February, 2022

TechRate

AUDIT COMPANY

Smart Contract Security Audit

TechRate

February, 2022

Audit Details

Audited project

CateDogeInuSafeElonMoonMars

Deployer address

0x5864ce873e3742b9abb90fa3cb8a8ac9e22dec9a

Client contacts:

CateDogeInuSafeElonMoonMars team

Blockchain

Binance Smart Chain

Project website:

https://cdisemmtoken.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 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 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 CateDogeInuSafeElonMoonMars to perform an audit of smart contracts:
https://bscscan.com/address/0x385ca01bbc634a984c46d71031b35b581f16f57b#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 24.02.2022

Contract name	CateDogeInuSafeElonMoonMars
Contract address	0x385ca01bbC634A984C46D71031B35b581f16F57b
Total supply	1,000,000,000,000,000
Token ticker	CDISEMM
Decimals	9
Token holders	141
Transactions count	293
Top 100 holders dominance	99.63%
Liquidity fee	7
Tax fee	1
Total fees	2325541578673608040408
Uniswap V2 pair	0x37e47a0e916931773b20c9761738aa441fe20bd3
Contract deployer address	0x5864ce873e3742b9abb90fa3cb8a8ac9e22dec9a
Contract's current owner address	0x0000000000000000000000000000000000000000

CateDogeInuSafeElonMoonMars Token Distribution

CateDogeInuSafeElonMoonMars Top 100 Token Holders
Source: BscScan.com

0x006740ab1c5e30957927854663d7c7fa983604fd
0x7fd04e77a3087ab69760599f42f8eaf42449c9c7
0x87dce9be4c75bc9f9fb4e3f27912fef567743b15
0x7d7e5118d73c1e197e5f28cff0f608d5bb6fa2c1
0x0425d695ac8e6a6790d25164504af6abe6b1a89c
0x253590071b3c2ba52b8e681a2a1d0e295ddc3d9a
0x5864ce873e3742b9abb90fa3cb8a8ac9e22dec9a
0xa59716b6ca19a8146bc761d6fa680e2eee0c9cc5

0x0000000000000000000000000000000000000dead
(Null Address: 0x000...dEaD)

0x37e47a0e916931773b20c9761738aa441fe20bd3
(PancakeSwap V2: CDISEMM)

(A total of 996,310,604,650,133.00 tokens held by the top 100 accounts from the total supply of 1,000,000,000,000,000.00 token)

CateDogeInuSafeElonMoonMars Contract Interaction Details

Time Series: Token Contract Overview

Sun 13, Feb 2022 - Wed 23, Feb 2022

Token Contract 0x385ca01bbc634a984c46d71031b35b581f16f57b (CateDogeInuSafeElonMoonMars)
Source: BscScan.com

Zoom 1m 6m 1y **All**

From Feb 12, 2022 To Feb 23, 2022

● Transfer Amount   -●- Transfers Count   -●- Unique Receivers   -■- Unique Senders   -▲- Total Uniques

CateDogeInuSafeElonMoonMars Top 10 Token Holders

Rank	Address	Quantity (Token)	Percentage
1	Null Address: 0x000...dEaD	500,000,000,000,000	50.0000%
2	PancakeSwap V2: CDISEMM	275,054,035,280,491.762493967	27.5054%
3	0xa59716b6ca19a8146bc761d6fa680e2eee0c9cc5	25,000,000,000,000	2.5000%
4	0x5864ce873e3742b9abb90fa3cb8a8ac9e22dec9a	25,000,000,000,000	2.5000%
5	0x253590071b3c2ba52b8e681a2a1d0e295ddc3d9a	12,880,910,720,526.861709921	1.2881%
6	0x0425d695ac8e6a6790d25164504af6abe6b1a89c	9,205,851,578,194.056979298	0.9206%
7	0x7d7e5118d73c1e197e5f28cff0f608d5bb6fa2c1	7,054,192,513,338.21072496	0.7054%
8	0x87dce9be4c75bc9f9fb4e3f27912fef567743b15	6,490,020,100,955.838427074	0.6490%
9	0x7fd04e77a3087ab69760599f42f8eaf42449c9c7	6,339,700,152,380.012996833	0.6340%
10	0x006740ab1c5e30957927854663d7c7fa983604fd	6,223,843,552,245.058560088	0.6224%

Contract functions details

+ Context
- [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)
- [Pub] <Constructor> #
- [Pub] owner
- [Pub] renounceOwnership #
  - modifiers: onlyOwner
- [Pub] transferOwnership #
  - modifiers: onlyOwner
- [Pub] geUnlockTime
- [Pub] lock #
  - modifiers: onlyOwner
- [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]** decimals
  - **[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]** 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 **#**

+ CDISEMM (Context, IERC20, Ownable)
- **[Pub]** <Constructor> **#**
- **[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 **#**
  - modifiers: onlyOwner
- **[Ext]** includeInReward **#**
  - modifiers: onlyOwner
- **[Prv]** _transferBothExcluded **#**
- **[Ext]** <Fallback> **($)**
- **[Prv]** _reflectFee **#**
- **[Prv]** _getValues
- **[Prv]** _getTValues
- **[Prv]** _getRValues
- **[Prv]** _getRate
- **[Prv]** _getCurrentSupply
- **[Prv]** _takeLiquidity **#**
- **[Prv]** calculateLiquidityFee
- **[Prv]** calculateTaxFee
- **[Prv]** removeAllFee **#**
- **[Prv]** restoreAllFee **#**
- **[Pub]** isExcludedFromFee
- **[Prv]** _approve **#**
- **[Prv]** _transfer **#**
- **[Prv]** swapAndLiquify **#**
  - modifiers: lockTheSwap
- **[Prv]** swapTokensForEth **#**
- **[Prv]** addLiquidity **#**
- **[Prv]** _tokenTransfer **#**
- **[Prv]** _transferStandard **#**
- **[Prv]** _transferToExcluded **#**
- **[Prv]** _transferFromExcluded **#**
- **[Pub]** excludeFromFee **#**
  - modifiers: onlyOwner
- **[Pub]** includeInFee **#**
  - modifiers: onlyOwner
- **[Prv]** setAllFees **#**
- **[Ext]** setFees **#**

- modifiers: onlyOwner
- **[Ext]** setSaleFees **#**
  - modifiers: onlyOwner
- **[Ext]** setMinimumTokensBeforeSwap **#**
  - modifiers: onlyOwner
- **[Ext]** setMaxBuyTxAmount **#**
  - modifiers: onlyOwner
- **[Ext]** setMaxSellTxAmount **#**
  - modifiers: onlyOwner
- **[Pub]** setSwapAndLiquifyEnabled **#**
  - 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.	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.	Low issues
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 includeInReward() uses the loop to find and remove addresses from the _excluded list. Function will be aborted with OUT_OF_GAS exception if there will be a long excluded addresses list.

- The function _getCurrentSupply also uses the loop for evaluating total supply. It also could be aborted with OUT_OF_GAS exception if there will be a long excluded addresses list.

Recommendation:
Check that the excluded array length is not too big.

2. Rounding error

Issue:

- At some calculation with division, it is goes first. In Solidity we don't have floating points, but instead we get rounding errors.

Recommendation:
Do division after multiplication.

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

- Owner can change fees.
- Owner can change the maximum buy/sell transaction amounts.
- Owner can exclude from the fee.
- Owner can change minimumTokensBeforeSwap.
- Owner can enable/disable swapAndLiquify.
- Owner can lock and unlock. By the way, using these functions the owner could retake privileges even after the ownership was renounced.

Conclusion

Smart contracts contain low severity issues! Liquidity pair contract's security is not checked due to out of scope.

Liquidity locking details are provided by the team: https://bscscan.com/tx/0xf3d560f0de81e2ed7b0eeafc71f68b276b03b97b 4b8c2d45c16e6f0319b6a99b

Ownership renounce details are provided by the team: https://bscscan.com/tx/0x5e4cc1ee55ee4ad1d99ee9825e507a6f9c0df7d 4d1f0377c8b9d0893fd5ca143

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.