TECH RATE

SMART CONTRACTS SECURITY

AUDIT REPORT

Techrate_audits   Techrate   Techrate1

Audit Details

Audited project

The Commission

Deployer address

0x5b169a812a2fcc8288d5948f02717719c1bf9730

Client contacts:

The Commission team

Blockchain

Ethereum

Project website:

https://thecommission.xyz

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 The Commission to perform an audit of smart contracts:
https://etherscan.io/address/0xaeb813653bb20d5fa4798dc4fc63af9cad4f3f67#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.

TECH
RATE

Contracts Details

Token contract details for 17.03.2022

|	
Contract name	The Commission
Contract address	0xaeB813653bb20d5Fa4798dc4fc63Af9cad4f3f67
Total supply	1,000,000,000
Token ticker	CMSN
Decimals	18
Token holders	1,638
Transactions count	18,148
Top 100 holders dominance	77.61%
Sell total fees	9
Buy total fees	7
Trading active	true
Uniswap V2 pair	0x92b5123b675033914888d201ad348d1713304957
Contract deployer address	0x5b169a812a2fcc8288d5948f02717719c1bf9730
Owner address	0x0000000000000000000000000000000000000000

The Commission Token Distribution

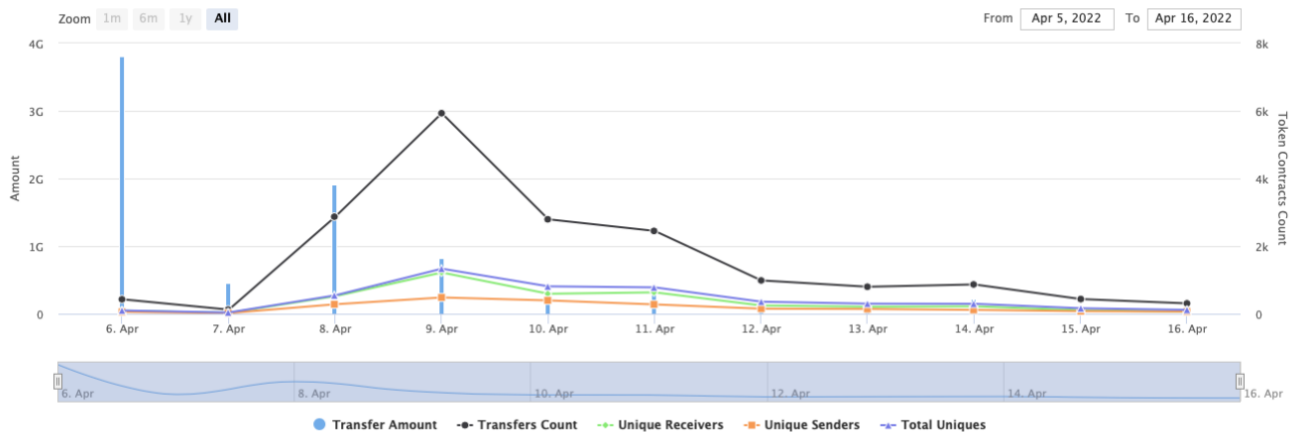The Commission Top 100 Token Holders
Source: Etherscan.io
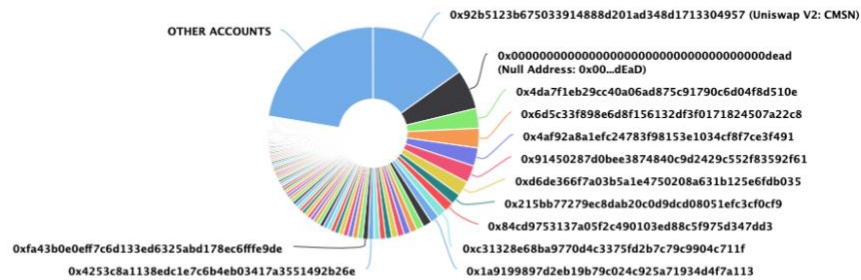
(A total of 776,078,532.57 tokens held by the top 100 accounts from the total supply of 1,000,000,000.00 token)

The Commission Contract Interaction Details

Time Series: Token Contract Overview

Wed 6, Apr 2022 - Sat 16, Apr 2022

Token Contract 0xaeb813653bb20d5fa4798dc4fc63af9cad4f3f67 (The Commission)
Source: Etherscan.io

TECH
RATE

The Commission Top 10 Token Holders

Rank	Address	Quantity (Token)	Percentage
1	🖹 Uniswap V2: CMSN	151,798,430.122457101778595072	15.1798%
2	Null Address: 0x00...dEaD	60,680,232.452419948079257859	6.0680%
3	0x4da7f1eb29cc40a06ad875c91790c6d04f8d510e	30,200,000	3.0200%
4	0x6d5c33f898e6d8f156132df3f0171824507a22c8	29,800,000	2.9800%
5	0x4af92a8a1efc24783f98153e1034cf8f7ce3f491	27,850,000	2.7850%
6	0x91450287d0bee3874840c9d2429c552f83592f61	26,000,000	2.6000%
7	0xd6de366f7a03b5a1e4750208a631b125e6fdb035	22,538,791.1412512160370 88177	2.2539%
8	0x215bb77279ec8dab20c0d9dcd08051efc3cf0cf9	16,325,841.588708088712862194	1.6326%
9	0x84cd9753137a05f2c490103ed88c5f975d347dd3	15,008,059.509623919835080244	1.5008%
10	0xc31328e68ba9770d4c3375fd2b7c79c9904c711f	13,731,310.58050720753116936	1.3731%

Contract functions details

+ **[Int]** IUniswapV2Factory
    - **[Ext]** createPair #

+ **[Int]** IUniswapV2Router01
    - **[Ext]** factory
    - **[Ext]** WETH
    - **[Ext]** addLiquidityETH ($)

+ **[Int]** IUniswapV2Router02 (IUniswapV2Router01)
    - **[Ext]** swapExactTokensForETHSupportingFeeOnTransferTokens #

+ **[Int]** IUniswapV2Pair
    - **[Ext]** sync #

+ Context
    - [Int] _msgSender
    - [Int] _msgData

+ Ownable (Context)
    - **[Pub]** <Constructor> #
    - **[Pub]** owner
    - **[Pub]** renounceOwnership #
        - modifiers: onlyOwner
    - **[Pub]** transferOwnership #
        - modifiers: onlyOwner
    - [Int] _transferOwnership #

+ **[Int]** IERC20
    - **[Ext]** totalSupply
    - **[Ext]** balanceOf
    - **[Ext]** transfer #
    - **[Ext]** allowance
    - **[Ext]** approve #
    - **[Ext]** transferFrom #

+ **[Int]** IERC20Metadata (IERC20)
    - **[Ext]** name
    - **[Ext]** symbol
    - **[Ext]** decimals

+ ERC20 (Context, IERC20, IERC20Metadata)

- [Pub] <Constructor> #
- [Pub] name
- [Pub] symbol
- [Pub] decimals
- [Pub] totalSupply
- [Pub] balanceOf
- [Pub] transfer #
- [Pub] allowance
- [Pub] approve #
- [Pub] transferFrom #
- [Pub] increaseAllowance #
- [Pub] decreaseAllowance #
- [Int] _transfer #
- [Int] _mint #
- [Int] _burn #
- [Int] _approve #
- [Int] _beforeTokenTransfer #
- [Int] _afterTokenTransfer #

+ [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

+ TheCommission (ERC20, Ownable)
- [Pub] <Constructor> #
   - modifiers: ERC20
- [Ext] <Fallback> ($)
- [Ext] startTrading #
   - modifiers: onlyOwner
- [Ext] removeLimits #
   - modifiers: onlyOwner
- [Ext] disableTransferDelay #
   - modifiers: onlyOwner
- [Ext] updateSwapTokensAtAmount #

- modifiers: onlyOwner
- **[Ext]** updateMaxTxnAmount #
  - modifiers: onlyOwner
- **[Ext]** updateMaxWalletAmount #
  - modifiers: onlyOwner
- **[Pub]** excludeFromMaxTransaction #
  - modifiers: onlyOwner
- **[Ext]** updateSwapEnabled #
  - modifiers: onlyOwner
- **[Pub]** excludeFromFees #
  - modifiers: onlyOwner
- **[Pub]** setAutomatedMarketMakerPair #
  - modifiers: onlyOwner
- **[Prv]** _setAutomatedMarketMakerPair #
- **[Ext]** updateMarketingWallet #
  - modifiers: onlyOwner
- **[Ext]** updateDevWallet #
  - modifiers: onlyOwner
- **[Pub]** isExcludedFromFees
- [Int] _transfer #
- **[Prv]** swapTokensForEth #
- **[Prv]** addLiquidity #
- **[Prv]** swapBack #
- **[Ext]** setAutoLPBurnSettings #
  - modifiers: onlyOwner
- [Int] autoBurnLiquidityPairTokens #
- **[Ext]** manualBurnLiquidityPairTokens #
  - 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

TECH
RATE

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:

- There is sending tokens to dead address instead of really burning (decreasing total supply).

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

- Owner can start trading.
- Owner can remove limits and disable transferDelayEnabled.
- Owner can change swapTokensAtAmount, maxTransactionAmount and maxWallet.
- Owner can exclude from max transaction amount.
- Owner can enable/disable swapEnabled.
- Owner can exclude from the fees.
- Owner can include in automated market pair array.
- Owner can change marketing and dev wallets.
- Owner can change auto burn settings.
- Owner can manually burn tokens.

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://app.unicrypt.network/amm/uni-v2/pair/0x92b5123b675033914888d201ad348d1713304957

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.