Techrate1 Techrate

TechRate

AUDIT COMPANY

Smart Contract Security Audit

TechRate

October, 2021

Audit Details

Audited project

Baby Moon Floki

Deployer address

0x75001ccda5b6a711546d9bc14ac805dd78ccc24f

Client contacts:

Baby Moon Floki 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 Baby Moon Floki to perform an audit of smart contracts:

https://bscscan.com/address/0x54e87ed5a096f09d9665fd114002bddfc2084a7f#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.

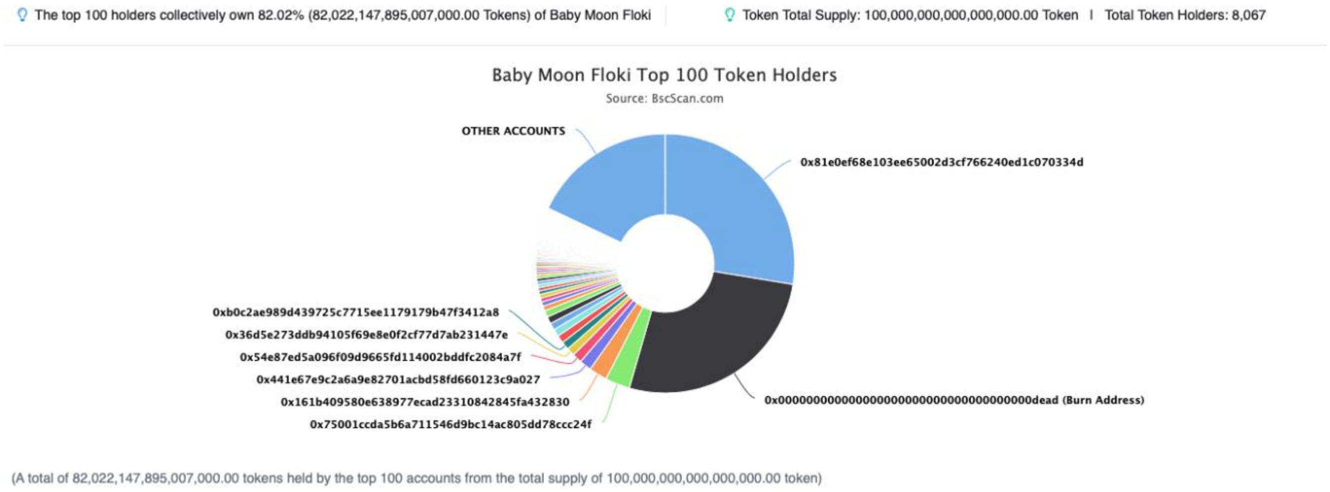
The information in this report should be used to understand the risk exposure of the smart contract, and as a guide to improve the security posture of the smart contract by remediating the issues that were identified.

Contracts Details

Token contract details for 27.10.2021

Contract name	Baby Moon Floki
Contract address	0x54E87ed5A096f09d9665fD114002bdDFc2084a7F
Total supply	100,000,000,000,000,000
Token ticker	Floki
Decimals	9
Token holders	8,067
Transactions count	23,487
Top 100 holders dominance	82.02%
Liquidity fee	6
Tax fee	2
Total fees	6443572172255557907559441
Uniswap V2 pair	0x161b409580e638977ecad23310842845fa432830
Contract deployer address	0x75001ccda5b6a711546d9bc14ac805dd78ccc24f
Contract’s current owner address	0x75001ccda5b6a711546d9bc14ac805dd78ccc24f

Baby Moon Floki Token Distribution



The top 100 holders collectively own 82.02% (82,022,147,895,007,000.00 Tokens) of Baby Moon Floki

Token Total Supply: 100,000,000,000,000,000.00 Token | Total Token Holders: 8,067

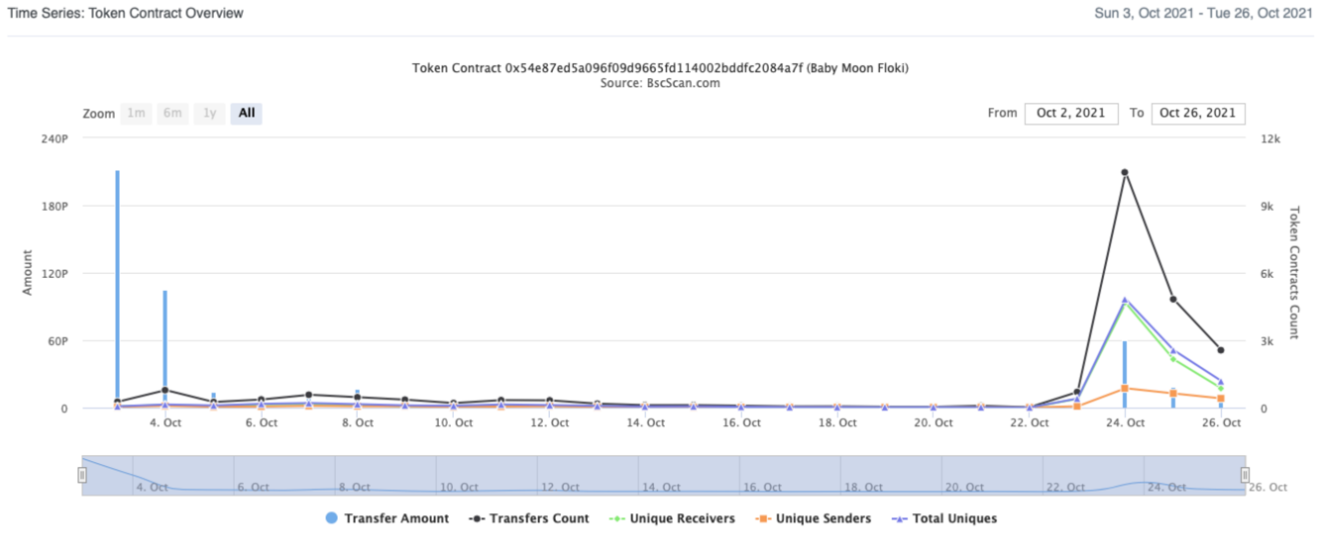
Baby Moon Floki Top 100 Token Holders

Source: BscScan.com

OTHER ACCOUNTS
0x81e0ef68e103ee65002d3cf766240ed1c070334d
0xb0c2ae989d439725c7715ee1179179b47f3412a8
0x36d5e273ddb94105f69e8e0f2cf77d7ab231447e
0x54e87ed5a096f09d9665fd114002bddfc2084a7f
0x441e67e9c2a6a9e82701acbd58fd660123c9a027
0x161b409580e638977ecad23310842845fa432830
0x75001ccda5b6a711546d9bc14ac805dd78ccc24f
0x000000000000000000000000000000000000dead (Burn Address)

(A total of 82,022,147,895,007,000.00 tokens held by the top 100 accounts from the total supply of 100,000,000,000,000,000.00 token)

Baby Moon Floki Contract Interaction Details



Time Series: Token Contract Overview

Sun 3, Oct 2021 - Tue 26, Oct 2021

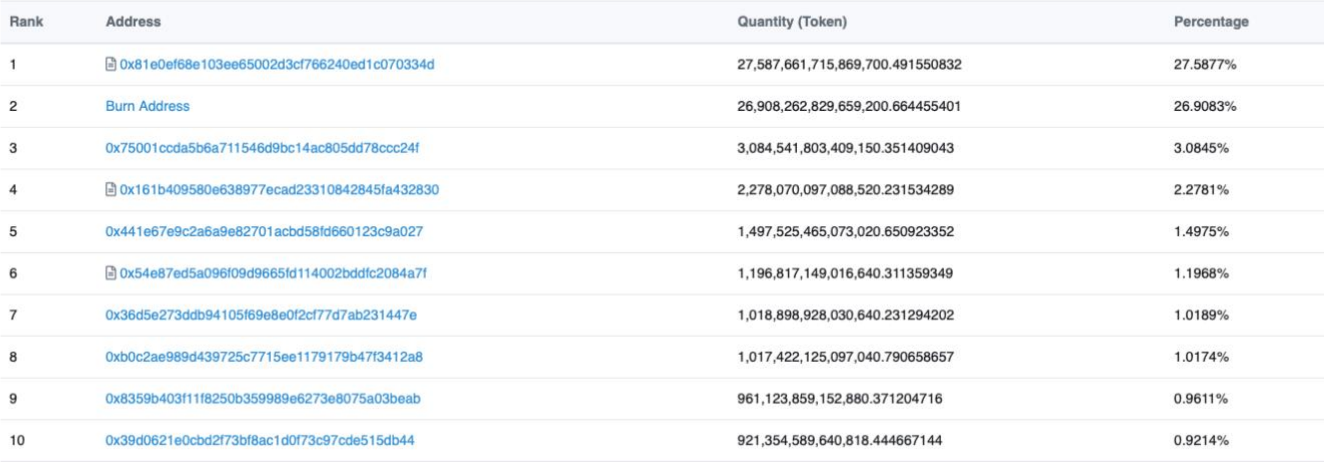
Token Contract 0x54e87ed5a096f09d9665fd114002bddfc2084a7f (Baby Moon Floki)

Source: BscScan.com

Zoom 1m 6m 1y All

From Oct 2, 2021 To Oct 26, 2021

Baby Moon Floki Top 10 Token Holders



Rank	Address	Quantity (Token)	Percentage
1	📄 0x81e0ef68e103ee65002d3cf766240ed1c070334d	27,587,661,715,869,700.491550832	27.5877%
2	Burn Address	26,908,262,829,659,200.664455401	26.9083%
3	0x75001ccda5b6a711546d9bc14ac805dd78ccc24f	3,084,541,803,409,150.351409043	3.0845%
4	📄 0x161b409580e638977ecad23310842845fa432830	2,278,070,097,088,520.231534289	2.2781%
5	0x441e67e9c2a6a9e82701acbd58fd660123c9a027	1,497,525,465,073,020.650923352	1.4975%
6	📄 0x54e87ed5a096f09d9665fd114002bddfc2084a7f	1,196,817,149,016,640.311359349	1.1968%
7	0x36d5e273ddb94105f69e8e0f2cf77d7ab231447e	1,018,898,928,030,640.231294202	1.0189%
8	0xb0c2ae989d439725c7715ee1179179b47f3412a8	1,017,422,125,097,040.790658657	1.0174%
9	0x8359b403f11f8250b359989e6273e8075a03beab	961,123,859,152,880.371204716	0.9611%
10	0x39d0621e0cbd2f73bf8ac1d0f73c97cde515db44	921,354,589,640,818.444667144	0.9214%

Contract functions details

+ Context
  - [Int] _msgSender
  - [Int] _msgData
+ [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
+ [Lib] Address
  - [Int] isContract
  - [Int] sendValue #
  - [Int] functionCall #
  - [Int] functionCall #
  - [Int] functionCallWithValue #
  - [Int] functionCallWithValue #
  - [Prv] _functionCallWithValue #
+ Ownable (Context)
  - [Pub] <Constructor> #
  - [Pub] owner
  - [Pub] renounceOwnership #
    - modifiers: onlyOwner
  - [Pub] transferOwnership #
    - modifiers: onlyOwner
  - [Pub] getUnlockTime
  - [Pub] getTime
  - [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] 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 #

  +  BabyMoonFloki (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] minimumTokensBeforeSwapAmount
- [Pub] buyBackSellLimitAmount
- [Pub] deliver #
- [Pub] reflectionFromToken
- [Pub] tokenFromReflection
- [Pub] excludeFromReward #
  - modifiers: onlyOwner
- [Ext] includeInReward #
  - modifiers: onlyOwner
- [Prv] _approve #
- [Prv] _transfer #
- [Prv] swapTokens #
  - modifiers: lockTheSwap
- [Prv] buyBackTokens #
  - modifiers: lockTheSwap
- [Prv] swapTokensForEth #
- [Prv] swapETHForTokens #
- [Prv] addLiquidity #
- [Prv] _tokenTransfer #
- [Prv] _transferStandard #
- [Prv] _transferToExcluded #
- [Prv] _transferFromExcluded #
- [Prv] _transferBothExcluded #
- [Prv] _reflectFee #
- [Prv] _getValues
- [Prv] _getTValues
- [Prv] _getRValues
- [Prv] _getRate
- [Prv] _getCurrentSupply
- [Prv] _takeLiquidity #
- [Prv] calculateTaxFee
- [Prv] calculateLiquidityFee
- [Prv] removeAllFee #
- [Prv] restoreAllFee #
- [Pub] isExcludedFromFee
- [Pub] excludeFromFee #
  - modifiers: onlyOwner
- [Pub] includeInFee #
  - modifiers: onlyOwner
- [Prv] _getSellBnBAmount
- [Prv] _removeOldSellHistories #
- [Ext] SetBuyBackMaxTimeForHistories #
  - modifiers: onlyOwner
- [Ext] SetBuyBackDivisor #

    - modifiers: onlyOwner
  - [Pub] GetBuyBackTimeInterval
  - [Ext] SetBuyBackTimeInterval #
    - modifiers: onlyOwner
  - [Ext] SetBuyBackRangeRate #
    - modifiers: onlyOwner
  - [Pub] GetSwapMinutes
  - [Ext] SetSwapMinutes #
    - modifiers: onlyOwner
  - [Ext] setTaxFeePercent #
    - modifiers: onlyOwner
  - [Ext] setBuyFee #
    - modifiers: onlyOwner
  - [Ext] setSellFee #
    - modifiers: onlyOwner
  - [Ext] setLiquidityFeePercent #
    - modifiers: onlyOwner
  - [Ext] setBuyBackSellLimit #
    - modifiers: onlyOwner
  - [Ext] setMaxTxAmount #
    - modifiers: onlyOwner
  - [Ext] setMarketingDivisor #
    - modifiers: onlyOwner
  - [Ext] setNumTokensSellToAddToBuyBack #
    - modifiers: onlyOwner
  - [Ext] setMarketingAddress #
    - modifiers: onlyOwner
  - [Pub] setSwapAndLiquifyEnabled #
    - modifiers: onlyOwner
  - [Pub] setBuyBackEnabled #
    - modifiers: onlyOwner
  - [Pub] setAutoBuyBackEnabled #
    - modifiers: onlyOwner
  - [Ext] prepareForPreSale #
    - modifiers: onlyOwner
  - [Ext] afterPreSale #
    - modifiers: onlyOwner
  - [Prv] transferToAddressETH #
  - [Pub] changeRouterVersion #
    - modifiers: onlyOwner
  - [Ext] <Fallback> ($)
  - [Pub] transferForeignToken #
    - modifiers: onlyOwner
  - [Ext] Sweep #
    - modifiers: onlyOwner
  - [Ext] setAddressFee #
    - modifiers: onlyOwner
  - [Ext] setBuyAddressFee #
    - modifiers: onlyOwner
  - [Ext] setSellAddressFee #
    - modifiers: onlyOwner

($) = 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

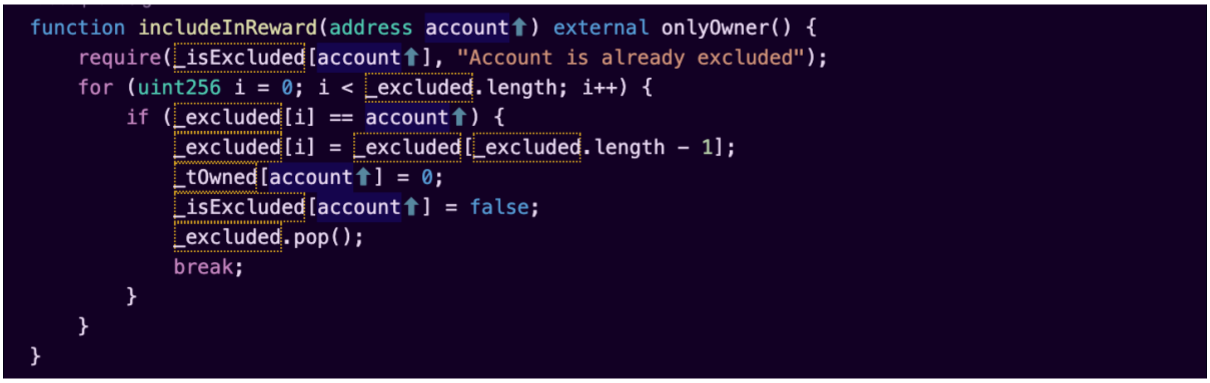
No medium severity issues found.

Low Severity Issues

1. Out of gas

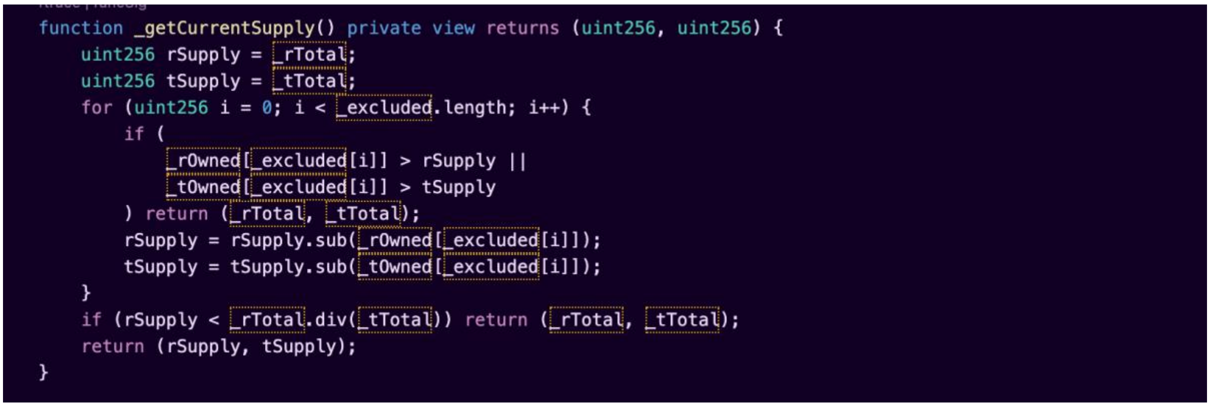
Issue:

- 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.

Notes:

- addLiquidity function is unused.

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

- Owner can withdraw tokens.
- Owner can withdraw BNBs.
- Owner can change tax and liquidity fees.
- Owner can change maximum transaction amount.
- Owner can exclude from the fee.
- Owner can change marketingDivisor.
- Owner can change minimum number of tokens to add to liquidity.
- Owner can change marketing address.
- Owner can enable and disable buyBack.
- Owner can enable before and after presale modes.
- Owner can lock and unlock. By the way, using these functions the owner could retake privileges even after the ownership was renounced.
- Owner can set addresses fees.
- Owner can Uniswap router address.
- Owner can disable and enable auto buyback.
- Owner can change buyBackSellLimit.
- Owner can change buy and sell fees.
- Owner can can change _intervalMinutesForSwap.
- Owner can change buyback time interval and range rate.
- Owner can change buyback devisor.
- Owner can change _buyBackMaxTimeForHistories.

Conclusion

Smart contracts contain low severity issues! Liquidity pair contract's security is not checked due to out of scope.
4% of the liquidity goes to the marketing address. The further transfers and operations with the funds raise are not related to this particular contract.

Liquidity locking details are NOT provided by the team.

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.