https://t.me/SolCheck

< SolCheck >

Smart Contract Security Audit

Audit Details

Project:
ChampInu

Deployer Address:
0x5e2491d1bc154a3331d711435e8e31B88C7f6D1c

Contract Address:
0x44C263E76814dCf9c710E992306c4FdfBfB0429D

Blockchain:
Binance Smart Chain (BSC)

Project website:
https://champinu.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 below 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 SolCheck and its affiliates (including holding companies, shareholders, subsidiaries, employees, directors, officers and other representatives) (SolCheck) owe no duty of care towards you or any other person, nor does SolCheck 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 SolCheck 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, SolCheck hereby excludes all liability and responsibility, and neither you nor any other person shall have any claim against SolCheck, 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

SolCheck performed a free smart contract audit of contract:

https://bscscan.com/address/0x44C263E76814dCf9c710E992306c4FdfBfB0429D

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.

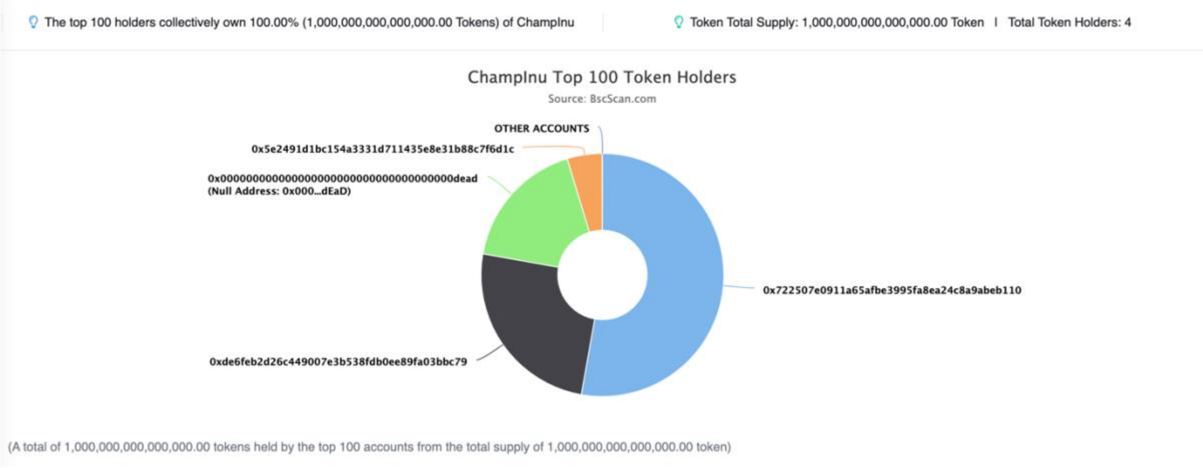
The information in this report should be used to understand the risk exposure of the smart contract, and as a guide to improve the security posture of the smart contract by remediating the issues that were identified.

Contract Details

Contract details for 23.01.2022

Contract Name	ChampInu
Contract Address	0x44C263E76814dCf9c710E992306c4FdfBfB0429D
Total Supply	1,000,000,000,000,000
Token Symbol	ChampInu
Decimals	9
Token holders	4
Transactions count	7
Top 100 holders dominance	100%
Contract Deployer address	0x5e2491d1bc154a3331d711435e8e31B88C7f6D1c
Contract's current owner address	0x5e2491d1bc154a3331d711435e8e31B88C7f6D1c

ChampInu Token Distribution



The top 100 holders collectively own 100.00% (1,000,000,000,000,000.00 Tokens) of ChampInu

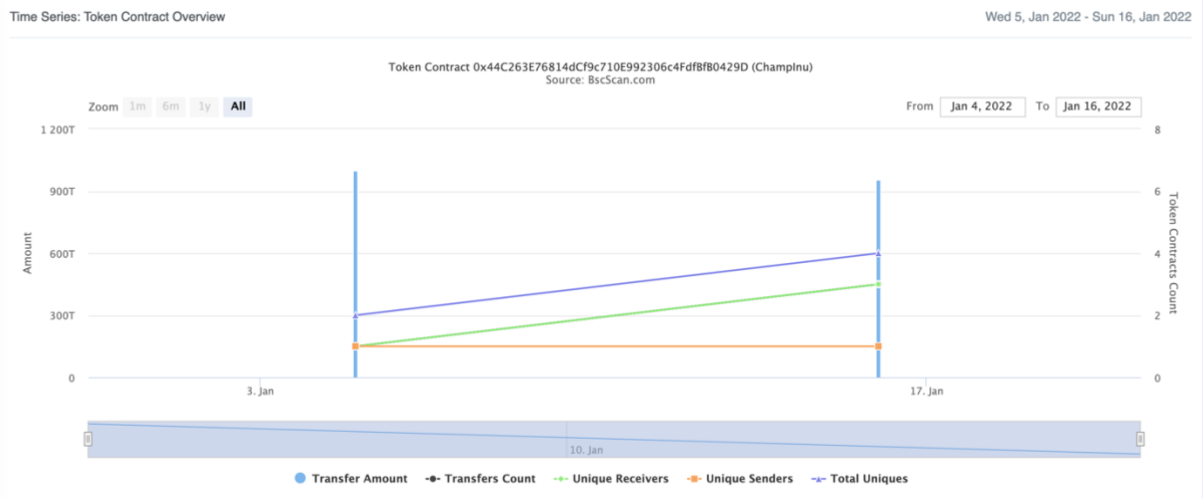
Token Total Supply: 1,000,000,000,000,000.00 Token | Total Token Holders: 4

ChampInu Top 100 Token Holders

Source: BscScan.com

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

Contract Interaction Details



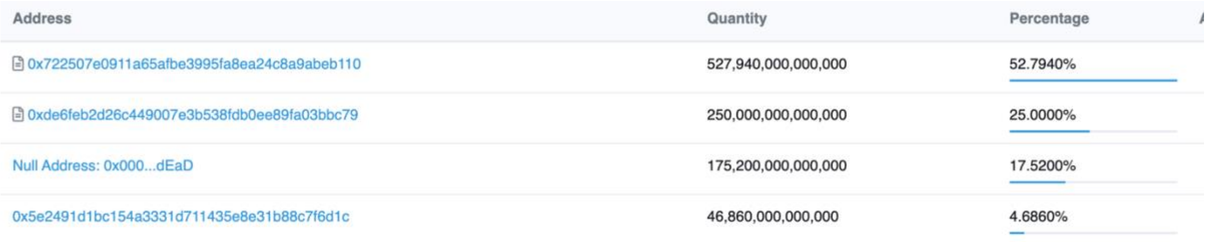
Time Series: Token Contract Overview

Wed 5, Jan 2022 - Sun 16, Jan 2022

Token Contract 0x44C263E76814dCf9c710E992306c4FdfBfB0429D (ChampInu)

Source: BscScan.com

ChampInu Top 100 Holders



Address	Quantity	Percentage
0x722507e0911a65afbe3995fa8ea24c8a9abeb110	527,940,000,000,000	52.7940%
0xde6feb2d26c449007e3b538fdb0ee89fa03bbc79	250,000,000,000,000	25.0000%
Null Address: 0x000...dEaD	175,200,000,000,000	17.5200%
0x5e2491d1bc154a3331d711435e8e31b88c7f6d1c	46,860,000,000,000	4.6860%

Contract Functions Details

+ **Context**
    - [Int] <Constructor>
    - [Int] _msgSender
    - [Int] _msgData
+ **[Int] IERC20**
    - [Ext] totalSupply
    - [Ext] balanceOf
    - [Ext] transfer
    - [Ext] allowance
    - [Ext] approve
    - [Ext] transferFrom
+ **[Lib] SafeMath**
    - [Int] add
    - [Int] sub
    - [Int] sub
    - [Int] mul
    - [Int] div
    - [Int] div
    - [Int] mod
    - [Int] mod
+ **[Lib] Address**
    - [Int] isContract
    - [Int] sendValue
    - [Int] functionCall
    - [Int] functionCall
    - [Int] functionCallWithValue
    - [Int] functionCallWithValue
    - [Prv] _functionCallWithValue
+ **Ownable (Context)**
    - [Int] <Constructor>
        - modifier: onlyOwner
    - [Pub] owner
    - [Pub] renounceOwnership #
    - [Pub] transferOwnership #
    - [Pub] getUnlockTime
    - [Pub] getTime
    - [Pub] lock #
    - [Pub] unlock
+ **[Int] IUniswapV2Factory**
    - [Ext] feeTo
    - [Ext] feeToSetter
    - [Ext] getPair
    - [Ext] allPairs
    - [Ext] allPairsLength
    - [Ext] createPair
    - [Ext] setFeeTo
    - [Ext] setFeeToSetter
+ **[Int] IUniswapV2Pair**
    - [Ext] name
    - [Ext] symbol

```
    - [Ext] totalSupply
    - [Ext] balanceOf
    - [Ext] allowance
    - [Ext] approve
    - [Ext] transfer
    - [Ext] transferFrom
    - [Ext] DOMAIN_SEPARATOR
    - [Ext] PERMIT_TYPEHASH
    - [Ext] nonces
    - [Ext] permit
    - [Ext] MINIMUM_LIQUIDITY
    - [Ext] factory
    - [Ext] token0
    - [Ext] token1
    - [Ext] getReserves
    - [Ext] price0CumulativeLast
    - [Ext] price1CumulativeLast
    - [Ext] kLast
    - [Ext] mint
    - [Ext] burn
    - [Ext] swap
    - [Ext] skim
    - [Ext] sync
    - [Ext] initialize
+ [Int] IUniswapV2Router01
    - [Ext] factory
    - [Ext] WETH
    - [Ext] addLiquidity
    - [Ext] addLiquidityETH $
    - [Ext] removeLiquidity
    - [Ext] removeLiquidityETH
    - [Ext] removeLiquidityWithPermit
    - [Ext] removeLiquidityETHWithPermit
    - [Ext] swapExactTokensForTokens
    - [Ext] swapTokensForExactTokens
    - [Ext] swapExactETHForTokens $
    - [Ext] swapTokensForExactETH
    - [Ext] swapExactTokensForETH
    - [Ext] swapETHForExactTokens $
    - [Ext] quote
    - [Ext] getAmountOut
    - [Ext] getAmountIn
    - [Ext] getAmountsOut
    - [Ext] getAmountsIn
+ [Int] IUniswapV2Router02 (IUniswapV2Router01)
    - [Ext] removeLiquidityETHSupportingFeeOnTransferTokens
    - [Ext] removeLiquidityETHWithPermitSupportingFeeOnTransferTokens
    - [Ext] swapExactTokensForTokensSupportingFeeOnTransferTokens
    - [Ext] swapExactETHForTokensSupportingFeeOnTransferTokens $
    - [Ext] swapExactTokensForETHSupportingFeeOnTransferTokens
+ ChampInu (Context, IERC20, Ownable)
    - [Int] <Constructor>
        - modifier: lockTheSwap
    - [Pub] name
    - [Pub] symbol
    - [Pub] decimals
    - [Pub] totalSupply
    - [Pub] balanceOf
    - [Pub] transfer
    - [Pub] allowance
    - [Pub] approve
    - [Pub] transferFrom
    - [Pub] increaseAllowance
    - [Pub] decreaseAllowance
    - [Pub] isExcludedFromReward
    - [Pub] totalFees
    - [Pub] deliver
    - [Pub] reflectionFromToken
    - [Pub] tokenFromReflection
    - [Pub] excludeFromReward #
    - [Ext] includeInReward #
    - [Prv] _approve
    - [Prv] _transfer
    - [Prv] swapToken
        - modifier: lockTheSwap
    - [Prv] buyBackTokens
        - modifier: lockTheSwap
    - [Prv] swapTokensForEth
    - [Prv] swapETHForTokens
    - [Prv] addLiquidity
    - [Prv] _tokenTransfer
    - [Prv] _transferStandard
    - [Prv] _transferToExcluded
    - [Prv] _transferFromExcluded
    - [Prv] _transferBothExcluded
    - [Prv] _reflectFee
    - [Prv] _getValues
    - [Prv] _getTValues
    - [Prv] _getRValues
    - [Prv] _getRate
    - [Prv] _getCurrentSupply
    - [Prv] _takeLiquidity
    - [Prv] _takeMarketingFee
    - [Prv] calculateReflectionFee
    - [Prv] calculateMarketingFee
    - [Prv] calculateLiquidityFee
    - [Prv] removeAllFee
    - [Prv] restoreAllFee
    - [Pub] isExcludedFromFee
    - [Pub] excludeFromFee #
    - [Pub] includeInFee #
    - [Pub] excludeFromSwapAndLiquify #
    - [Pub] includeInSwapAndLiquify #
    - [Prv] _getSellBnBAmount
    - [Prv] _removeOldSellHistories
    - [Ext] SetBuyBackMaxTimeForHistories #
```

- [Ext] SetBuyBackDivisor #
- [Pub] GetBuyBackTimeInterval
- [Ext] SetBuyBackTimeInterval #
- [Ext] SetBuyBackRangeRate #
- [Pub] GetSwapMinutes
- [Ext] SetSwapMinutes
- [Ext] setReflectionFeePercent #
- [Ext] setMarketingFeePercent #
- [Ext] setLiquidityFeePercent #
- [Ext] setSellFee #
- [Ext] setBuyBackSellLimit #
- [Ext] setMaxTxAmount #
- [Ext] setNumTokensSellToAddToBuyBack #
- [Ext] setMarketingAddress #
- [Ext] setMarketingDivisor #
- [Pub] setSwapAndLiquifyEnabled #
- [Pub] setBuyBackEnabled #
- [Pub] setAutoBuyBackEnabled #
- [Ext] prepareForPreSale #
- [Ext] afterPreSale #
- [Prv] transferToAddressETH
- [Pub] changeRouterVersion #
- [Pub] transferForeignToken #
- [Ext] Sweep #
- [Ext] setAddressFee #
- [Ext] setSellAddressFee #

* $ - payable function
** # - modifier: onlyOwner

Issues Checking Status

Issue Description	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.	Warning
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.	Warning
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.	Warning
19. Cross-function race conditions.	Passed
20. Safe Open Zeppelin contracts implementation and usage	Warning
21. Fallback function security	Passed

Security Checks

☑ High Severity Issues

No high severity issues found

⚠ Medium Severity Issues

- Some function names are declared with starting capital letter

⚠ Low Severity Issues

- _getSellBNBAmount does not account for slippage

Owner Abilities

- ⚠ Exclude / Include in Rewards
- ⚠ Exclude / Include in Fee
- ⚠ Exclude / Include in Swap and Liquify
- ⚠ Change _buyBackMaxTimeForHistories
- ⚠ Change _buyBackDivisor
- ⚠ Change _buyBackTimeInterval
- ⚠ Change _buyBackRange
- ⚠ Change _intervalMinutesForSwap
- ⚠ Change Reflection Fee (up to 100%)
- ⚠ Change Marketing Fee (up to 100%)
- ⚠ Change Liquidity Fee (up to 100%)
- ⚠ Change Sell Fees
- ⚠ Change buyBackSellLimit
- ⚠ Change Maximum Transaction Amount
- ⚠ Change Minimum tokens before swap
- ⚠ Change Marketing Address
- ⚠ Change Marketing Divisor
- ⚠ Enable / Disable Swap and Liquify
- ⚠ Enable / Disable Buy Back
- ⚠ Enable / Disable Auto Buy Back
- ⚠ Change Router Address
- ⚠ Withdraw ERC20 token from the contract (excluding ChampInu)
- ⚠ Withdraw BNB from contract
- ⚠ Change Liquidity and Reflection Fee addresses

Conclusion

Although this ERC20-compatible token smart contract does not have any severe security issues, owner has a lot of control over token functionality. Until ownership is renounces, addresses could be potentially banned from swapping and transferring tokens.

SolCheck 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.