Techrate1 Techrate

TechRate

AUDIT COMPANY

Smart Contract Security Audit

TechRate

July, 2021

Audit Details

Audited project

AetherV2

Deployer address

0x7bd4bddaa330696edb1592e81c35cc751510839f

Client contacts:

AetherV2 team

Blockchain

Binance Smart Chain

Project 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) (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 AetherV2 to perform an audit of smart contracts:
https://bscscan.com/address/0x6d3a0fb0070ea61f901ebc0b675c30450acac737#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.

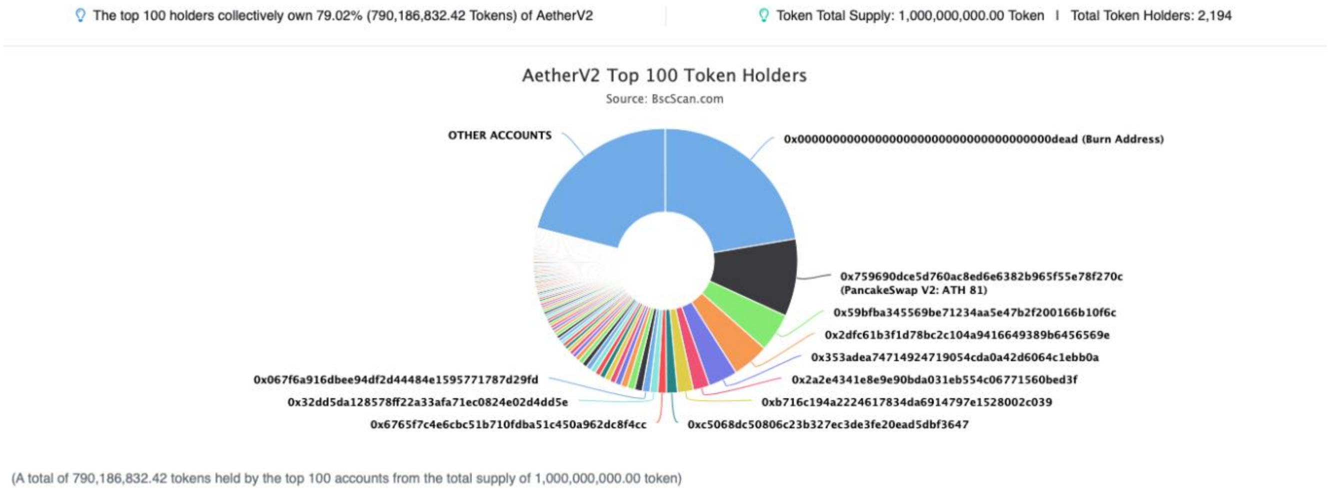
The information in this report should be used to understand the risk exposure of the smart contract, and as a guide to improve the security posture of the smart contract by remediating the issues that were identified.

Contracts Details

Token contract details for 27.09.2021

Contract name	AetherV2
Contract address	0x6d3A0Fb0070EA61F901eBc0b675c30450ACAc737
Total supply	1,000,000,000
Token ticker	ATH
Decimals	9
Token holders	2,194
Transactions count	7,494
Top 100 holders dominance	79.02%
Liquidity fee	9
Tax fee	5
Total fees	87775026537516813
Uniswap V2 pair	0x759690dce5d760ac8ed6e6382b965f55e78f270c
Contract deployer address	0x7bd4bddaa330696edb1592e81c35cc751510839f
Contract’s current owner address	0x7bd4bddaa330696edb1592e81c35cc751510839f

AetherV2 Token Distribution



The top 100 holders collectively own 79.02% (790,186,832.42 Tokens) of AetherV2

Token Total Supply: 1,000,000,000.00 Token | Total Token Holders: 2,194

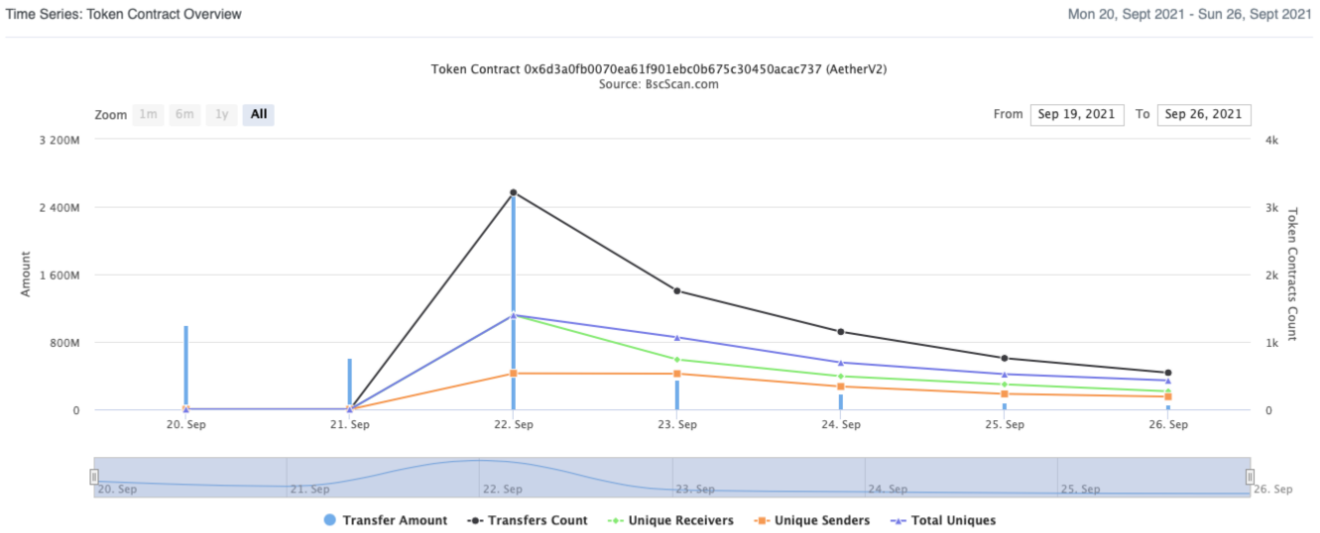
AetherV2 Top 100 Token Holders

Source: BscScan.com

OTHER ACCOUNTS
0x000000000000000000000000000000000000dead (Burn Address)
0x759690dce5d760ac8ed6e6382b965f55e78f270c (PancakeSwap V2: ATH 81)
0x59bfba345569be71234aa5e47b2f200166b10f6c
0x2dfc61b3f1d78bc2c104a9416649389b6456569e
0x353adea74714924719054cda0a42d6064c1ebb0a
0x2a2e4341e8e9e90bda031eb554c06771560bed3f
0xb716c194a2224617834da6914797e1528002c039
0xc5068dc50806c23b327ec3de3fe20ead5dbf3647
0x6765f7c4e6cbc51b710fdba51c450a962dc8f4cc
0x32dd5da128578ff22a33afa71ec0824e02d4dd5e
0x067f6a916dbee94df2d44484e1595771787d29fd

(A total of 790,186,832.42 tokens held by the top 100 accounts from the total supply of 1,000,000,000.00 token)

AetherV2 Contract Interaction Details



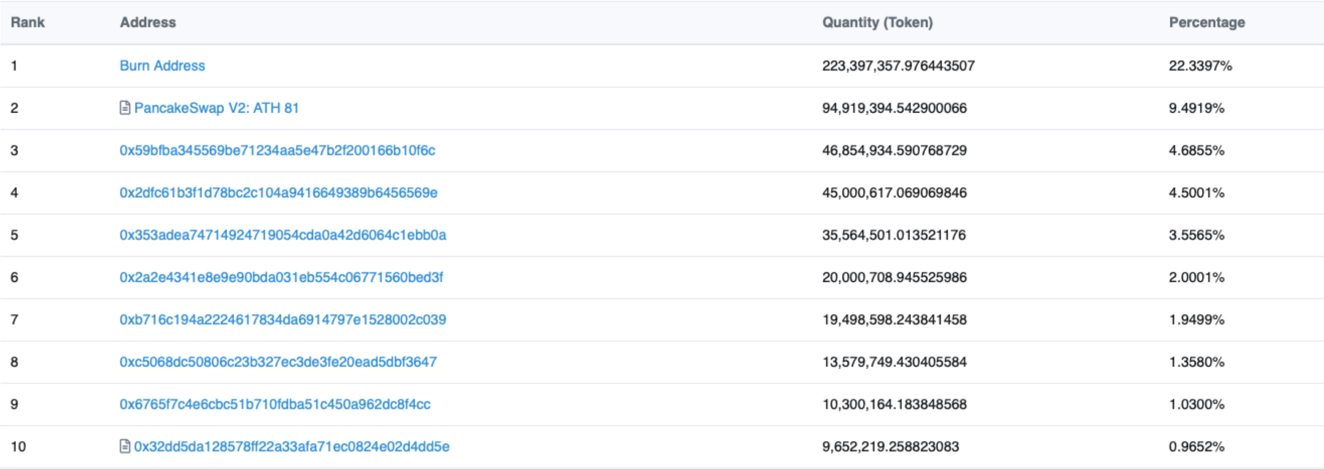
Time Series: Token Contract Overview

Mon 20, Sept 2021 - Sun 26, Sept 2021

Token Contract 0x6d3a0fb0070ea61f901ebc0b675c30450acac737 (AetherV2)

Source: BscScan.com

AetherV2 Top 10 Token Holders



Rank	Address	Quantity (Token)	Percentage
1	Burn Address	223,397,357.976443507	22.3397%
2	PancakeSwap V2: ATH 81	94,919,394.542900066	9.4919%
3	0x59bfba345569be71234aa5e47b2f200166b10f6c	46,854,934.590768729	4.6855%
4	0x2dfc61b3f1d78bc2c104a9416649389b6456569e	45,000,617.069069846	4.5001%
5	0x353adea74714924719054cda0a42d6064c1ebb0a	35,564,501.013521176	3.5565%
6	0x2a2e4341e8e9e90bda031eb554c06771560bed3f	20,000,708.945525986	2.0001%
7	0xb716c194a2224617834da6914797e1528002c039	19,498,598.243841458	1.9499%
8	0xc5068dc50806c23b327ec3de3fe20ead5dbf3647	13,579,749.430405584	1.3580%
9	0x6765f7c4e6cbc51b710fdba51c450a962dc8f4cc	10,300,164.183848568	1.0300%
10	0x32dd5da128578ff22a33afa71ec0824e02d4dd5e	9,652,219.258823083	0.9652%

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

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

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

+ [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 #
  - [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 #

```
+ AetherV2 (Context, IERC20, Ownable)
  - [Pub] <Constructor> #
  - [Pub] setRouterAddress #
    - modifiers: onlyOwner
  - [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
  - [Prv] _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] _calculateFee
  - [Prv] removeAllFee #
  - [Prv] restoreAllFee #
  - [Pub] isExcludedFromFee
  - [Prv] _approve #
  - [Prv] _transfer #
  - [Prv] swapAndLiquify #
    - modifiers: lockTheSwap
  - [Ext] withdrawResidualBNB #
    - modifiers: onlyOwner
```

- [Pub] setDevWallet #
  - modifiers: onlyOwner
- [Pub] setMarketingWallet #
  - modifiers: onlyOwner
- [Pub] setArcaWallet #
  - modifiers: onlyOwner
- [Pub] setBuybackWallet #
  - modifiers: onlyOwner
- [Ext] enableTransfer #
  - modifiers: onlyOwner
- [Ext] multiTransfer #
  - modifiers: onlyOwner
- [Prv] swapTokensForEth #
- [Prv] addLiquidity #
- [Prv] _tokenTransfer #
- [Prv] _transferStandard #
- [Prv] _transferToExcluded #
- [Prv] _transferFromExcluded #

($) = 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

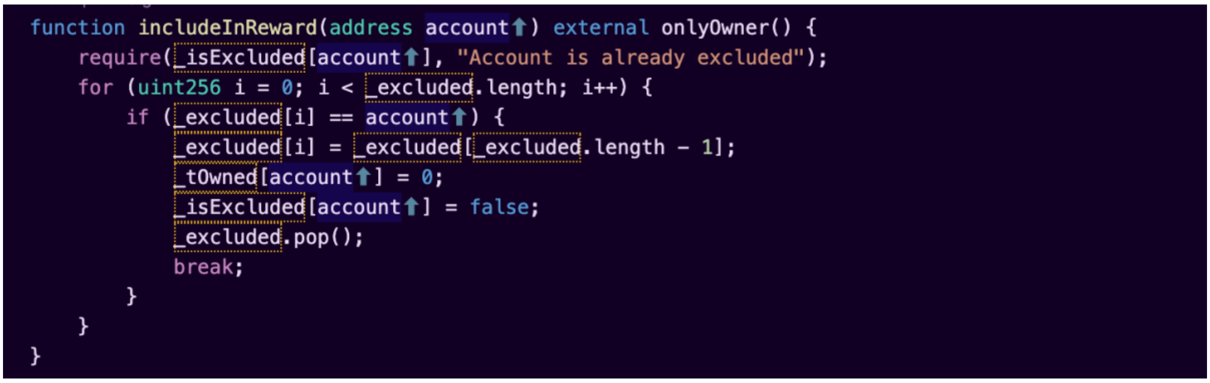
No medium severity issues found.

Low Severity Issues

1. Out of gas

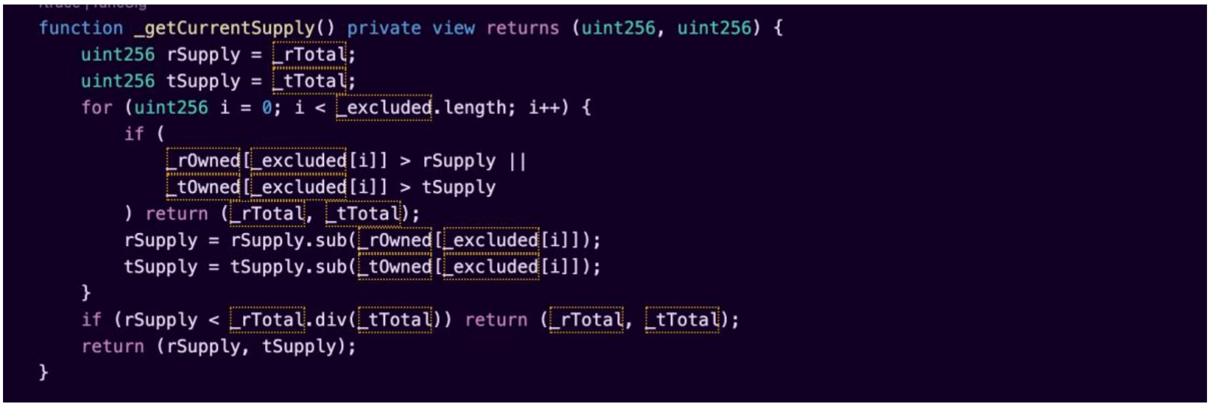
Issue:

- 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 already 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.



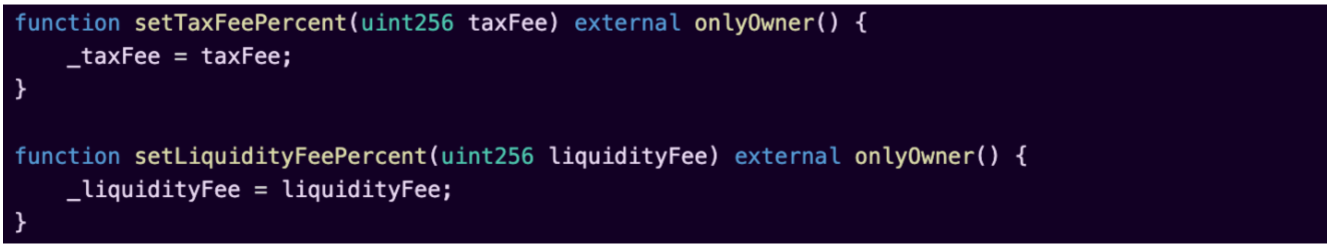
```
function _getCurrentSupply() private view returns (uint256, uint256) {
    uint256 rSupply = _rTotal;
    uint256 tSupply = _tTotal;
    for (uint256 i = 0; i < _excluded.length; i++) {
        if (
            _rOwned[_excluded[i]] > rSupply ||
            _tOwned[_excluded[i]] > tSupply
      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

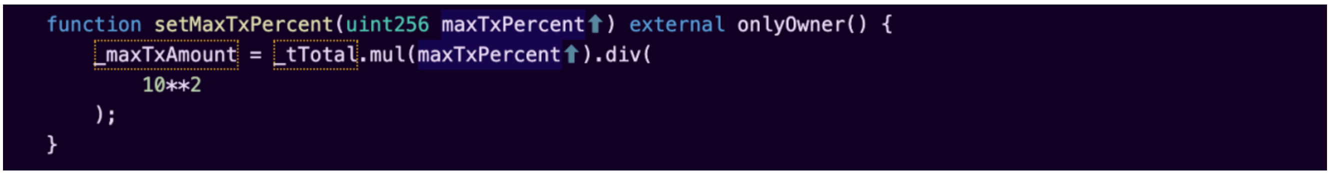
Owner privileges (In the period when the owner is not renounced)

- Owner can change the tax and liquidity fee.



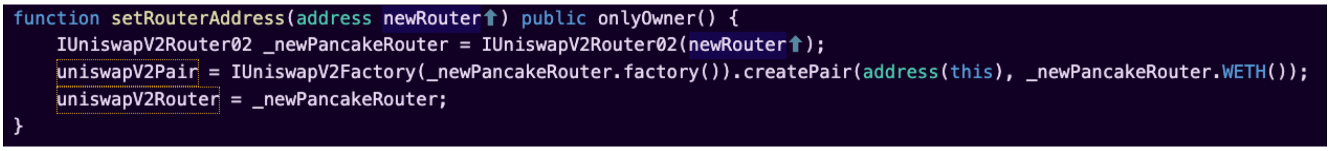
```
function setTaxFeePercent(uint256 taxFee) external onlyOwner() {
    _taxFee = taxFee;
}

function setLiquidityFeePercent(uint256 liquidityFee) external onlyOwner() {
    _liquidityFee = liquidityFee;
}
```

- Owner can change the maximum transaction amount.



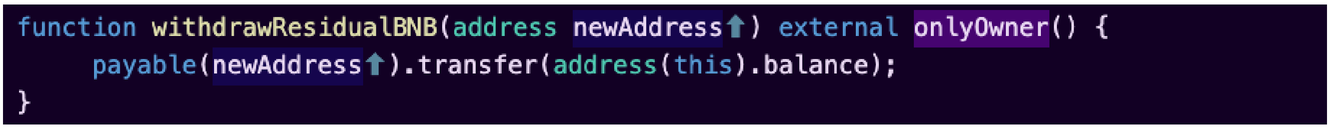
```
  function setMaxTxPercent(uint256 maxTxPercent) external onlyOwner() {
      _maxTxAmount = _tTotal.mul(maxTxPercent).div(
          10**2
      );
  }
```

- Owner can change router address.



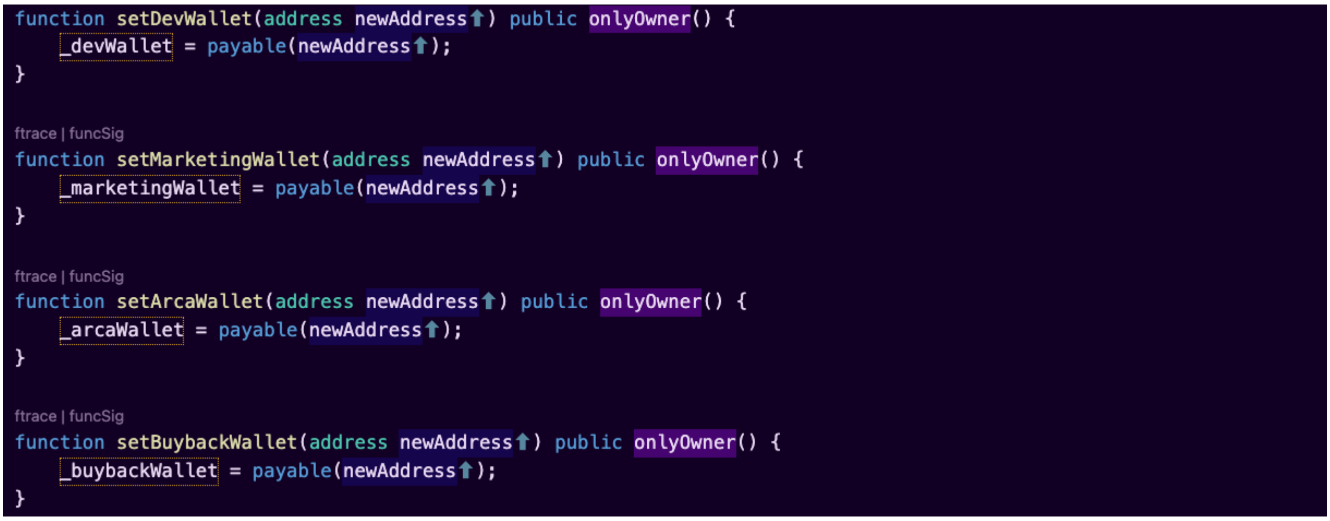
```
function setRouterAddress(address newRouter) public onlyOwner() {
    IUniswapV2Router02 _newPancakeRouter = IUniswapV2Router02(newRouter);
    uniswapV2Pair = IUniswapV2Factory(_newPancakeRouter.factory()).createPair(address(this), _newPancakeRouter.WETH());
    uniswapV2Router = _newPancakeRouter;
}
```

- Owner can withdraw contract BNBs.



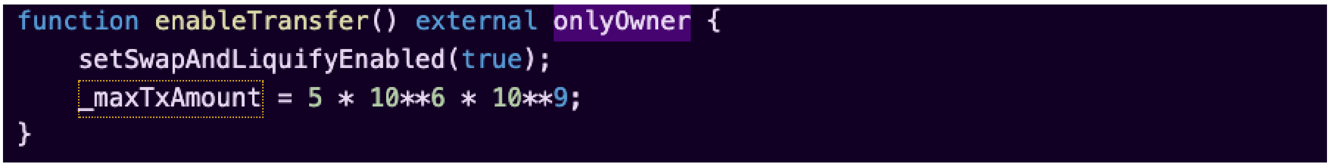
```
function withdrawResidualBNB(address newAddress) external onlyOwner() {
    payable(newAddress).transfer(address(this).balance);
}
```

- Owner can change fee addresses.



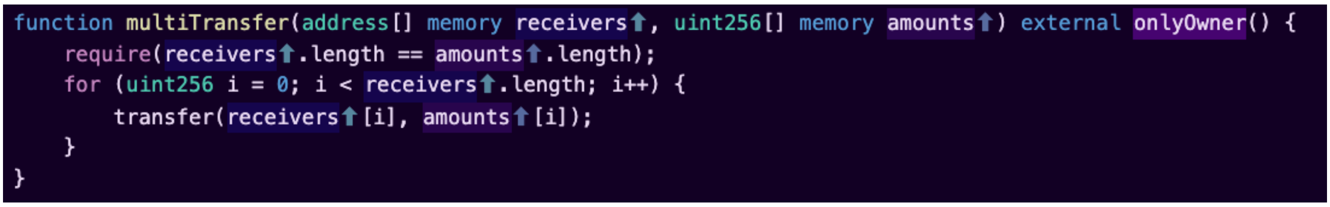
```
function setDevWallet(address newAddress) public onlyOwner() {
    _devWallet = payable(newAddress);
}

ftrace | funcSig
function setMarketingWallet(address newAddress) public onlyOwner() {
    _marketingWallet = payable(newAddress);
}

ftrace | funcSig
function setArcaWallet(address newAddress) public onlyOwner() {
    _arcaWallet = payable(newAddress);
}

ftrace | funcSig
function setBuybackWallet(address newAddress) public onlyOwner() {
    _buybackWallet = payable(newAddress);
}
```

- Owner can init swap and liquify and reset _maxTxAmount.



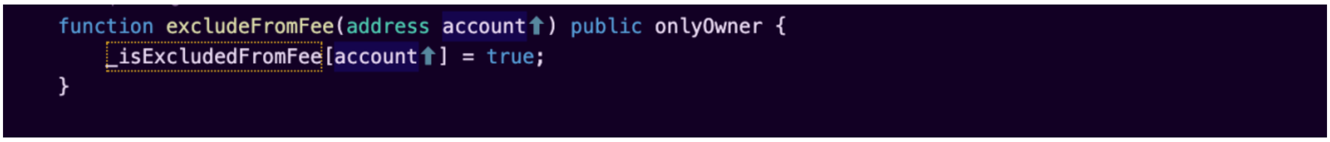
```
function enableTransfer() external onlyOwner {
    setSwapAndLiquifyEnabled(true);
    _maxTxAmount = 5 * 10**6 * 10**9;
}
```

- Owner can multitransfer.



```
function multiTransfer(address[] memory receivers, uint256[] memory amounts) external onlyOwner() {
    require(receivers.length == amounts.length);
    for (uint256 i = 0; i < receivers.length; i++) {
        transfer(receivers[i], amounts[i]);
    }
}
```

- Owner can exclude from the fee.



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

Conclusion

Smart contracts contain low severity issues! Liquidity pair contract's security is not checked due to out of scope. There is no liquidity adding in the contract.

Liquidity locking details provided by the team:
https://dxsale.app/app/v3/dxlplocksearch?id=0&add=0x6d3A0Fb0070EA61F901eBc0b675c30450ACAc737&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.