Techrate1 Techrate

TechRate

AUDIT COMPANY

Smart Contract Security Audit

TechRate

November, 2021

Audit Details

Audited project

PulseFeg

Deployer address

0xf1662adf6d4d6de9d39f44e13f19db268ff3c01d

Client contacts:

PulseFeg team

Blockchain

Binance Smart Chain

Project website:

https://pulsefeg.finance

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 PulseFeg to perform an audit of smart contracts:

https://bscscan.com/address/0x1e5dd94a6d7190ab77f834e2ccdf9072597ae4e3#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.

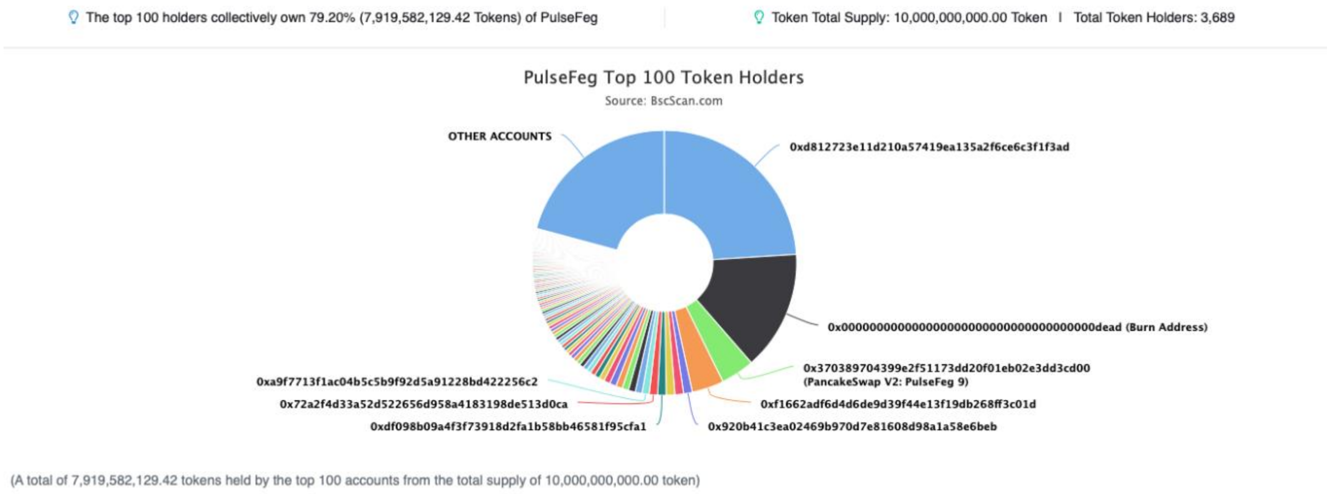
The information in this report should be used to understand the risk exposure of the smart contract, and as a guide to improve the security posture of the smart contract by remediating the issues that were identified.

Contracts Details

Token contract details for 07.11.2021

Contract name	PulseFeg
Contract address	0x1E5Dd94A6d7190ab77f834E2cCDF9072597ae4E3
Total supply	10,000,000,000
Token ticker	PulseFeg
Decimals	9
Token holders	3,689
Transactions count	12,516
Top 100 holders dominance	79.20%
Buyback fee	2
Marketing fee	2
Total fees	268479513977093787
Uniswap V2 pair	0x370389704399e2f51173dd20f01eb02e3dd3cd00
Contract deployer address	0xf1662adf6d4d6de9d39f44e13f19db268ff3c01d
Contract’s current owner address	0xf1662adf6d4d6de9d39f44e13f19db268ff3c01d

PulseFeg Token Distribution



The top 100 holders collectively own 79.20% (7,919,582,129.42 Tokens) of PulseFeg

Token Total Supply: 10,000,000,000.00 Token | Total Token Holders: 3,689

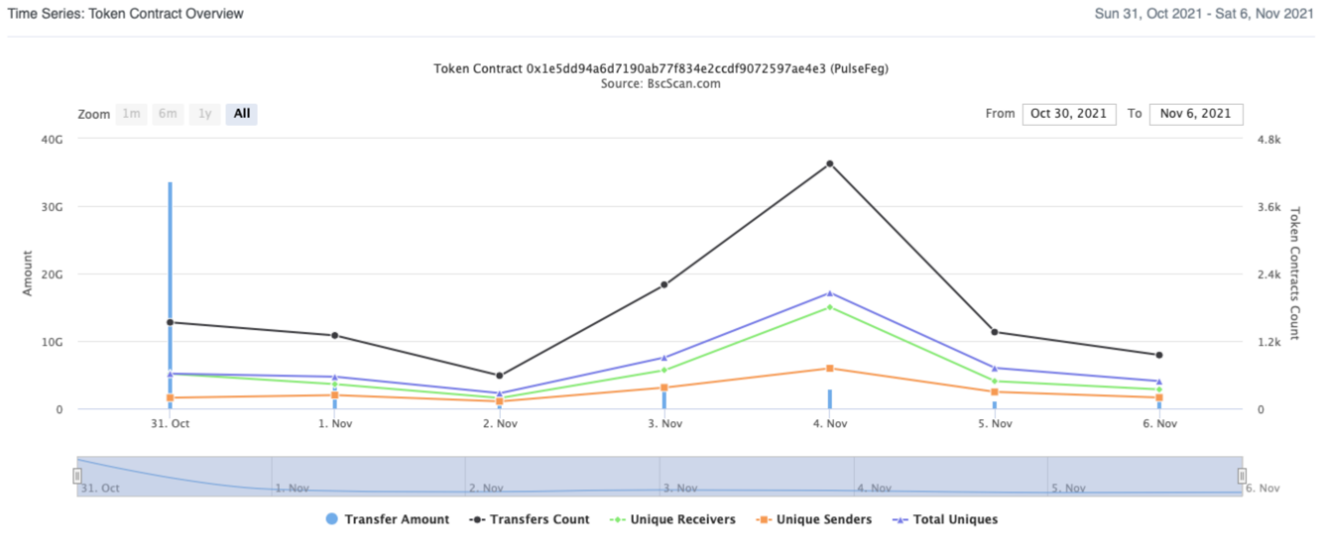
PulseFeg Top 100 Token Holders

Source: BscScan.com

OTHER ACCOUNTS
0xd812723e11d210a57419ea135a2f6ce6c3f1f3ad
0x000000000000000000000000000000000000dead (Burn Address)
0x370389704399e2f51173dd20f01eb02e3dd3cd00
(PancakeSwap V2: PulseFeg 9)
0xa9f7713f1ac04b5c5b9f92d5a91228bd422256c2
0x72a2f4d33a52d522656d958a4183198de513d0ca
0xf1662adf6d4d6de9d39f44e13f19db268ff3c01d
0xdf098b09a4f3f73918d2fa1b58bb46581f95cfa1
0x920b41c3ea02469b970d7e81608d98a1a58e6beb

(A total of 7,919,582,129.42 tokens held by the top 100 accounts from the total supply of 10,000,000,000.00 token)

PulseFeg Contract Interaction Details



Time Series: Token Contract Overview

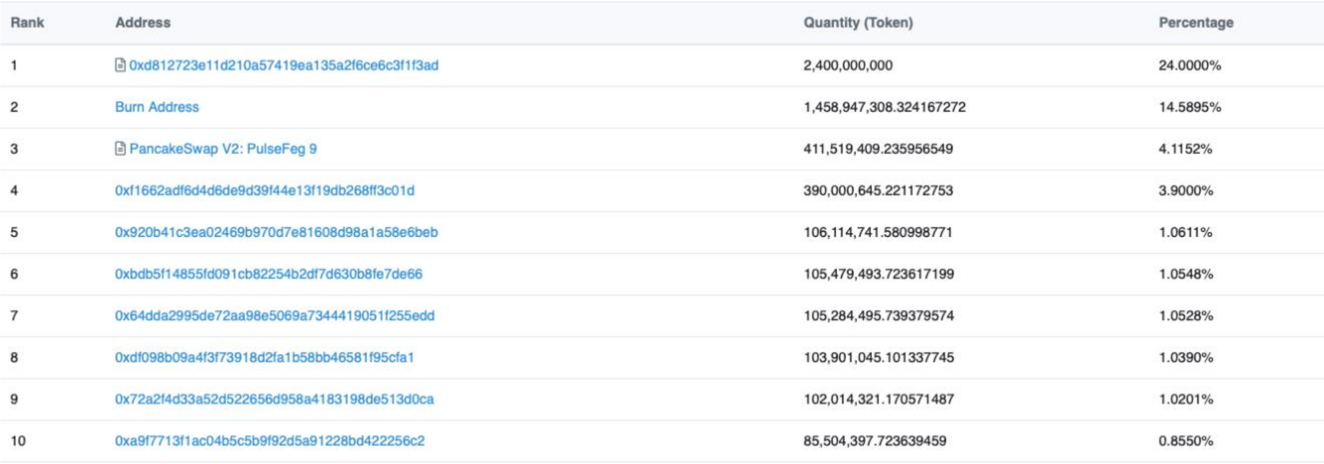
Sun 31, Oct 2021 - Sat 6, Nov 2021

Token Contract 0x1e5dd94a6d7190ab77f834e2ccdf9072597ae4e3 (PulseFeg)

Source: BscScan.com

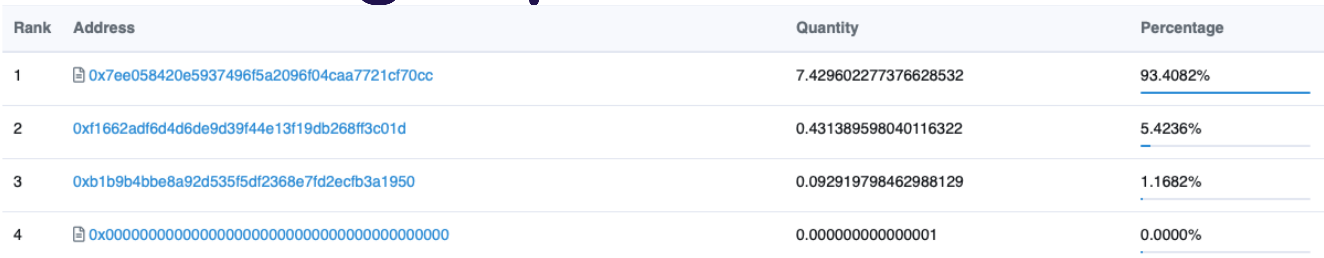
From Oct 30, 2021 To Nov 6, 2021

PulseFeg Top 10 Token Holders



Rank	Address	Quantity (Token)	Percentage
1	0xd812723e11d210a57419ea135a2f6ce6c3f1f3ad	2,400,000,000	24.0000%
2	Burn Address	1,458,947,308.324167272	14.5895%
3	PancakeSwap V2: PulseFeg 9	411,519,409.235956549	4.1152%
4	0xf1662adf6d4d6de9d39f44e13f19db268ff3c01d	390,000,645.221172753	3.9000%
5	0x920b41c3ea02469b970d7e81608d98a1a58e6beb	106,114,741.580998771	1.0611%
6	0xbdb5f14855fd091cb82254b2df7d630b8fe7de66	105,479,493.723617199	1.0548%
7	0x64dda2995de72aa98e5069a7344419051f255edd	105,284,495.739379574	1.0528%
8	0xdf098b09a4f3f73918d2fa1b58bb46581f95cfa1	103,901,045.101337745	1.0390%
9	0x72a2f4d33a52d522656d958a4183198de513d0ca	102,014,321.170571487	1.0201%
10	0xa9f7713f1ac04b5c5b9f92d5a91228bd422256c2	85,504,397.723639459	0.8550%

PulseFeg Top LP Token Holders



Rank	Address	Quantity	Percentage
1	0x7ee058420e5937496f5a2096f04caa7721cf70cc	7.429602277376628532	93.4082%
2	0xf1662adf6d4d6de9d39f44e13f19db268ff3c01d	0.431389598040116322	5.4236%
3	0xb1b9b4bbe8a92d535f5df2368e7fd2ecfb3a1950	0.092919798462988129	1.1682%
4	0x0000000000000000000000000000000000000000	0.000000000000001	0.0000%

Contract functions details

```
+  Context
   - [Int] _msgSender
   - [Int] _msgData
+ [Int] IERC20
   - [Ext] totalSupply
   - [Ext] balanceOf
   - [Ext] transfer #
   - [Ext] allowance
   - [Ext] approve #
   - [Ext] transferFrom #
 +  Ownable (Context)
   - [Pub] <Constructor> #
   - [Pub] owner
   - [Pub] renounceOwnership #
     - modifiers: onlyOwner
   - [Pub] transferOwnership #
     - modifiers: onlyOwner
+ [Int] IUniswapV2Factory
   - [Ext] createPair #
 + [Int] IUniswapV2Router01
   - [Ext] factory
   - [Ext] WETH
   - [Ext] swapETHForExactTokens ($)
 + [Int] IUniswapV2Router02 (IUniswapV2Router01)
   - [Ext] swapExactETHForTokensSupportingFeeOnTransferTokens ($)
   - [Ext] swapExactTokensForETHSupportingFeeOnTransferTokens #

 +  PulseFeg (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] buybackThresholdAmount
   - [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] _tokenTransfer #
- [Prv] _transferStandard #
- [Prv] _transferToExcluded #
- [Prv] _transferFromExcluded #
- [Prv] _transferBothExcluded #
- [Prv] _reflectFee #
- [Prv] _getValues
- [Prv] _getTValues
- [Prv] _getRValues
- [Prv] _getRate
- [Prv] _getCurrentSupply
- [Prv] _takeSwap #
- [Prv] calculateTaxFee
- [Prv] calculateSwapFee
- [Prv] removeAllFee #
- [Prv] restoreAllFee #
- [Pub] isExcludedFromFee
- [Pub] excludeFromFee #
  - modifiers: onlyOwner
- [Pub] includeInFee #
  - modifiers: onlyOwner
- [Ext] setTaxFeePercent #
  - modifiers: onlyOwner
- [Ext] setSwapFeePercent #
  - modifiers: onlyOwner
- [Ext] setMarketingFee #
  - modifiers: onlyOwner
- [Ext] setMarketingAddress #
  - modifiers: onlyOwner
- [Ext] setSellFees #
  - modifiers: onlyOwner
- [Ext] setMaxTxAmount #
  - modifiers: onlyOwner
- [Ext] setNumTokensSellToAddToBuyback #
  - modifiers: onlyOwner
- [Ext] setSwapUpperLimit #
  - modifiers: onlyOwner
- [Pub] setSwapAndLiquifyEnabled #
  - modifiers: onlyOwner
- [Pub] setSwapEnabled #
  - modifiers: onlyOwner
- [Ext] transferToAddress #
  - modifiers: onlyOwner
- [Ext] <Fallback> ($)

($) = 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

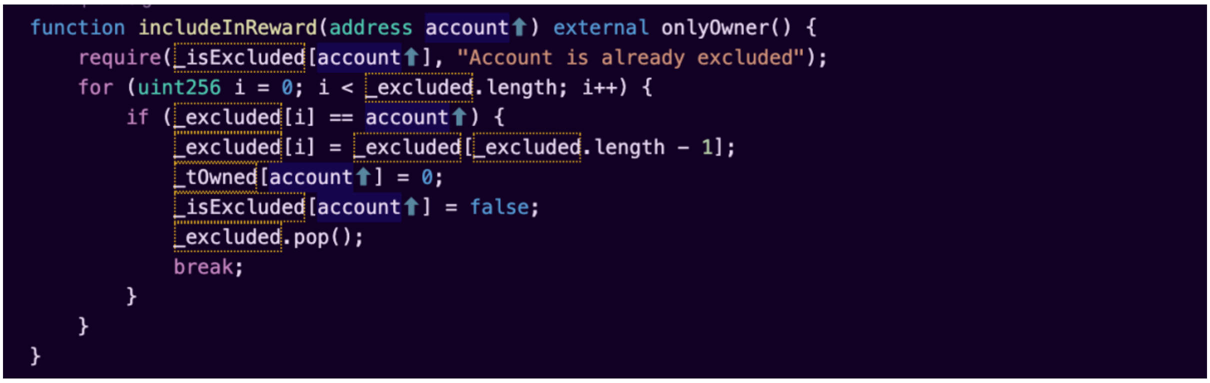
No medium severity issues found.

Low Severity Issues

1. Out of gas

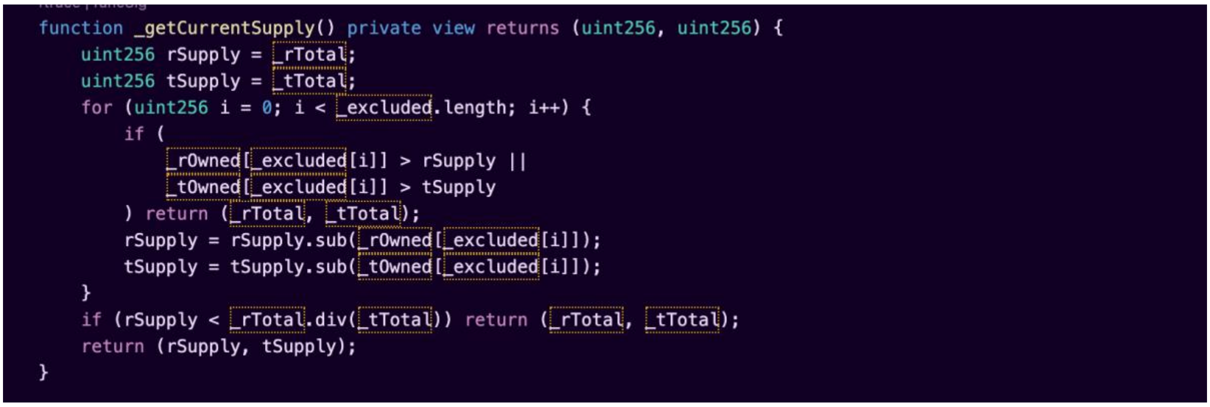
Issue:

- 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.



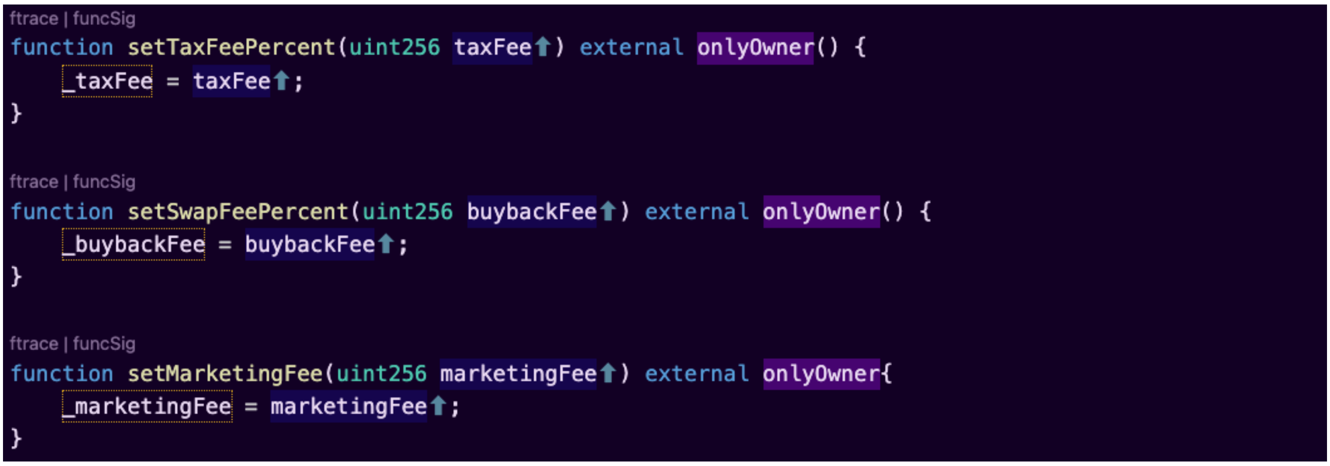
```
function _getCurrentSupply() private view returns (uint256, uint256) {
    uint256 rSupply = _rTotal;
    uint256 tSupply = _tTotal;
    for (uint256 i = 0; i < _excluded.length; i++) {
        if (
            _rOwned[_excluded[i]] > rSupply ||
            _tOwned[_excluded[i]] > tSupply
      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

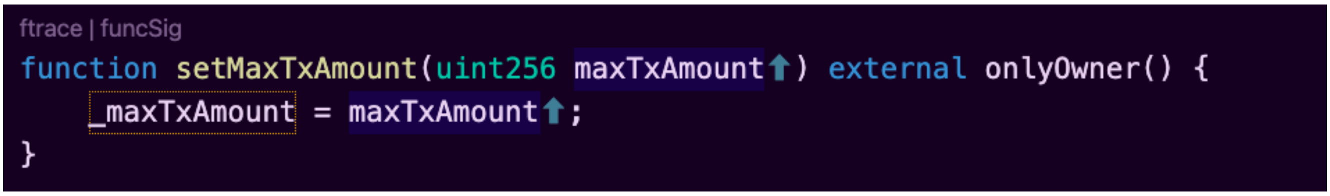
Owner privileges (In the period when the owner is not renounced)

- Owner can change tax, swap and marketing fees.



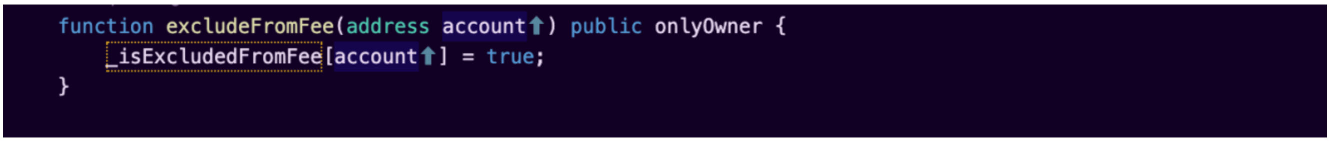
```
ftrace | funcSig
function setTaxFeePercent(uint256 taxFee) external onlyOwner() {
    _taxFee = taxFee;
}

ftrace | funcSig
function setSwapFeePercent(uint256 buybackFee) external onlyOwner() {
    _buybackFee = buybackFee;
}

ftrace | funcSig
function setMarketingFee(uint256 marketingFee) external onlyOwner{
    _marketingFee = marketingFee;
}
```

- Owner can change maximum transaction amount.



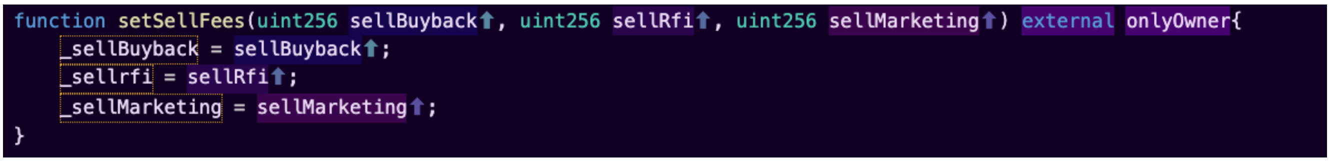
```
ftrace | funcSig
function setMaxTxAmount(uint256 maxTxAmount) external onlyOwner() {
    _maxTxAmount = maxTxAmount;
}
```

- Owner can exclude from the fee.



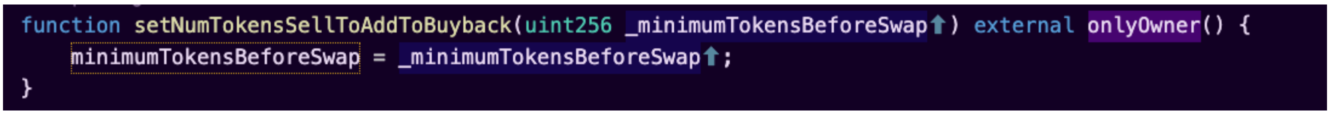
```
    function excludeFromFee(address account) public onlyOwner {
        _isExcludedFromFee[account] = true;
    }
```

- Owner can change sell fees.



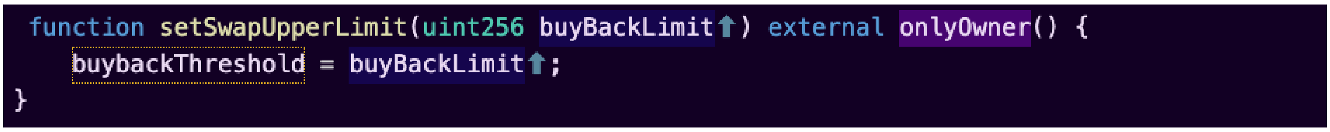
```
function setSellFees(uint256 sellBuyback, uint256 sellRfi, uint256 sellMarketing) external onlyOwner{
    _sellBuyback = sellBuyback;
    _sellrfi = sellRfi;
    _sellMarketing = sellMarketing;
}
```

- Owner can change minimum number of tokens to add to liquidity.



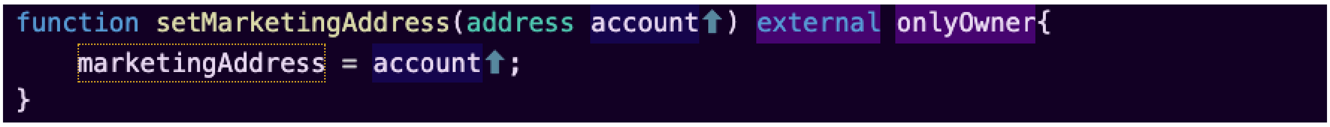
```
function setNumTokensSellToAddToBuyback(uint256 _minimumTokensBeforeSwap) external onlyOwner() {
    minimumTokensBeforeSwap = _minimumTokensBeforeSwap;
}
```

- Owner can change buybackThreshold.



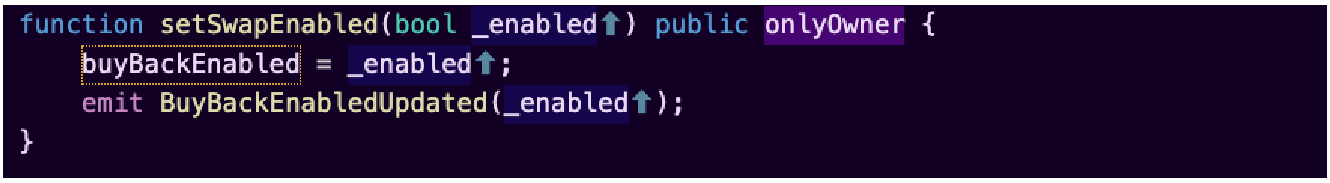
```
function setSwapUpperLimit(uint256 buyBackLimit) external onlyOwner() {
    buybackThreshold = buyBackLimit;
}
```

- Owner can change marketing address.



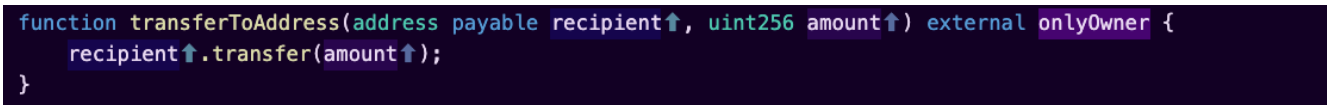
```
function setMarketingAddress(address account) external onlyOwner{
    marketingAddress = account;
}
```

- Owner can enable and disable buyBack.



```
function setSwapEnabled(bool _enabled) public onlyOwner {
    buyBackEnabled = _enabled;
    emit BuyBackEnabledUpdated(_enabled);
}
```

- Owner can withdraw BNBs.



```
function transferToAddress(address payable recipient, uint256 amount) external onlyOwner {
    recipient.transfer(amount);
}
```

Conclusion

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

Liquidity locking details provided by the team:
https://www.pinksale.finance/#/pinklock/record/964?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.