HackSafe

Smart Contract Security Audit Report

PEPE COIN

February 2023

Security Status

★★★★☆

www.hacksafe.io

Audit Details

Audited project
PEPE COIN

Deployer address
0xd778875dcb2c2313d243270b42177d521a6897df

Client contacts
PEPE COIN 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 PEPE COIN to perform an audit of smart contracts:

- https://bscscan.com/token/0xFf593Cb838547700C565024C42ce9A2a24511b01#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 15.02.2023

Token Type	: DEFI
Contract name	: $PePe
Contract address	: 0xFf593Cb838547700C565024C42ce9A2a24511b01
Total supply	: 1,000,000,000,000
Token ticker	: $PePe
Decimals	: 18
Token Holders	: 1,336
Transactions count	: 3,035
Compiler version	: v0.8.4+commit.c7e474f2
Contract deployer address	: 0xd778875dcb2c2313d243270b42177d521a6897df
Owner address	: 0xf1872b9ab82a571ccbb69def5dc64922804c8df8

Audit Summary

According to the standard audit assessment, Customer`s solidity smart contracts are **“Secure”.** This token contract does contain owner control as ownership has not been renounced, 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, 1 medium and 0 low.

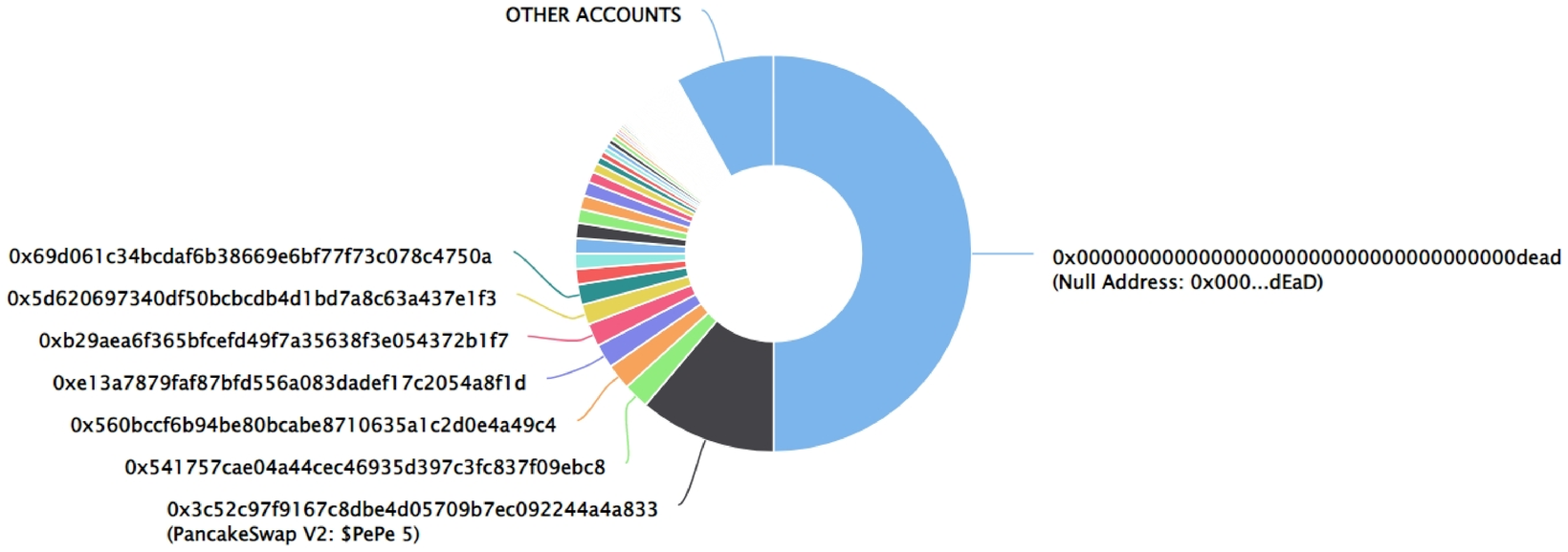
PEPE COIN Token Distribution

The top 100 holders collectively own 91.94% (919,429,657,752.59 Tokens) of $PePe Coin

Token Total Supply: 1,000,000,000,000.00 Token | Total Token Holders: 1,336

$PePe Coin Top 100 Token Holders

Source: BscScan.com



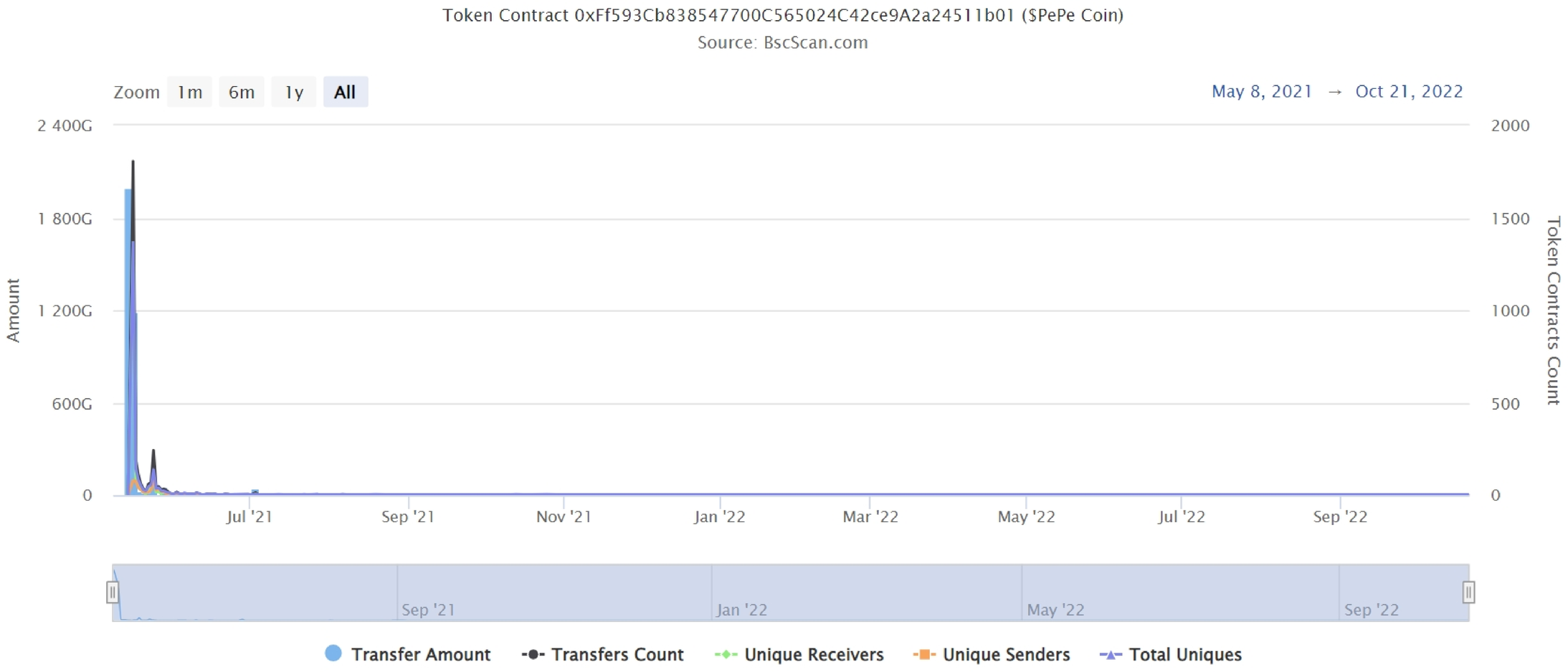
PEPE COIN TOKEN Top 20 Token Holders

(A total of 919,429,657,752.59 tokens held by the top 100 accounts from the total supply of 1,000,000,000,000.00 token)

Rank	Address	Quantity (Token)	Percentage
1	Null Address: 0x000...dEaD	500,000,000,000	50.0000%
2	PancakeSwap V2: $PePe 5	111,870,769,380.373216956897154357	11.1871%
3	0x541757cae04a44cec46935d397c3fc837f09ebc8	21,043,771,043	2.1044%
4	0x560bccf6b94be80bcabe8710635a1c2d0e4a49c4	20,622,895,624	2.0623%
5	0xe13a7879faf87bfd556a083dadef17c2054a8f1d	19,833,754,206	1.9834%
6	0xb29aea6f365bfcefd49f7a35638f3e054372b1f7	18,560,359,589.147807916810572248	1.8560%
7	0x5d620697340df50bcbcdb4d1bd7a8c63a437e1f3	16,519,360,629	1.6519%
8	0x69d061c34bcdaf6b38669e6bf77f73c078c4750a	16,462,771,375.909651323268884188	1.6463%
9	0x6207fc22be4e8b78d18e088a3f449c792836f0c2	12,784,090,909	1.2784%
10	0x0016fb762795334a64d77452ffc4f29872b0fbc1	12,633,179,470	1.2633%
11	0xf9fff407349b69ea5d2b913cc4f3049e161527af	12,290,896,498.116940142498380888	1.2291%
12	0xe209bda7e51a2c0d44f0a7d9e62f104d71d31827	12,253,520,177.842591310047414067	1.2254%
13	0xc7fae3f5aa92b9afc82ce173063bae4c88751bfc	11,311,026,936	1.1311%
14	0xfff409b1586790bb3d9888a5f8bf0984ed6daaa3	11,311,026,936	1.1311%
15	0xff2ec3023c9d521caf1d3d9e05c42b3ef643808e	11,311,026,936	1.1311%
16	0x63506cb7b0c80419e1652ca3ecb9e480c51ebaad	8,819,539,853.424272868080606489	0.8820%
17	0xd93a63e709fe047e710191843634233b36266640	7,523,148,148	0.7523%
18	0x58bbf245fe03e5b2876ff30562d7c7f8807865f6	5,957,991,355	0.5958%
19	0x8b1184e9923d510322a71deb0d50c67e22ec929a	4,807,661,732.555207755938984302	0.4808%
20	0x0e1490d98bd5842a68ddf905c2725121bb73a430	3,937,420,157.823367540720147232	0.3937%

PEPE COIN Token Distribution

PEPE COIN 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] #
- [Pub] owner
- [Pub] renounceOwnership #
  - modifiers: onlyOwner
- [Pub] transferOwnership #
  - modifiers: onlyOwner
- [Pub] geUnlockTime
- [Pub] lock #
  - modifiers: onlyOwner
- [Pub] unlock #

+[Int] IPancakeSwapV2Factory
- [Ext] feeTo
- [Ext] feeToSetter
- [Ext] getPair
- [Ext] allPairs
- [Ext] allPairsLength
- [Ext] createPair #
- [Ext] setFeeTo #
- [Ext] setFeeToSetter #

+[Int] IPancakeSwapV2Pair
- [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

Contract functions details

- [Ext] getReserves
- [Ext] price0CumulativeLast
- [Ext] price1CumulativeLast
- [Ext] kLast
- [Ext] mint #
- [Ext] burn #
- [Ext] swap #
- [Ext] skim #
- [Ext] sync #
- [Ext] initialize #

+[Int] IPancakeSwapV2Router01
- [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] IPancakeSwapV2Router02 (IPancakeSwapV2Router01)
- [Ext] removeLiquidityETHSupportingFeeOnTransferTokens #
- [Ext] removeLiquidityETHWithPermitSupportingFeeOnTransferTokens #
- [Ext] swapExactTokensForTokensSupportingFeeOnTransferTokens #
- [Ext] swapExactETHForTokensSupportingFeeOnTransferTokens ($)
- [Ext] swapExactTokensForETHSupportingFeeOnTransferTokens #

Contract functions details

+$PePe (Context, IBEP20, Ownable)
  - [Pub] #
  - [Pub] name
  - [Pub] symbol
  - [Pub] decimals
  - [Pub] totalSupply
  - [Pub] balanceOf
  - [Pub] transfer #
  - [Pub] allowance
  - [Pub] approve #
  - [Pub] transferFrom #
  - [Pub] increaseAllowance #
  - [Pub] decreaseAllowance #
  - [Pub] isExcludedFromReward
  - [Pub] totalFees
  - [Pub] deliver #
  - [Pub] reflectionFromToken
  - [Pub] tokenFromReflection
  - [Pub] excludeFromReward #
    - modifiers: onlyOwner
  - [Ext] includeInReward #
    - modifiers: onlyOwner
  - [Pub] excludeFromFee #
    - modifiers: onlyOwner
  - [Pub] includeInFee #
    - modifiers: onlyOwner
  - [Ext] setTaxFeePercent #
    - modifiers: onlyOwner
  - [Ext] setMarketingFeePercent #
    - modifiers: onlyOwner
  - [Ext] setLiquidityFeePercent #
    - modifiers: onlyOwner
  - [Ext] setMaxTxPercent #
    - modifiers: onlyOwner
  - [Pub] setSwapAndLiquifyEnabled #
    - modifiers: onlyOwner
  - [Ext] ($)
  - [Pvt] _reflectFee #

Contract functions details

- [Pvt] _getValues
- [Pvt] _getTValues
- [Pvt] _getRValues
- [Pvt] _getRate
- [Pvt] _getCurrentSupply
- [Pvt] _takeLiquidity #
- [Pvt] _takeMarketing #
- [Pvt] calculateTaxFee
- [Pvt] calculateMarketingFee
- [Pvt] calculateLiquidityFee
- [Pvt] removeAllFee #
- [Pvt] restoreAllFee #
- [Pub] isExcludedFromFee
- [Pvt] _approve #
- [Pvt] _transfer #
- [Pvt] swapAndLiquify #
  - modifiers: lockTheSwap
  - [Pvt] swapTokensForEth #
  - [Pvt] addLiquidity #
  - [Pvt] _tokenTransfer #
  - [Pvt] _transferStandard #
  - [Pvt] _transferToExcluded #
  - [Pvt] _transferFromExcluded #
  - [Pvt] _transferBothExcluded #

($) = payable function
= non-constant function

Issues Checking Status

No.	Title	Status
1.	Compiler error	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.	Passed
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**
  One medium severity issue found.

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:**

  Use EnumerableSet instead of array or do not use long arrays.

- **Low Severity Issues**
  No low severity issue found.

Centralization

Owner Privileges

- PEPE Coin Contract:
    - Owner can change the tax, marketing and liquidity fee.
    - 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 Coined, 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.