Techrate1 Techrate

TechRate

AUDIT COMPANY

Smart Contract Security Audit

TechRate

August, 2021

Audit Details

Audited project

Rhythm

Deployer address

0xa5878853f75e812411cf863cf9b1f2604e597b6e

Client contacts:

Rhythm team

Blockchain

Binance Smart Chain

Project website:

https://rhythm.cash/

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 Rhythm to perform an audit of smart contracts:

https://bscscan.com/address/0xE4318F2aCf2b9c3f518A3a03B5412F4999970Ddb#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.

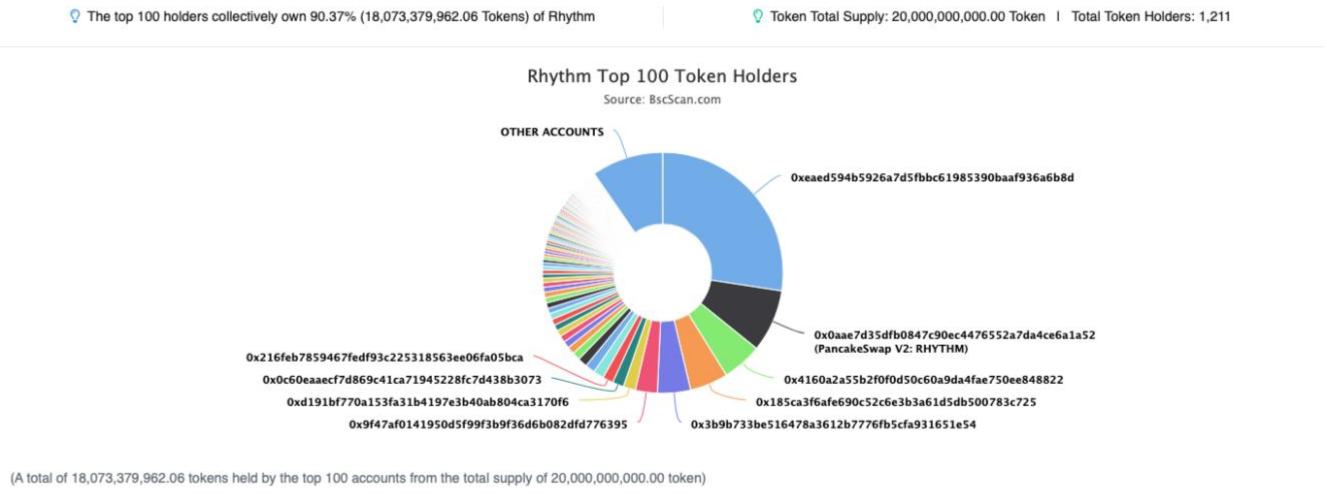
The information in this report should be used to understand the risk exposure of the smart contract, and as a guide to improve the security posture of the smart contract by remediating the issues that were identified.

Contracts Details

Token contract details for 18.07.2021

Contract name	Rhythm
Contract address	0xE4318F2aCf2b9c3f518A3a03B5412F4999970Ddb
Total supply	20,000,000,000
Token ticker	RHYTHM
Decimals	9
Token holders	1,211
Transactions count	4,732
Top 100 holders dominance	90.37%
Liquidity fee	5
Tax fee	3
Total fees	1874635823303608182
Pancake V2 pair	0x0aae7d35dfb0847c90ec4476552a7da4ce6a1a52
Contract deployer address	0xa5878853f75e812411cf863cf9b1f2604e597b6e
Contract's current owner address	0xa5878853f75e812411cf863cf9b1f2604e597b6e

Rhythm Token Distribution



The top 100 holders collectively own 90.37% (18,073,379,962.06 Tokens) of Rhythm

Token Total Supply: 20,000,000,000.00 Token | Total Token Holders: 1,211

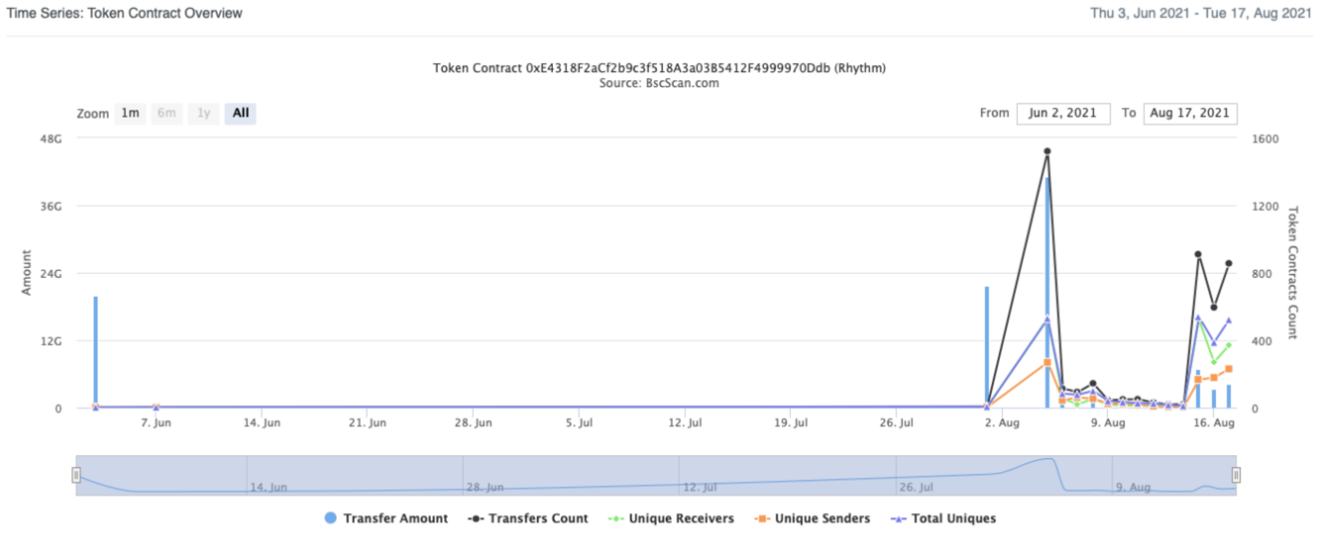
Rhythm Top 100 Token Holders

Source: BscScan.com

OTHER ACCOUNTS
0xeaed594b5926a7d5fbbc61985390baaf936a6b8d
0x0aae7d35dfb0847c90ec4476552a7da4ce6a1a52 (PancakeSwap V2: RHYTHM)
0x4160a2a55b2f0f0d50c60a9da4fae750ee848822
0x185ca3f6afe690c52c6e3b3a61d5db500783c725
0x3b9b733be516478a3612b7776fb5cfa931651e54
0x9f47af0141950d5f99f3b9f36d6b082dfd776395
0xd191bf770a153fa31b4197e3b40ab804ca3170f6
0x0c60eaaecf7d869c41ca71945228fc7d438b3073
0x216feb7859467fedf93c225318563ee06fa05bca

(A total of 18,073,379,962.06 tokens held by the top 100 accounts from the total supply of 20,000,000,000.00 token)

Rhythm Contract Interaction Details



Time Series: Token Contract Overview

Thu 3, Jun 2021 - Tue 17, Aug 2021

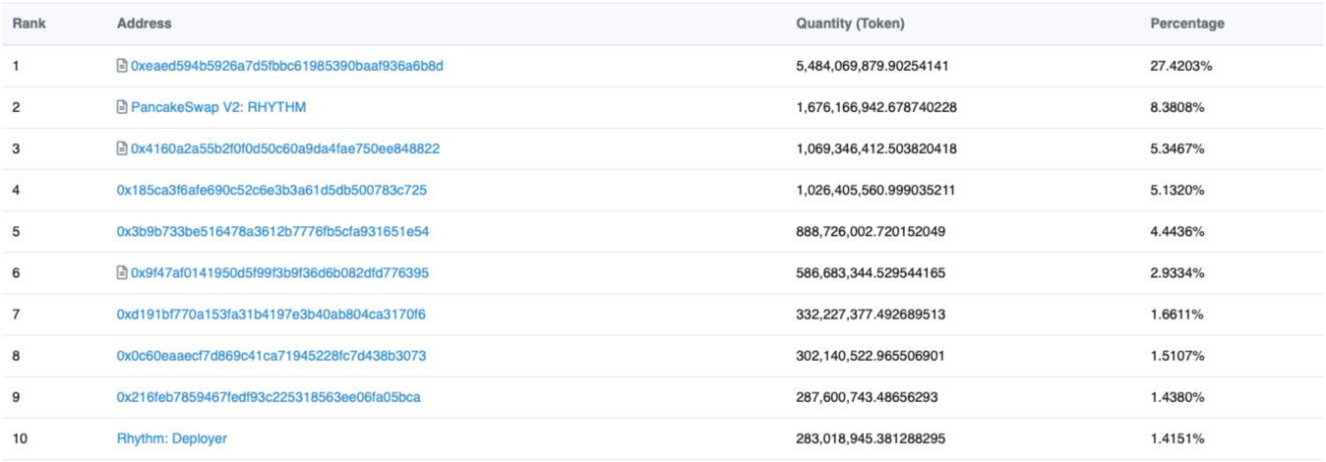
Token Contract 0xE4318F2aCf2b9c3f518A3a03B5412F4999970Ddb (Rhythm)

Source: BscScan.com

Zoom 1m 6m 1y All

From Jun 2, 2021 To Aug 17, 2021

Rhythm Top 10 Token Holders



Rank	Address	Quantity (Token)	Percentage
1	📄 0xeaed594b5926a7d5fbbc61985390baaf936a6b8d	5,484,069,879.90254141	27.4203%
2	📄 PancakeSwap V2: RHYTHM	1,676,166,942.678740228	8.3808%
3	📄 0x4160a2a55b2f0f0d50c60a9da4fae750ee848822	1,069,346,412.503820418	5.3467%
4	0x185ca3f6afe690c52c6e3b3a61d5db500783c725	1,026,405,560.999035211	5.1320%
5	0x3b9b733be516478a3612b7776fb5cfa931651e54	888,726,002.720152049	4.4436%
6	📄 0x9f47af0141950d5f99f3b9f36d6b082dfd776395	586,683,344.529544165	2.9334%
7	0xd191bf770a153fa31b4197e3b40ab804ca3170f6	332,227,377.492689513	1.6611%
8	0x0c60eaaecf7d869c41ca71945228fc7d438b3073	302,140,522.965506901	1.5107%
9	0x216feb7859467fedf93c225318563ee06fa05bca	287,600,743.48656293	1.4380%
10	Rhythm: Deployer	283,018,945.381288295	1.4151%

Contract functions details

```
+ [Int] BEP20
  - [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

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

+  Ownable (Context)
  - [Int] <Constructor> #
  - [Pub] owner
  - [Pub] artist
  - [Pub] renounceOwnership #
    - modifiers: onlyOwner
  - [Pub] transferOwnership #
    - modifiers: onlyOwner
  - [Pub] setArtistWalletAddress #
    - modifiers: onlyOwner
  - [Pub] getUnlockTime
  - [Pub] lock #
    - modifiers: onlyOwner
  - [Pub] unlock #

+  Rhythm (Context, BEP20, 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
- [Pub] excludeFromFee #
  - modifiers: onlyOwner
- [Pub] includeInFee #
  - modifiers: onlyOwner
- [Ext] setReflectionTaxFeePercent #
  - modifiers: onlyOwner
- [Ext] setLiquidityFeePercent #
  - modifiers: onlyOwner
- [Ext] setArtistFeePercent #
  - modifiers: onlyOwner
- [Ext] setMaxTxPercent #
  - modifiers: onlyOwner
- [Ext] setNumTokensSellToAddToLiquidity #
  - modifiers: onlyOwner
- [Pub] setSwapAndLiquifyEnabled #
  - modifiers: onlyOwner
- [Pub] setRouterAddress #
  - modifiers: onlyOwner
- [Ext] <Fallback> ($)
- [Prv] _reflectFee #
- [Prv] _getValues
- [Prv] _getTValues
- [Prv] _getRValues
- [Prv] _getRate
- [Prv] _getCurrentSupply
- [Prv] _takeLiquidity #
- [Prv] _takeArtistFee #
- [Prv] calculateFee
- [Prv] removeAllFee #
- [Prv] restoreAllFee #
- [Pub] isExcludedFromFee
- [Prv] _approve #
- [Prv] _transfer #
- [Prv] swapAndLiquify #
  - modifiers: lockTheSwap
- [Pub] withdrawLeftoverBNBToArtist #
  - modifiers: onlyOwner
- [Pub] getLeftOverContractBNBBalance

  - [Prv] swapTokensForBNB #
  - [Prv] addLiquidity #
  - [Prv] _tokenTransfer #
  - [Prv] _transferStandard #
  - [Prv] _transferToExcluded #
  - [Prv] _transferFromExcluded #
  - [Prv] _transferBothExcluded #
  - [Prv] _takeFee #

+ [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
  - [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 #

 ($) = 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.	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

Security Issues

High Severity Issues

No high severity issues found.

Medium Severity Issues

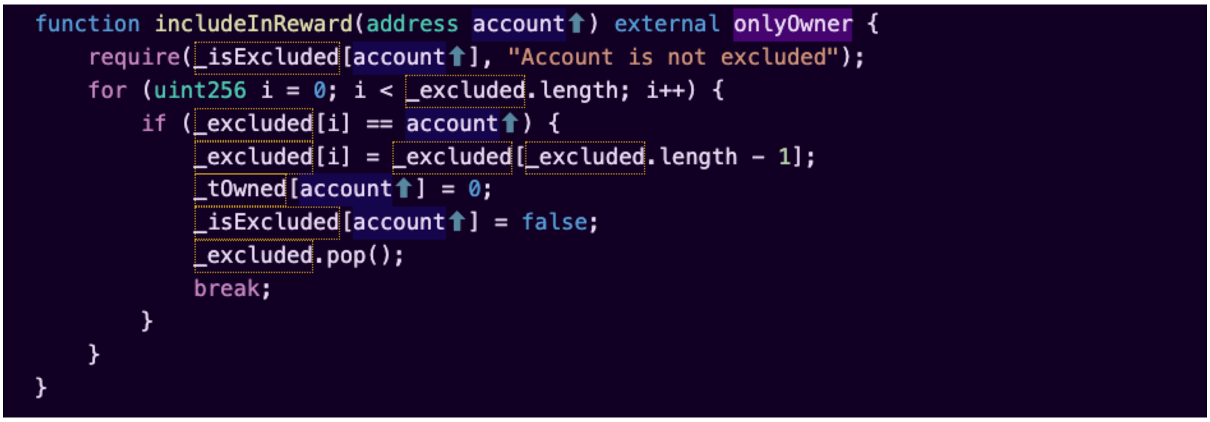
No medium severity issues found.

Low Severity Issues

1. Out of gas

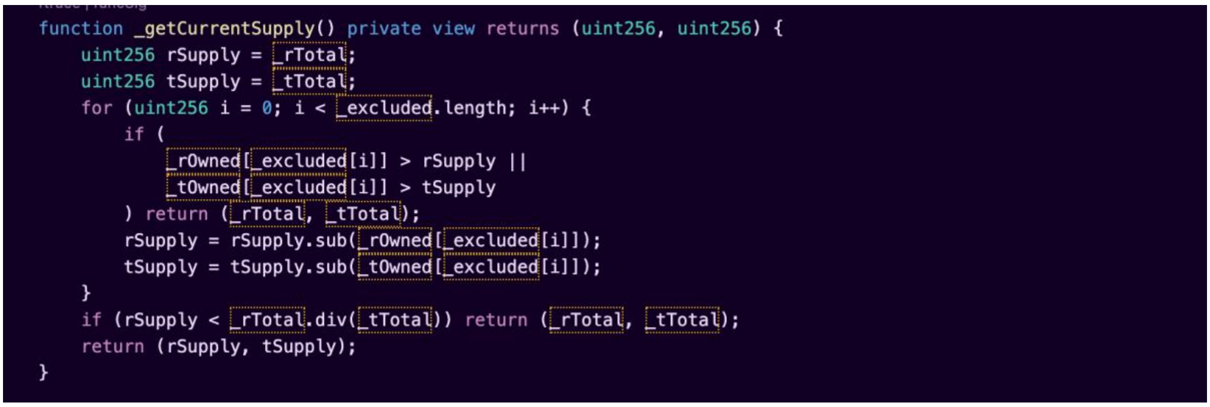
Issue:

- 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.



```
function includeInReward(address account) external onlyOwner {
    require(_isExcluded[account], "Account is not excluded");
    for (uint256 i = 0; i < _excluded.length; i++) {
        if (_excluded[i] == account) {
            _excluded[i] = _excluded[_excluded.length - 1];
            _tOwned[account] = 0;
            _isExcluded[account] = false;
            _excluded.pop();
            break;
        }
    }
}
```

- 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.



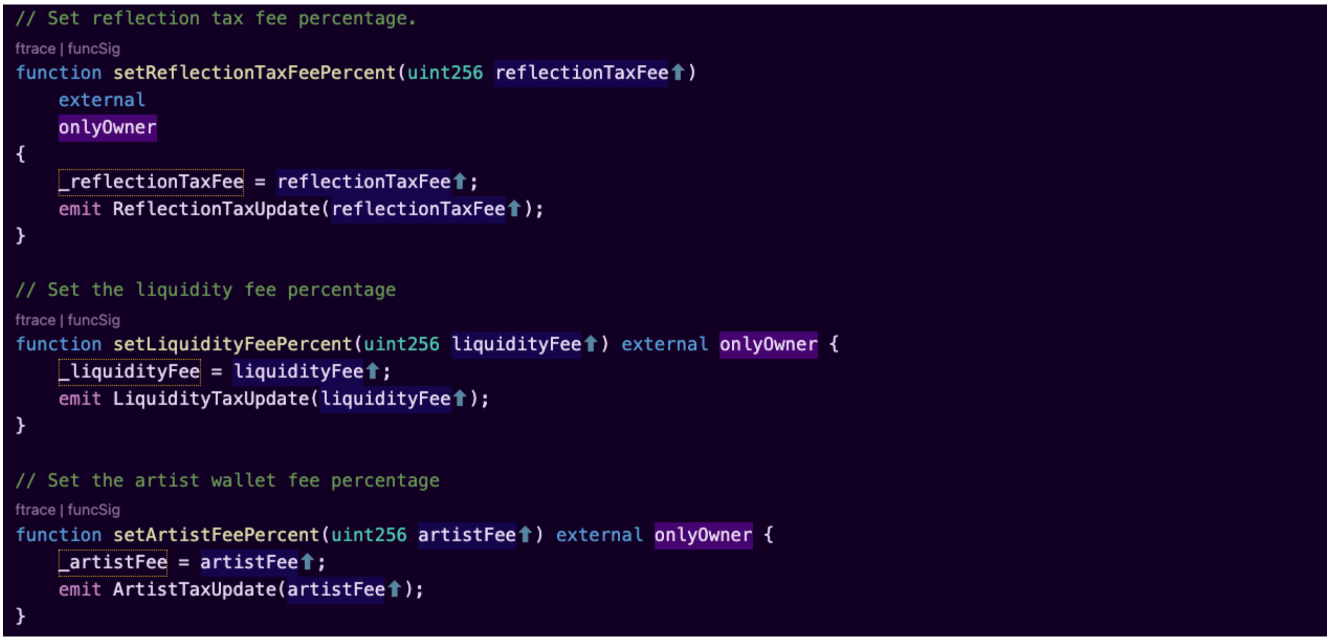
```
function _getCurrentSupply() private view returns (uint256, uint256) {
    uint256 rSupply = _rTotal;
    uint256 tSupply = _tTotal;
    for (uint256 i = 0; i < _excluded.length; i++) {
        if (
            _rOwned[_excluded[i]] > rSupply ||
            _tOwned[_excluded[i]] > tSupply
        ) return (_rTotal, _tTotal);
        rSupply = rSupply.sub(_rOwned[_excluded[i]]);
        tSupply = tSupply.sub(_tOwned[_excluded[i]]);
    }
    if (rSupply < _rTotal.div(_tTotal)) return (_rTotal, _tTotal);
    return (rSupply, tSupply);
}
```

Recommendation:

Check that the excluded array length is not too big.

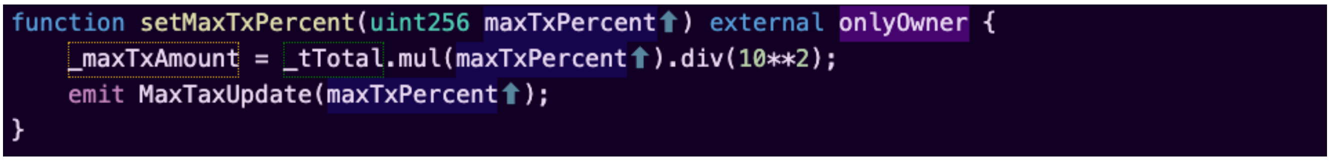
Owner privileges (In the period when the owner is not renounced)

- Owner can change the tax, artist and liquidity fees.



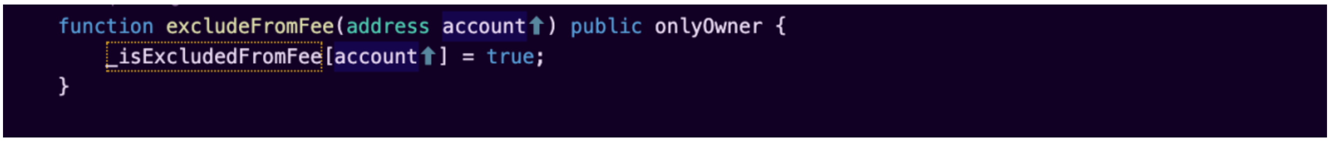
```
// Set reflection tax fee percentage.
ftrace | funcSig
function setReflectionTaxFeePercent(uint256 reflectionTaxFee)
    external
    onlyOwner
{
    _reflectionTaxFee = reflectionTaxFee;
    emit ReflectionTaxUpdate(reflectionTaxFee);
}

// Set the liquidity fee percentage
ftrace | funcSig
function setLiquidityFeePercent(uint256 liquidityFee) external onlyOwner {
    _liquidityFee = liquidityFee;
    emit LiquidityTaxUpdate(liquidityFee);
}

// Set the artist wallet fee percentage
ftrace | funcSig
function setArtistFeePercent(uint256 artistFee) external onlyOwner {
    _artistFee = artistFee;
    emit ArtistTaxUpdate(artistFee);
}
```

- Owner can change the maximum transaction amount.



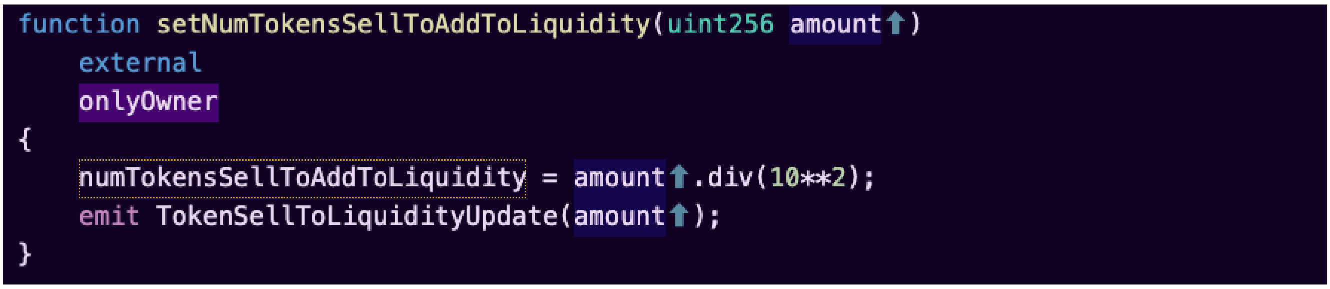
```
function setMaxTxPercent(uint256 maxTxPercent) external onlyOwner {
    _maxTxAmount = _tTotal.mul(maxTxPercent).div(10**2);
    emit MaxTaxUpdate(maxTxPercent);
}
```

- Owner can exclude from the fee.



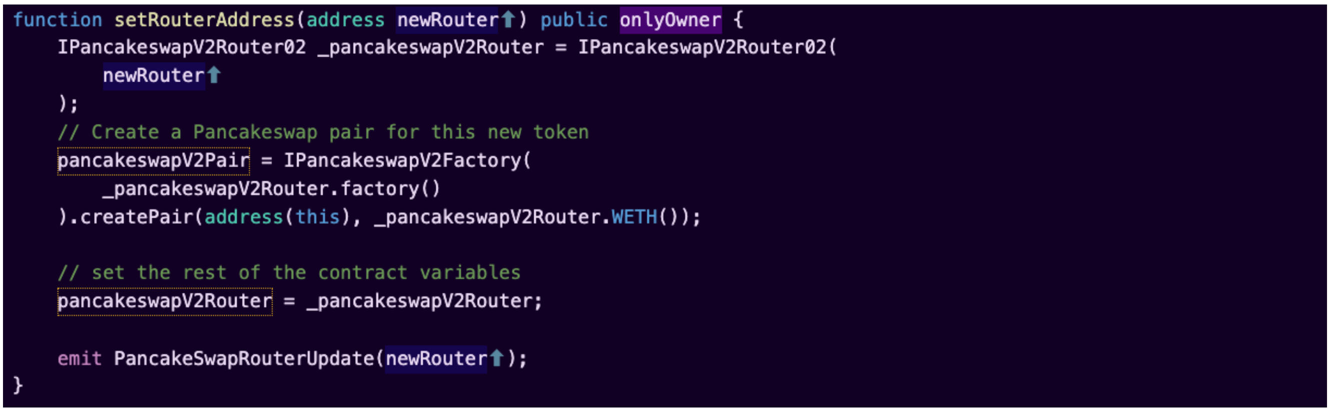
```
    function excludeFromFee(address account) public onlyOwner {
        _isExcludedFromFee[account] = true;
    }
```

- Owner can number of tokens to sell to add to liquidity.



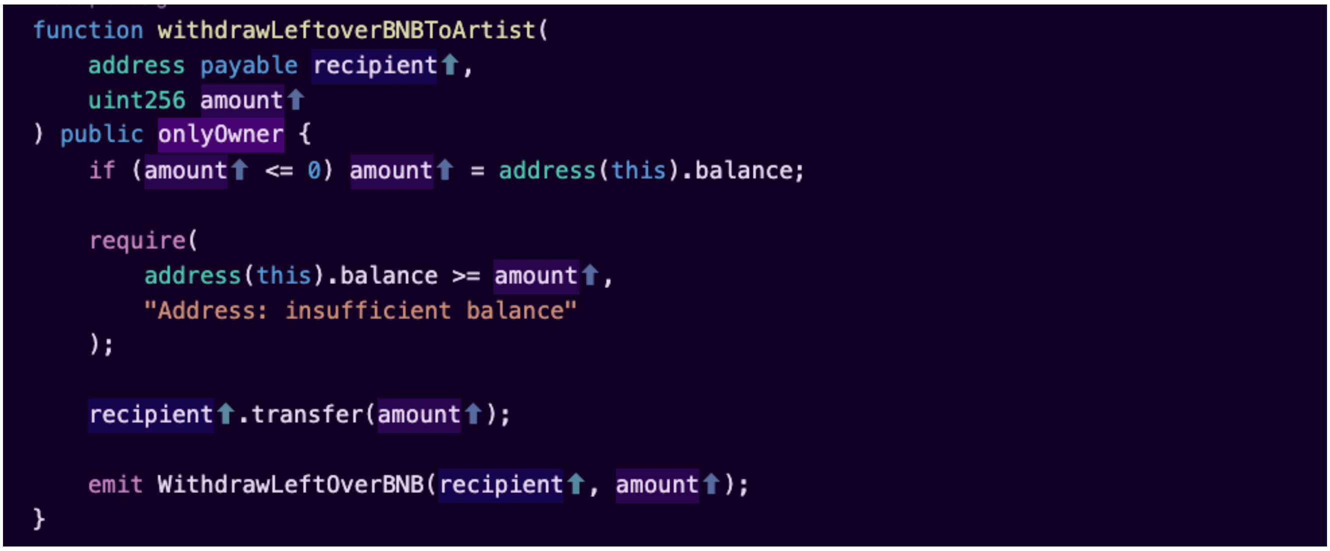
```
function setNumTokensSellToAddToLiquidity(uint256 amount)
    external
    onlyOwner
{
    numTokensSellToAddToLiquidity = amount.div(10**2);
    emit TokenSellToLiquidityUpdate(amount);
}
```

- Owner can change router address.



```
function setRouterAddress(address newRouter) public onlyOwner {
    IPancakeswapV2Router02 _pancakeswapV2Router = IPancakeswapV2Router02(
        newRouter
    );
    // Create a Pancakeswap pair for this new token
    pancakeswapV2Pair = IPancakeswapV2Factory(
        _pancakeswapV2Router.factory()
    ).createPair(address(this), _pancakeswapV2Router.WETH());

    // set the rest of the contract variables
    pancakeswapV2Router = _pancakeswapV2Router;

    emit PancakeSwapRouterUpdate(newRouter);
}
```

- Owner can withdraw contract BNBs.



```
function withdrawLeftoverBNBToArtist(
    address payable recipient,
    uint256 amount
) public onlyOwner {
    if (amount <= 0) amount = address(this).balance;

    require(
        address(this).balance >= amount,
        "Address: insufficient balance"
    );

    recipient.transfer(amount);

    emit WithdrawLeftOverBNB(recipient, amount);
}
```

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:
Presale Liquidity Locked:
https://dxsale.app/app/v2_9/dxlockview?id=2045&add=0&type=lpdefi&chain=BSC

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.