HackSafe

Smart Contract Security Audit Report

SAPT

February 2023

Security Status

★★★★☆

www.hacksafe.io

Audit Details

Audited project
SAPT

Deployer address
0x528c57bc3f990821b38a94d004fff5246a67a50d

Client contacts
SAPT 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 SAPT to perform an audit of smart contracts:

- https://bscscan.com/token/0xD6eBB2286bD420F3fE586a163F92AEF044959330#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 14.02.2023

Token Type	: Utility
Contract name	: SAPT
Contract address	: 0xD6eBB2286bD420F3fE586a163F92AEF044959330
Total supply	: 1,000,000,000,000
Token ticker	: SAPT
Decimals	: 9
Token Holders	: 1,347
Transactions count	: 8,910
Compiler version	: v0.6.12+commit.27d51765
Contract deployer address	: 0x528c57bc3f990821b38a94d004fff5246a67a50d
Owner address	: 0x528c57bc3f990821b38a94d004fff5246a67a50d

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.

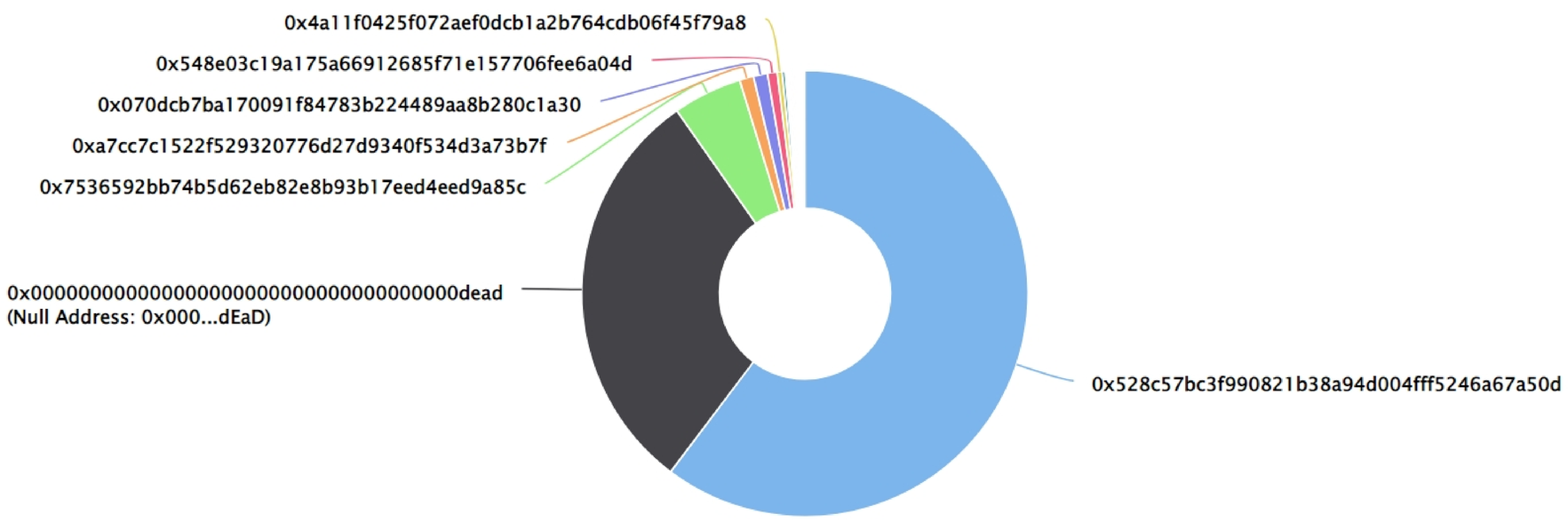
We found 0 critical, 0 high, 1 medium and 1 low.

SAPT Token Distribution

The top 100 holders collectively own 99.91% (999,097,511,625.31 Tokens) of SAPT | Token Total Supply: 1,000,000,000,000.00 Token | Total Token Holders: 1,347

SAPT Top 100 Token Holders

Source: BscScan.com



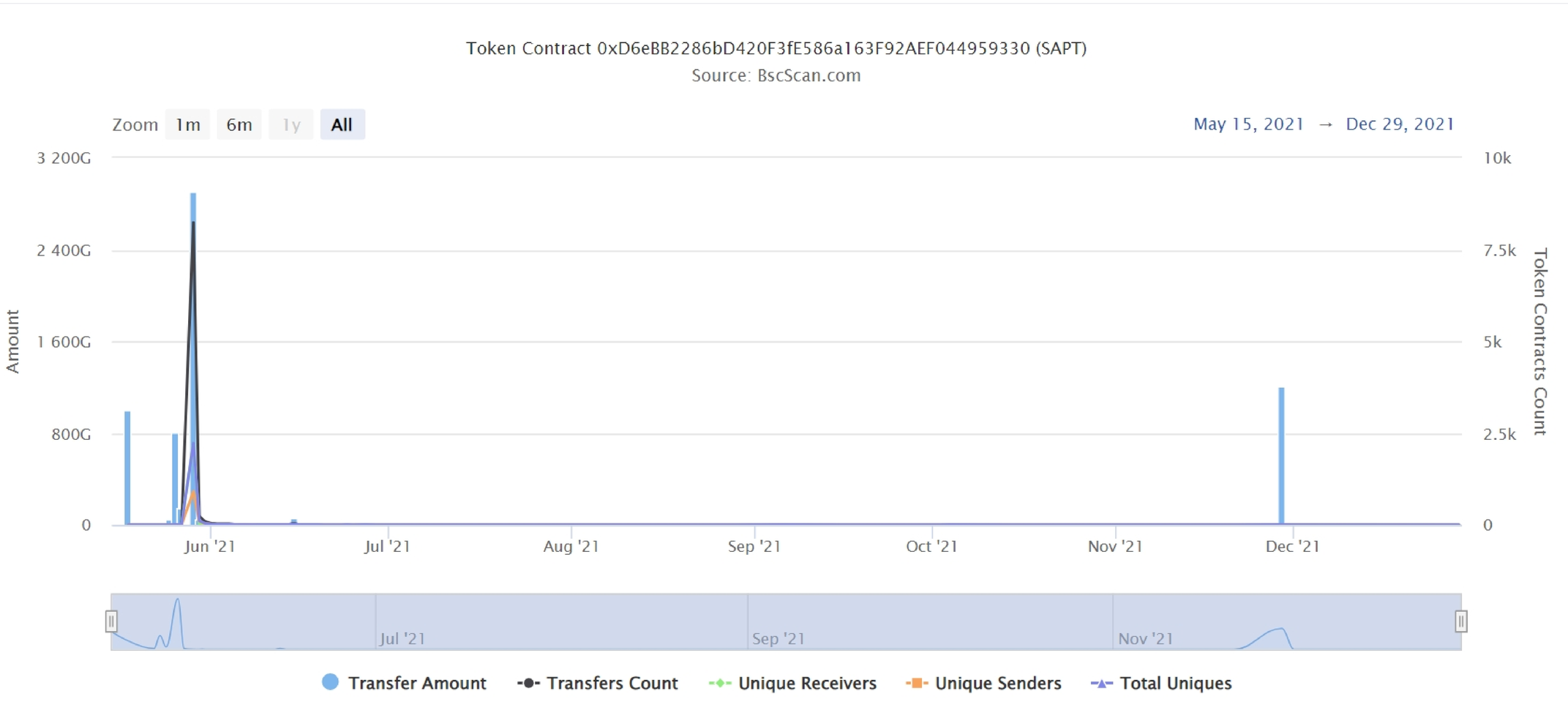
SAPT TOKEN Top 20 Token Holders

(A total of 999,097,511,625.31 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	0x528c57bc3f990821b38a94d004fff5246a67a50d	602,802,666,600.886835733	60.2803%
2	Null Address: 0x000...dEaD	300,008,345,070.297338099	30.0008%
3	0x7536592bb74b5d62eb82e8b93b17eed4eed9a85c	50,000,000,000	5.0000%
4	0xa7cc7c1522f529320776d27d9340f534d3a73b7f	10,270,893,102.226522238	1.0271%
5	0x070dcb7ba170091f84783b224489aa8b280c1a30	10,062,931,950.535648686	1.0063%
6	0x548e03c19a175a66912685f71e157706fee6a04d	6,999,705,999.999999997	0.7000%
7	0x4a11f0425f072aef0dcb1a2b764cdb06f45f79a8	3,499,300,000	0.3499%
8	PancakeSwap V2: SAPT	2,342,748,658.450674532	0.2343%
9	0x1504d03e079afcbf160038af4f19bb9103ec2ba5	1,237,508,398.008610315	0.1238%
10	0x1a46ba6de83f319ed9a29580a3f9e5ddbd15937c	1,013,065,456.184556736	0.1013%
11	0xa722218f046e6cb84d08ff8d43427351bd243d11	846,936,569.95241616	0.0847%
12	0x5efcf568efe583be0cb7e3ae72134ea2a5de78fe	751,274,250.775216877	0.0751%
13	0xb0792dacf15f612082e4a113d6c600c976987800	700,000,000	0.0700%
14	0x5cfa3acef2cfaea33396f1ff8e2068765f887833	660,606,609.648085256	0.0661%
15	0x48933d0e231d203c543830d715aaf1fa1f473e02	444,759,763.619089837	0.0445%
16	0x5d02aa514605a11a86f68e2b0367e1fd16441ad3	434,674,421.116979319	0.0435%
17	0xca4bcc12e96f83c727ddf78d233eda4bbe221dd9	365,026,329.907925638	0.0365%
18	0x7b7498fa40de9b307926fc11aca7eb449328023d	315,004,474.682856243	0.0315%
19	0xa0ebf4f41ba800a534883daeb0b661029986385c	288,356,716.439322372	0.0288%
20	0x4b703b61fd4c541e22a000f2ba94fd4b610b5d62	252,006,001	0.0252%

SAPT Token Distribution

SAPT Contract overview



Contract functions details

+[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

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

+[Lib] Address
    - [Int] isContract
    - [Int] sendValue #
    - [Int] functionCall #
    - [Int] functionCall #
    - [Int] functionCallWithValue #
    - [Int] functionCallWithValue #
    - [Pvt] _functionCallWithValue #

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

Contract functions details

- [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] mint #
- - [Ext] burn #
- - [Ext] swap #
- - [Ext] skim #

Contract functions details

- [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 #

+SAPT (Context, IERC20, Ownable)
- [Pub] <Constructor>#
- [Pub] name
- [Pub] symbol
- [Pub] decimals
- [Pub] totalSupply
- [Pub] balanceOf
- [Pub] transfer #
- [Pub] allowance

Contract functions details

- [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
- [Prt] _transferBothExcluded #
- [Pub] excludeFromFee #
  - modifiers: onlyOwner
- [Pub] includeInFee #
  - modifiers: onlyOwner
- [Ext] setTaxFeePercent #
  - modifiers: onlyOwner
- [Ext] setLiquidityFeePercent #
  - modifiers: onlyOwner
- [Ext] setMaxTxPercent #
  - modifiers: onlyOwner
- [Pub] setSwapAndLiquifyEnabled #
  - modifiers: onlyOwner
- [Ext] <Fallback >($)
- [Prv] _reflectFee #
- [Prv] _getValues
- [Prv] _getTValues
- [Prv] _getRValues
- [Prv] _getRate
- [Prv] _getCurrentSupply
- [Prv] _takeLiquidity #
- [Prv] calculateTaxFee
- [Prv] calculateLiquidityFee
- [Prv] removeAllFee #
- [Prv] restoreAllFee #

Contract functions details

- [Pub] isExcludedFromFee
- [Pvt] _approve #
- [Pvt] _transfer #
- [Pvt] swapAndLiquify #
  - modifiers: lockTheSwap
  - [Pvt] swapTokensForEth #
  - [Pvt] addLiquidity #
  - [Pvt] _tokenTransfer #
  - [Pvt] _transferStandard #
  - [Pvt] _transferToExcluded #
  - [Pvt] _transferFromExcluded #
  - [Pvt] _sendToCharity #

($) = 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	Low issue

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

One low severity issue found.

1. Old compiler version

- **Description**

  Contract has been deployed using too old solidity version.

- **Recommendation**

  It is advisable to deploy contract using any of the latest version of solidity.

- **Notes:**

  LP pair contract is not checked.

Centralization

Owner Privileges

- POGCOIN Coin Contract:
    - Owner can change the tax, charity and liquidity fee.
    - Owner can change the maximum transaction amount.
    - Owner can exclude from the fee.
    - Owner can lock and unlock. By the way, using these functions the owner could leave as owner even after the ownership was renounced.

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 low and 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.