HackSafe

Smart Contract Security Audit Report

MEO.TOOLS

March 2023

Security Status

★★★⯪☆

www.hacksafe.io

Audit Details

Audited project
MEO.TOOLS

Deployer address
0xdac833a4fbb2f7173c498646981774547c17d43a

Client contacts
MEO.TOOLS Team

Blockchain
Binance smart chain

Website
Not Provided

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) (HackSafe) owe no duty of care towards you or any other person, nor does HackSafe 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 HackSafe 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, HackSafe hereby excludes all liability and responsibility, and neither you nor any other person shall have any claim against HackSafe, 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.

Procedure

Step 1 - In-Depth Manual Review

Manual line-by-line code reviews to ensure the logic behind each function is sound and safe from various attack vectors. This is the most important and lengthy portion of the audit process (as automated tools often cannot find the nuances that lead to exploits such as flash loan attacks).

Step 2 - Automated Testing

Simulation of a variety of interactions with your Smart Contract on a test blockchain leveraging a combination of automated test tools and manual testing to determine if any security vulnerabilities exist.

Step 3 – Leadership Review

The engineers assigned to the audit will schedule meetings with our leadership team to review the contracts, any comments or findings, and ask questions to further apply adversarial thinking to discuss less common attack vectors.

Step 4 - Resolution of Issues

Consulting with the team to provide our recommendations to ensure the code's security and optimize its gas efficiency, if possible. We assist project team's in resolving any outstanding issues or implementing our recommendations.

Step 5 - Published Audit Report

Boiling down results and findings into an easy-to-read report tailored to the project. Our audit reports highlight resolved issues and any risks that exist to the project or its users, along with any remaining suggested remediation measures. Diagrams are included at the end of each report to help users understand the interactions which occur within the project.

Background

HackSafe was commissioned by MEO.TOOLS to perform an audit of smart contracts:

- https://bscscan.com/token/0x37C4A3a9ACFaa4BBe543DCB0D6CE4b2443B3b0D7#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 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

Token contract details for 13.03.2023

Token Type	: DEFI
Contract name	: MEO
Contract address	: 0x37C4A3a9ACFaa4BBe543DCB0D6CE4b2443B3b0D7
Total supply	: 1,000,000,000
Token ticker	: MEO
Decimals	: 9
Token Holders	: 30
Transactions count	: 101
Compiler version	: v0.7.6+commit.7338295f
Contract deployer address	: 0xdac833a4fbb2f7173c4986469817745 47c17d43a
owner address	: 0xdac833a4fbb2f7173c4986469817745 47c17d43a

Audit Summary

According to the standard audit assessment, Customer`s solidity smart contracts are **“Poor Secure”.** This token contract does contain owner control, which do not make it fully decentralized.

Insecure	Poor secured	Secure	Well-secured

You are here 

We used various tools like Slither, Mythril and Remix IDE. At the same time this finding is based on critical analysis of the manual audit. All issues found during automated analysis were manually reviewed and applicable vulnerabilities are presented in the issues checking status.

We found 0 critical, 0 high, 2 medium and 0 low.

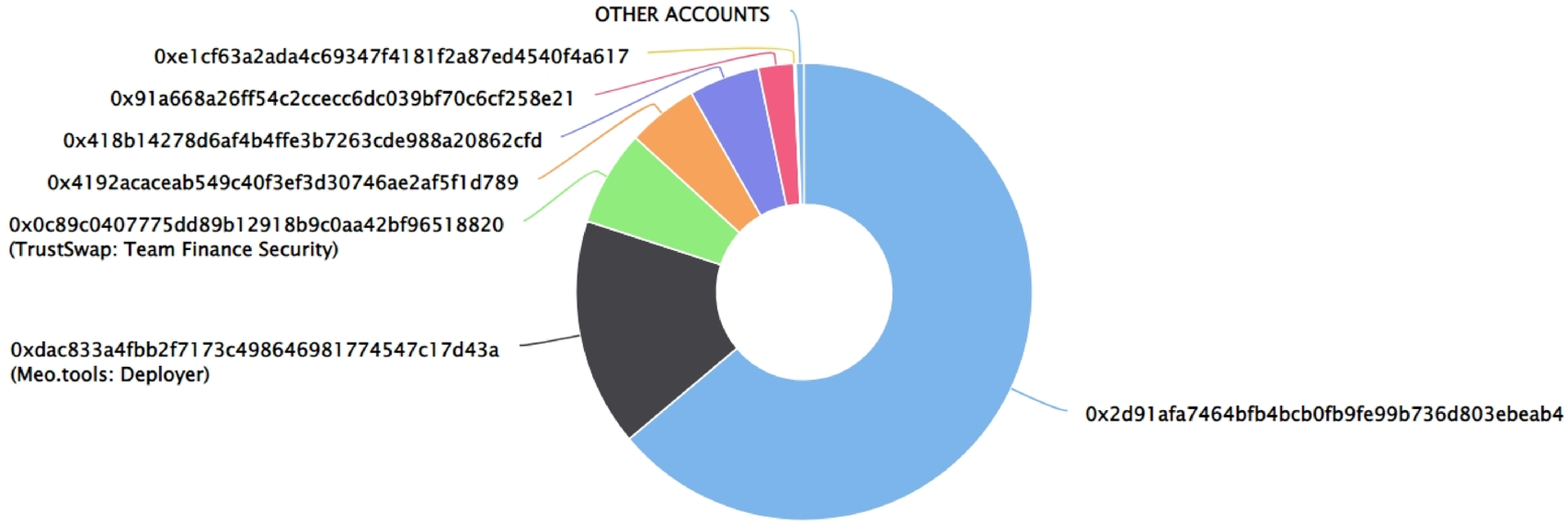
MEO.TOOLS TOKEN Distribution

The top 100 holders collectively own 99.43% (994,287,088.94 Tokens) of Meo.tools

Token Total Supply: 1,000,000,000.00 Token | Total Token Holders: 30

Meo.tools Top 100 Token Holders

Source: BscScan.com



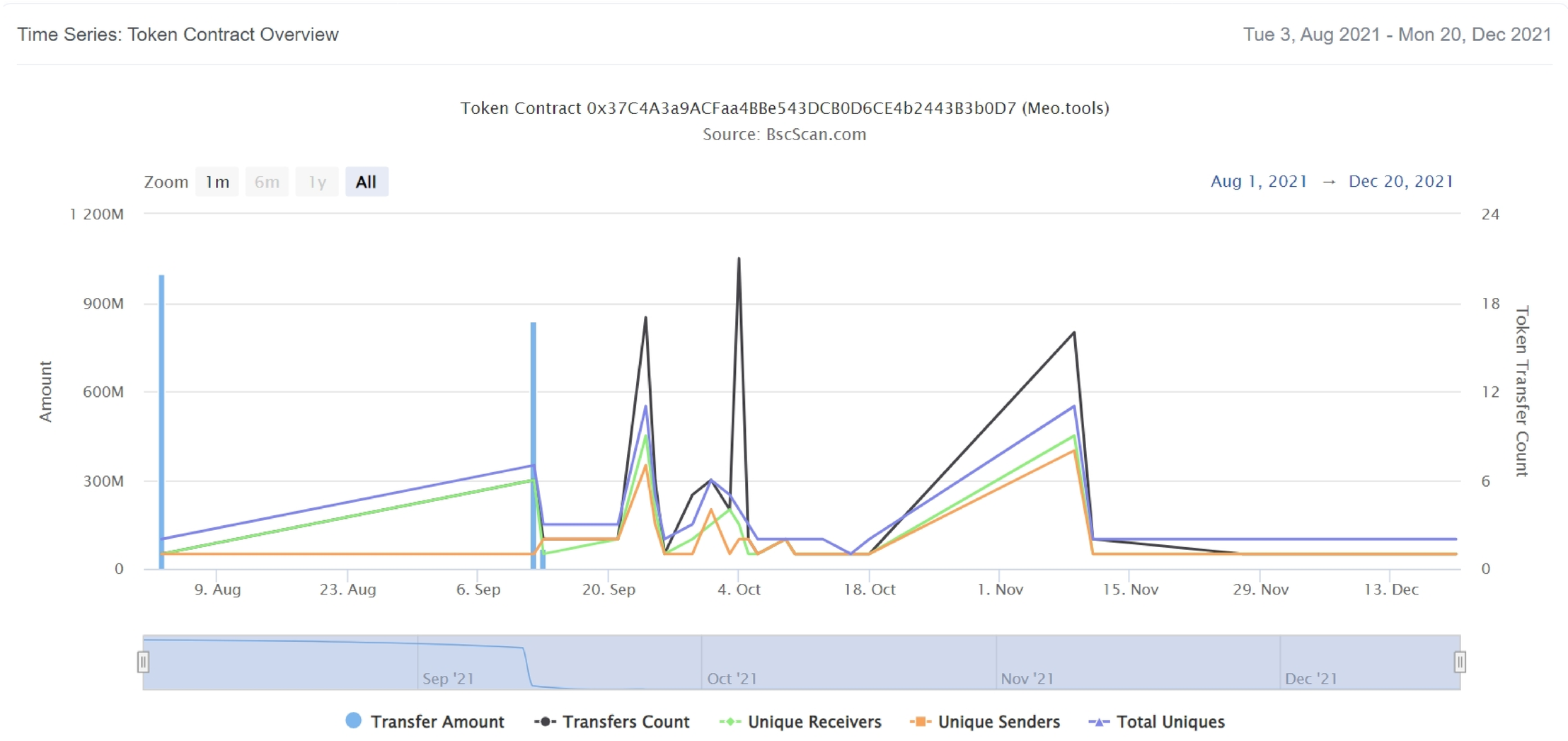
MEO.TOOLS Top 20 Token Holders

(A total of 994,287,088.94 tokens held by the top 100 accounts from the total supply of 1,000,000,000.00 token)

Rank	Address	Quantity (Token)	Percentage
1	0x2d91afa7464bfb4bcb0fb9fe99b736d803ebeab4	638,928,000	63.8928%
2	Meo.tools: Deployer	161,271,554.105218989	16.1272%
3	TrustSwap: Team Finance Security	67,578,834.462276183	6.7579%
4	0x4192acaceab549c40f3ef3d30746ae2af5f1d789	50,000,000	5.0000%
5	0x418b14278d6af4b4ffe3b7263cde988a20862cfd	50,000,000	5.0000%
6	0x91a668a26ff54c2ccecc6dc039bf70c6cf258e21	25,000,000	2.5000%
7	0xe1cf63a2ada4c69347f4181f2a87ed4540f4a617	269,931.99875105	0.0270%
8	0x37c4a3a9acfaa4bbe543dcb0d6ce4b2443b3b0d7	253,438.019698955	0.0253%
9	PancakeSwap V2: MEO 6	253,301.528284406	0.0253%
10	0x9d4e58611ba4e224653c2d5a309c11ba3b73c0e8	185,352.776313937	0.0185%
11	0x89975f860373f38daede54db04441f558b516e8a	145,351.679499542	0.0145%
12	0xfb2caa5f9660636dbc33bd5cc0b44f91d0962619	84,800.167375577	0.0085%
13	0xd265a93eaa8291b39285cd4a9ba892f60db596e8	72,684.176099221	0.0073%
14	0xccfd76b73528ead16af9c7536a4559a677876e3e	63,000.088200123	0.0063%
15	0xc248b0cfd00ff66a03f81ba39144607a253a6127	61,289.135856756	0.0061%
16	0xb96b88235ae2ef667b4fe5287b8d23402a6d95cf	46,920.124547696	0.0047%
17	0x7bf5060bfe5bb4ddcfd4b8a65b85656a9407aefb	25,037.543796923	0.0025%
18	0xbedac0bfc8bc247ee05bbfa255c501de1f50bf91	24,010.569135353	0.0024%
19	0xb561228a1221956affad13f5c05c34a4aee67ff3	9,000.0027	0.0009%
20	0x00b91425a031ae1358b70f3fb1272b6c318a6291	9,000.0018	0.0009%

MEO.TOOLS TOKEN Distribution

MEO.TOOLS Contract Overview



Contract functions details

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

+[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

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

+[Lib] Address
    -[Int] isContract
    -[Int] sendValue #
    -[Int] functionCall #
    -[Int] functionCall #
    -[Int] functionCallWithValue #
    -[Int] functionCallWithValue #
    -[Int] functionStaticCall
    -[Int] functionStaticCall
    -[Int] functionDelegateCall #
    -[Int] functionDelegateCall #
    -[Pvt] _verifyCallResult

Contract functions details

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

+[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 #

+[Int] IUniswapV2Factory
  -[Ext] feeTo
  -[Ext] feeToSetter
  -[Ext] getPair
  -[Ext] allPairs

Contract functions details

-[Ext] allPairsLength
-[Ext] createPair #
-[Ext] setFeeTo #
-[Ext] setFeeToSetter #

+MEO (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] reflectionFromToken
-[Pub] tokenFromReflection
-[Pub] excludeFromRFI #
- modifiers: onlyOwner
-[Ext] includeInRFI #
- modifiers: onlyOwner
-[Pub] excludeFromFeeAndRfi #
- modifiers: onlyOwner
-[Pub] excludeFromFee #
- modifiers: onlyOwner
-[Pub] includeInFee #
- modifiers: onlyOwner
-[Pub] isExcludedFromFee
-[Pub] setRfiRatesPercents #
- modifiers: onlyOwner
-[Pub] setWallets #
- modifiers: onlyOwner
-[Pub] setPresaleWallet #
- modifiers: onlyOwner

Contract functions details

-[Ext] setMaxTxPercent #
  - modifiers: onlyOwner
-[Ext] setMaxTxAmount #
  - modifiers: onlyOwner
-[Ext] setThreshholdForLP #
  - modifiers: onlyOwner
-[Pub] setSwapAndLiquifyEnabled #
  - modifiers: onlyOwner
-[Ext] <Fallback>($)
-[Pvt] _reflectRfi #
-[Pvt] _getValues
-[Pvt] _getTValues
-[Pvt] _getRValues
-[Pvt] _getRate
-[Pvt] _getCurrentSupply
-[Pvt] _takeLiquidity #
-[Pvt] _approve #
-[Pvt] _transfer #
-[Pvt] _tokenTransfer #
-[Pvt] reflectDevandResearchFee #
-[Pvt] swapAndLiquify #
  - modifiers: lockTheSwap
-[Pvt] swapTokensForBNB #
-[Pvt] addLiquidity #
-[Pub] totalDevelopmentFee
-[Pub] totalResearchFee

($) = payable function
= non-constant function

Issues Checking Status

No.	Title	Status
1.	Unlocked Compiler Version	Passed
2.	Missing Input Validation	Passed
3.	Race conditions and Reentrancy. Cross-function race conditions.	Passed
4.	Possible delays in data delivery	Passed
5.	Oracle calls.	Passed
6.	Timestamp dependence.	Passed
7.	Integer Overflow and Underflow	Passed
8.	DoS with Revert.	Passed
9.	DoS with block gas limit.	Medium Issue
10.	Methods execution permissions.	Passed
11.	Economy model of the contract.	Medium issue
12.	Private use data leaks.	Passed
13.	Malicious Event log.	Passed
14.	Scoping and Declarations.	Passed
15.	Uninitialized storage pointers.	Passed
16.	Arithmetic accuracy.	Passed
17.	Design Logic.	Passed
18.	Safe Open Zeppelin contracts implementation and usage.	Passed
19.	Incorrect Naming State Variable	Passed
20.	Too old version	Passed

Severity Definitions

Risk Level	Description
Critical	Critical vulnerabilities are usually straightforward to exploit and can lead to assets loss or data manipulations.
High	High-level vulnerabilities are difficult to exploit; however, they also have a significant impact on smart contract execution, e.g., public access to crucial functions
Medium	Medium-level vulnerabilities are important to fix; however, they can't lead to assets loss or data manipulations.
Low	Low-level vulnerabilities are mostly related to outdated, unused, etc. code snippets that can't have a significant impact on execution.

Security Issues

Critical Severity Issues

No critical severity issue found.

High Severity Issues

No high severity issue found.

Medium Severity Issues

Two medium severity issue found.

1. Out of gas

- **Issue:**

  The function includeInRFI() 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. Wrong reflectDevandResearchFee taking

- **Issue:**

  The function reflectDevandResearchFee() do not check dev and research addresses to be excluded from reward and do not increase _tOwned balance of this addresses if needed. If them would be it will be a high issue.

- **Recommendation**

  Check dev and research addresses to be excluded and increase addresses' _tOwned balance if needed

Low Severity Issues

No low severity issue found.

Centralization

Owner Privileges :

- MEO.TOOLS Contract:
    - Owner can change presale wallet.
    - Owner can change minimum number of tokens to add to liquidity.
    - Owner can exclude from fee and rfi.
    - Owner can change fee rates.
    - Owner can change research and dev wallets.
    - Owner can change the maximum transaction amount.
    - Owner can exclude from the fee.

This smart contract has some functions which can be executed by the admin (Owner) only. If the admin wallet private key would be compromised, then it would create trouble as smart contract ownership has not been renounced.

Conclusion

Smart contract contains medium severity issues! The further transfer and operations with the fund raised are not related to this particular contract.

HackSafe 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.