyOwner |
| L | setSwapBackSettings | External ! |  | onlyOwner |

Legend

| Symbol | Meaning |
|---|---------------------------|
|  | Function can modify state |
|  | Function is payable |

Conclusion

Smart contracts contain low 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 provided by the team:

<https://www.team.finance/view-coin/0xC5a9BC46A7dbe1c6dE493E84A18f02E70E2c5A32?name=WORLD%20CUP%20INU&symbol=WCI>

Security score: 82.

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.