TechRate
Blockchain solutions and consulting

Smart Contract Security Audit

Audit details:

Audited project:	Unifarm
Deployer address:	0xcea56632d348259e24e42f2a8bd6aee704103e68
Client contacts:	Unifarm team
Blockchain:	Binance Smart Chain
Project website:	https://unifarm.io

April, 2021
TechRate

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 Unifarm to perform an audit of smart contracts:

- *https://bscscan.com/address/0x18d883f6647cb3195f55eb93bf9ee8ae824e3a6f#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.

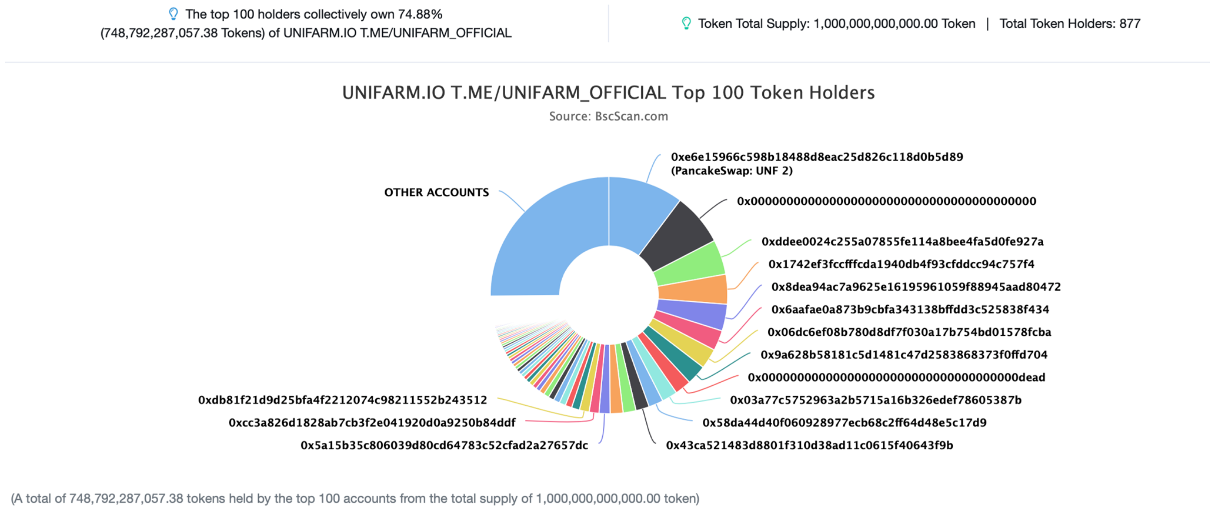
The information in this report should be used to understand the risk exposure of the smart contract, and as a guide to improve the security posture of the smart contract by remediating the issues that were identified.

Contracts details

Token contract details for 15.04.2021.

Contract name:	UNIFARM.IO T.ME/UNIFARM_OFFICIAL
Contract address:	0x18d883f6647cb3195f55eb93bf9ee8ae824e3a6f
Total supply:	1_000_000_000_000_000_000_000
Token ticker:	UNF
Decimals:	9
Token holders:	877
Transactions count:	7978
Top 100 holders dominance:	74.88 %
Contract deployer address:	0xcea56632d348259e24e42f2a8bd6aee704103e68
Contract's current owner address:	Zero address
Current liquidity fee:	3 percent
Current tax fee:	3 percent
Current charity fee:	1 percent
Current burn fee:	1 percent
Total fees:	180_748_765_012_856_256_229
Uniswap V2 pair:	0xe6e15966c598b18488d8eac25d826c118d0b5d89
Uniswap V2 router:	0x05ff2b0db69458a0750badebc4f9e13add608c7f
Max transaction amount:	1_000_000_000_000_000_000_000
Deployed at transaction:	0x67d35ea69f0115dd0be9c1632dd14c3ac58752d238df5226a044b10975ccb4fc

Unifarm token distribution



The top 100 holders collectively own 74.88%
(748,792,287,057.38 Tokens) of UNIFARM.IO T.ME/UNIFARM_OFFICIAL

Token Total Supply: 1,000,000,000,000.00 Token | Total Token Holders: 877

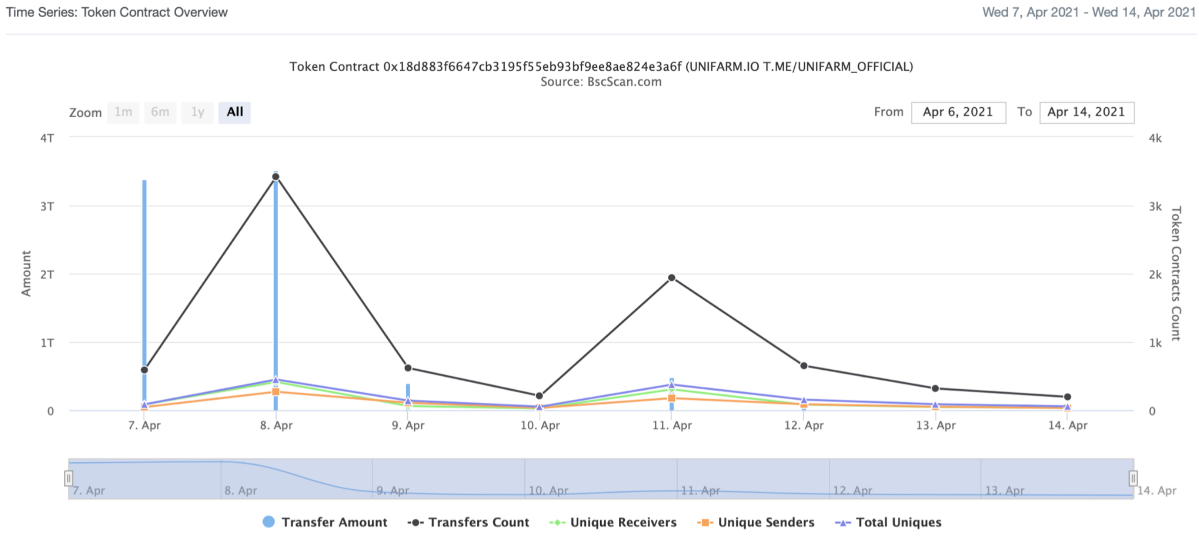
UNIFARM.IO T.ME/UNIFARM_OFFICIAL Top 100 Token Holders

Source: BscScan.com

0xe6e15966c598b18488d8eac25d826c118d0b5d89
(PancakeSwap: UNF 2)
OTHER ACCOUNTS
0x0000000000000000000000000000000000000000
0xddee0024c255a07855fe114a8bee4fa5d0fe927a
0x1742ef3fccfffcda1940db4f93cfddcc94c757f4
0x8dea94ac7a9625e16195961059f88945aad80472
0x6aafae0a873b9cbfa343138bffdd3c525838f434
0x06dc6ef08b780d8df7f030a17b754bd01578fcba
0x9a628b58181c5d1481c47d2583868373f0ffd704
0x000000000000000000000000000000000000dead
0xdb81f21d9d25bfa4f2212074c98211552b243512
0x03a77c5752963a2b5715a16b326edef78605387b
0xcc3a826d1828ab7cb3f2e041920d0a9250b84ddf
0x58da44d40f060928977ecb68c2ff64d48e5c17d9
0x5a15b35c806039d80cd64783c52cfad2a27657dc
0x43ca521483d8801f310d38ad11c0615f40643f9b

(A total of 748,792,287,057.38 tokens held by the top 100 accounts from the total supply of 1,000,000,000,000.00 token)

Unifarm contract interaction details



Time Series: Token Contract Overview

Wed 7, Apr 2021 - Wed 14, Apr 2021

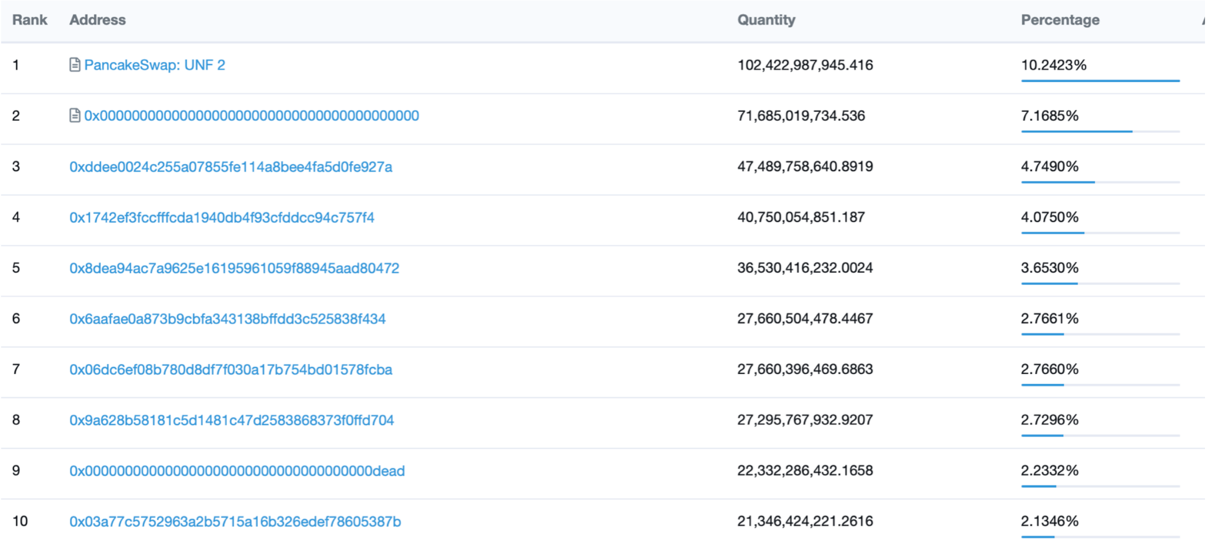
Token Contract 0x18d883f6647cb3195f55eb93bf9ee8ae824e3a6f (UNIFARM.IO T.ME/UNIFARM_OFFICIAL)

Source: BscScan.com

Zoom 1m 6m 1y All

From Apr 6, 2021 To Apr 14, 2021

Unifarm top 10 token holders



Rank	Address	Quantity	Percentage
1	PancakeSwap: UNF 2	102,422,987,945.416	10.2423%
2	0x0000000000000000000000000000000000000000	71,685,019,734.536	7.1685%
3	0xddee0024c255a07855fe114a8bee4fa5d0fe927a	47,489,758,640.8919	4.7490%
4	0x1742ef3fccfffcda1940db4f93cfddcc94c757f4	40,750,054,851.187	4.0750%
5	0x8dea94ac7a9625e16195961059f88945aad80472	36,530,416,232.0024	3.6530%
6	0x6aafae0a873b9cbfa343138bffdd3c525838f434	27,660,504,478.4467	2.7661%
7	0x06dc6ef08b780d8df7f030a17b754bd01578fcba	27,660,396,469.6863	2.7660%
8	0x9a628b58181c5d1481c47d2583868373f0ffd704	27,295,767,932.9207	2.7296%
9	0x000000000000000000000000000000000000dead	22,332,286,432.1658	2.2332%
10	0x03a77c5752963a2b5715a16b326edef78605387b	21,346,424,221.2616	2.1346%

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
  - [Pub] geUnlockTime
  - [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 #
  - [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 #

+  UNIFARM (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] deliver #
  - [Pub] reflectionFromToken
  - [Pub] tokenFromReflection
  - [Pub] excludeFromReward # - modifiers: onlyOwner
  - [Ext] includeInReward # - modifiers: onlyOwner
  - [Prv] _transferBothExcluded #
  - [Pub] excludeFromFee # - modifiers: onlyOwner
  - [Pub] includeInFee # - 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 #
  - [Pub] isExcludedFromFee
  - [Prv] _approve #
  - [Prv] _transfer #
  - [Prv] swapAndLiquify # - modifiers: lockTheSwap
  - [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

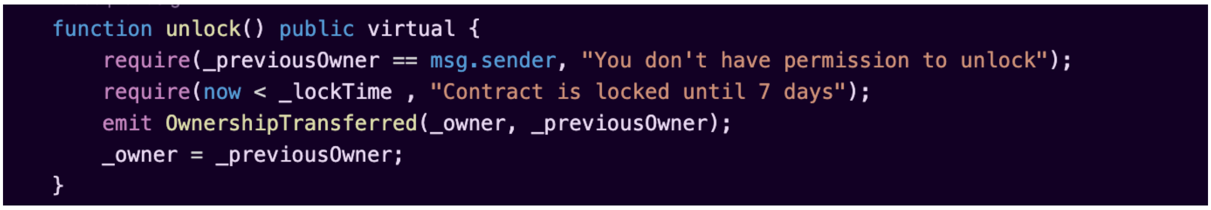
Security Issues

High Severity Issues

1. Unlock until lock finish

Issue:

Owner can unlock the contract earlier than lock ends.



```
function unlock() public virtual {
    require(_previousOwner == msg.sender, "You don't have permission to unlock");
    require(now < _lockTime , "Contract is locked until 7 days");
    emit OwnershipTransferred(_owner, _previousOwner);
    _owner = _previousOwner;
}
```

Recommendation:

There should be checking that now is greater than _lockTime.

Fix:

[Ownership renounced.](#)

Medium Severity Issues

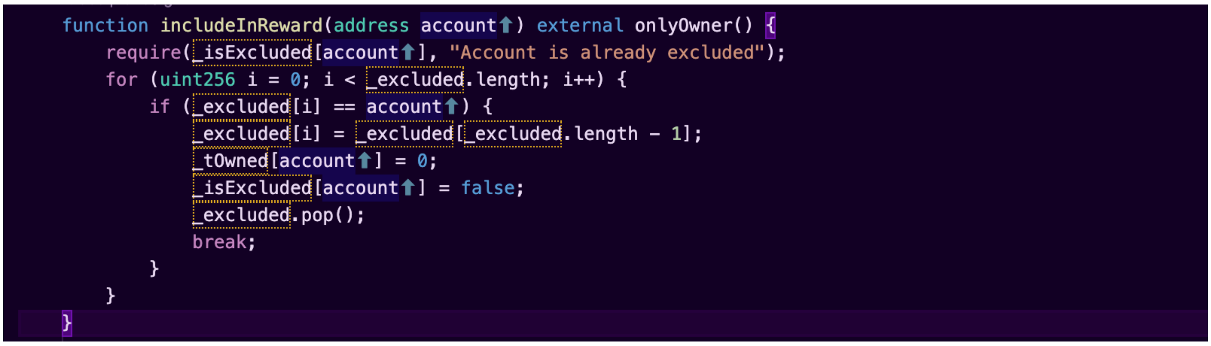
No medium severity issues found.

Low Severity Issues

1. Out of gas

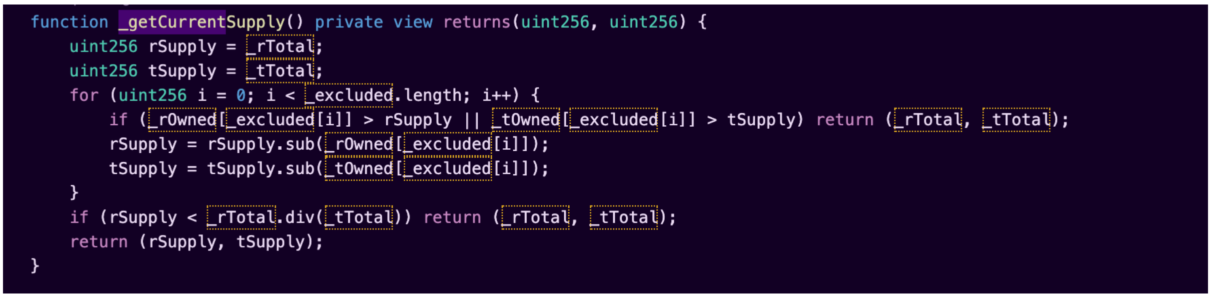
Issue:

❏ 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);
}
```

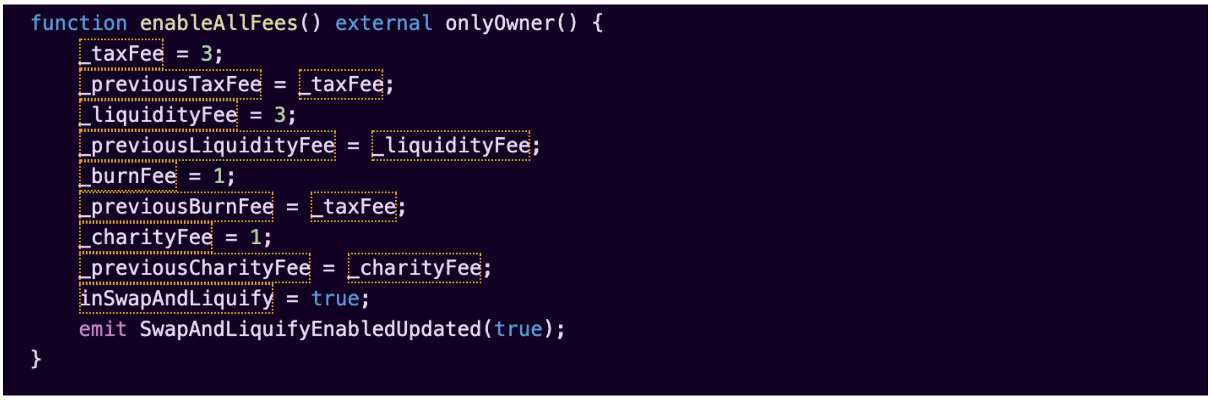
Recommendation:

Use EnumerableSet instead of array or do not use long arrays.

Owner privileges

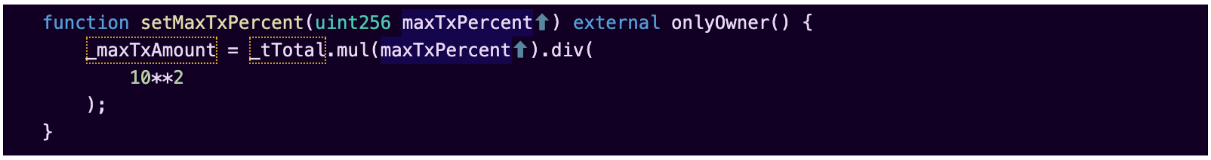
1. Owner privileges

❑ Owner can enable all fees and enable swap and liquidfy.



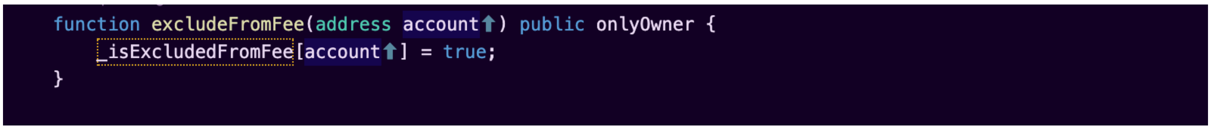
```
function enableAllFees() external onlyOwner() {
    _taxFee = 3;
    _previousTaxFee = _taxFee;
    _liquidityFee = 3;
    _previousLiquidityFee = _liquidityFee;
    _burnFee = 1;
    _previousBurnFee = _taxFee;
    _charityFee = 1;
    _previousCharityFee = _charityFee;
    inSwapAndLiquify = true;
    emit SwapAndLiquifyEnabledUpdated(true);
}
```

❑ Owner can change the maximum transaction amount.



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

❑ Owner can exclude from the fee.



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

Conclusion

Smart contracts contain high severity issues, which is fixed. Ownership renounced.

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.