Smart Contract Security Audit

Audit details:

Audited project:	LonelyFans
Deployer address:	0x10cd8079755bc23b7e644f60627478e62e8817d5
Client contacts:	LonelyFans team
Blockchain:	Binance Smart Chain
Project website:	http://lonelyfans.me

May, 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 LonelyFans to perform an audit of smart contracts:

- *https://bscscan.com/address/0xb3225ac90b741f762beca76dea1ead278ef26a96#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.

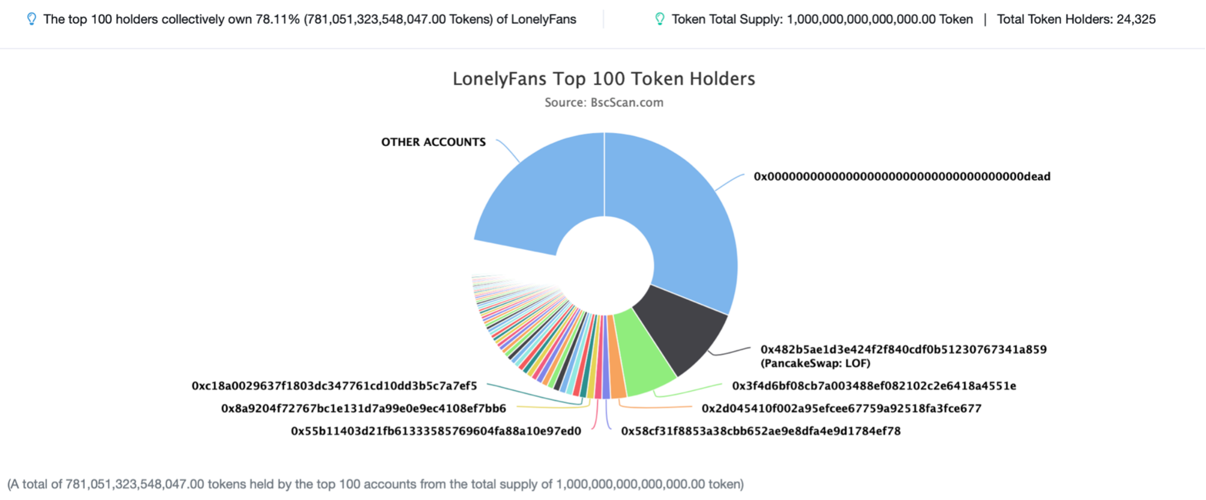
The information in this report should be used to understand the risk exposure of the smart contract, and as a guide to improve the security posture of the smart contract by remediating the issues that were identified.

Contracts details

Token contract details for 04.05.2021.

Contract name:	LonelyFans
Contract address:	0xb3225ac90b741f762beca76dea1ead278ef26a96
Total supply:	1_000_000_000_000_000_000_000_000
Token ticker:	LOF
Decimals:	9
Token holders:	24325
Transactions count:	76290
Top 100 holders dominance:	78.11 %
Liquidity fee:	3
Tax fee:	3
Total fees:	95_766_046_498_093_491_068_714
Uniswap V2 pair:	0x482b5ae1d3e424f2f840cdf0b51230767341a859
Contract deployer address:	0x10cd8079755bc23b7e644f60627478e62e8817d5
Contract’s current owner address:	0x0000000000000000000000000000000000000000

LonelyFans token distribution



The top 100 holders collectively own 78.11% (781,051,323,548,047.00 Tokens) of LonelyFans | Token Total Supply: 1,000,000,000,000,000.00 Token | Total Token Holders: 24,325

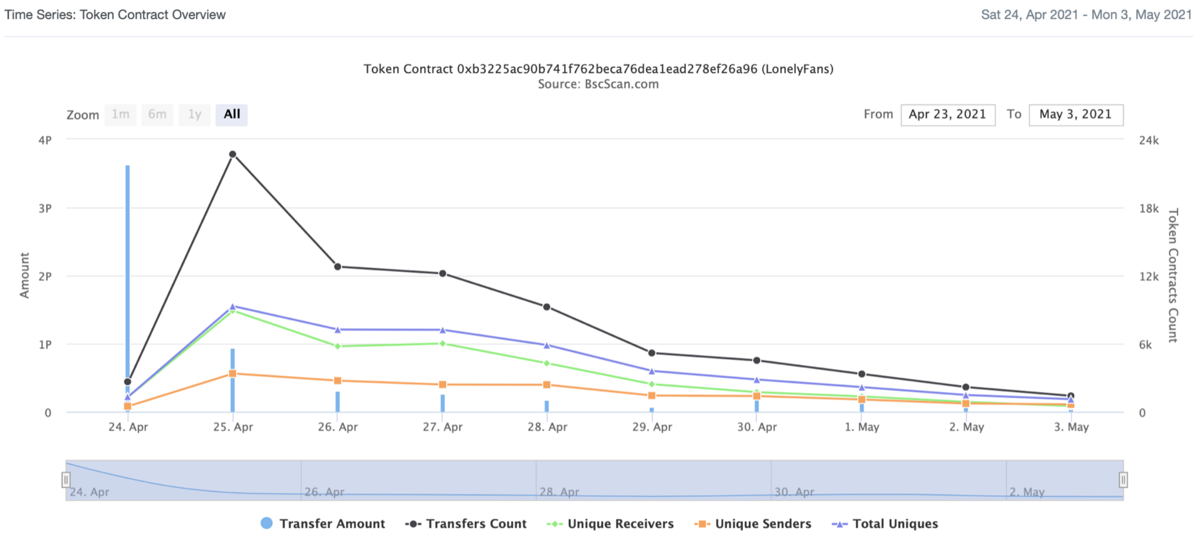
LonelyFans Top 100 Token Holders

Source: BscScan.com

OTHER ACCOUNTS
0x000000000000000000000000000000000000dead
0x482b5ae1d3e424f2f840cdf0b51230767341a859 (PancakeSwap: LOF)
0xc18a0029637f1803dc347761cd10dd3b5c7a7ef5
0x3f4d6bf08cb7a003488ef082102c2e6418a4551e
0x8a9204f72767bc1e131d7a99e0e9ec4108ef7bb6
0x2d045410f002a95efcee67759a92518fa3fce677
0x55b11403d21fb61333585769604fa88a10e97ed0
0x58cf31f8853a38cbb652ae9e8dfa4e9d1784ef78

(A total of 781,051,323,548,047.00 tokens held by the top 100 accounts from the total supply of 1,000,000,000,000,000.00 token)

LonelyFans contract interaction details



Time Series: Token Contract Overview

Sat 24, Apr 2021 - Mon 3, May 2021

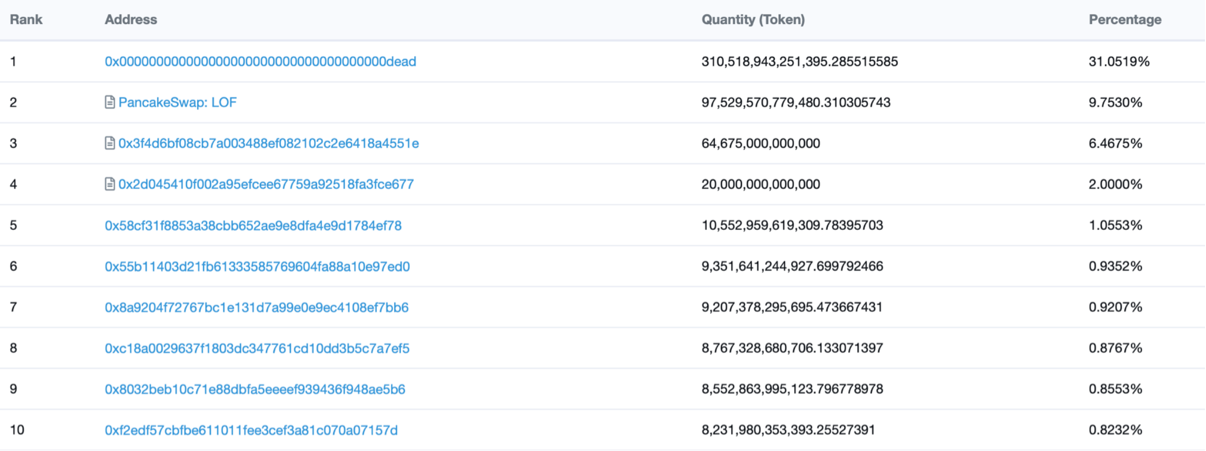
Token Contract 0xb3225ac90b741f762beca76dea1ead278ef26a96 (LonelyFans)

Source: BscScan.com

Zoom 1m 6m 1y All

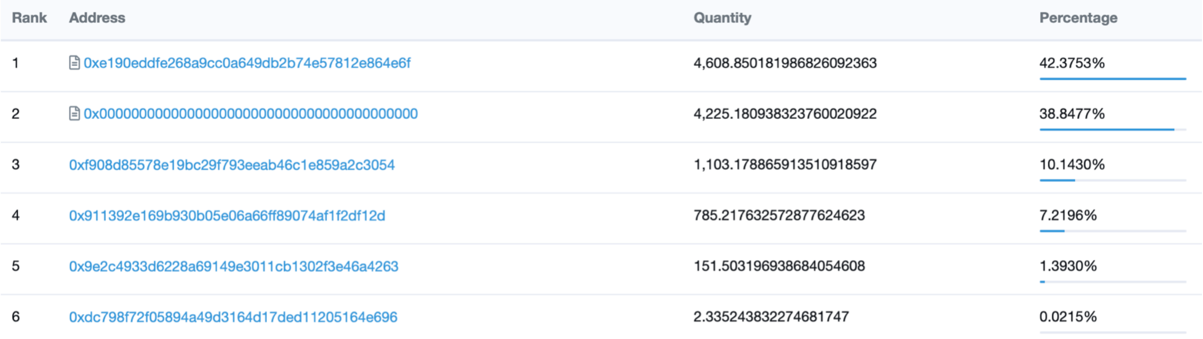
From Apr 23, 2021 To May 3, 2021

LonelyFans top 10 token holders



Rank	Address	Quantity (Token)	Percentage
1	0x000000000000000000000000000000000000dead	310,518,943,251,395.285515585	31.0519%
2	PancakeSwap: LOF	97,529,570,779,480.310305743	9.7530%
3	0x3f4d6bf08cb7a003488ef082102c2e6418a4551e	64,675,000,000,000	6.4675%
4	0x2d045410f002a95efcee67759a92518fa3fce677	20,000,000,000,000	2.0000%
5	0x58cf31f8853a38cbb652ae9e8dfa4e9d1784ef78	10,552,959,619,309.78395703	1.0553%
6	0x55b11403d21fb61333585769604fa88a10e97ed0	9,351,641,244,927.699792466	0.9352%
7	0x8a9204f72767bc1e131d7a99e0e9ec4108ef7bb6	9,207,378,295,695.473667431	0.9207%
8	0xc18a0029637f1803dc347761cd10dd3b5c7a7ef5	8,767,328,680,706.133071397	0.8767%
9	0x8032beb10c71e88dbfa5eeeef939436f948ae5b6	8,552,863,995,123.796778978	0.8553%
10	0xf2edf57cbfbe611011fee3cef3a81c070a07157d	8,231,980,353,393.25527391	0.8232%

LonelyFans LP token holders



Rank	Address	Quantity	Percentage
1	0xe190eddfe268a9cc0a649db2b74e57812e864e6f	4,608.850181986826092363	42.3753%
2	0x0000000000000000000000000000000000000000	4,225.180938323760020922	38.8477%
3	0xf908d85578e19bc29f793eeab46c1e859a2c3054	1,103.178865913510918597	10.1430%
4	0x911392e169b930b05e06a66ff89074af1f2df12d	785.217632572877624623	7.2196%
5	0x9e2c4933d6228a69149e3011cb1302f3e46a4263	151.503196938684054608	1.3930%
6	0xdc798f72f05894a49d3164d17ded11205164e696	2.335243832274681747	0.0215%

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 #

+ LonelyFans (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] 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] 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.	High issues
19	Cross-function race conditions.	Passed
20	Safe Open Zeppelin contracts implementation and usage.	Passed
21	Fallback function security.	Passed

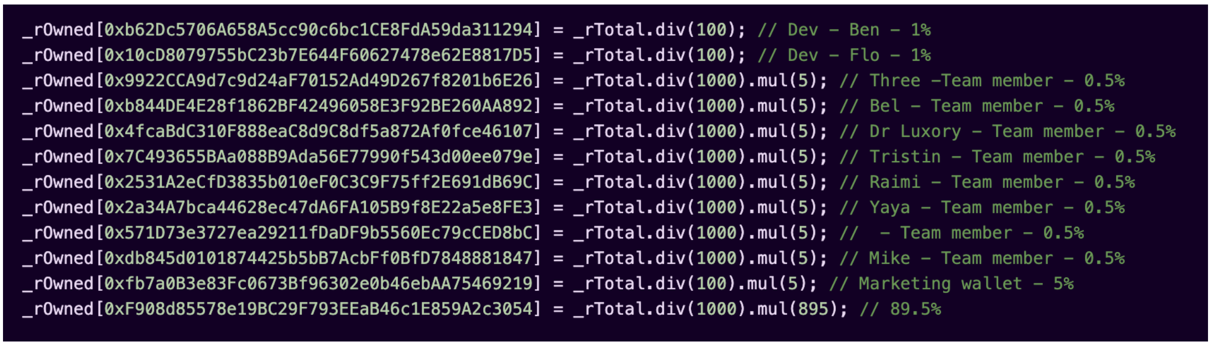
Security Issues

High Severity Issues

1. More tokens than 100% distributed

Issue:

There is a wrong tokens distribution in the constructor of the contract. Total distributed tokens in the constructor will be the 100.5% from the total supply! (1 + 1 + 0.5 * 8 + 5 + 89.5 = 100.5)



```
_rOwned[0xb62Dc5706A658A5cc90c6bc1CE8FdA59da311294] = _rTotal.div(100); // Dev - Ben - 1%
_rOwned[0x10cD8079755bC23b7E644F60627478e62E8817D5] = _rTotal.div(100); // Dev - Flo - 1%
_rOwned[0x9922CCA9d7c9d24aF70152Ad49D267f8201b6E26] = _rTotal.div(1000).mul(5); // Three -Team member - 0.5%
_rOwned[0xb844DE4E28f1862BF42496058E3F92BE260AA892] = _rTotal.div(1000).mul(5); // Bel - Team member - 0.5%
_rOwned[0x4fcaBdC310F888eaC8d9C8df5a872Af0fce46107] = _rTotal.div(1000).mul(5); // Dr Luxory - Team member - 0.5%
_rOwned[0x7C493655BAa088B9Ada56E77990f543d00ee079e] = _rTotal.div(1000).mul(5); // Tristin - Team member - 0.5%
_rOwned[0x2531A2eCfD3835b010eF0C3C9F75ff2E691dB69C] = _rTotal.div(1000).mul(5); // Raimi - Team member - 0.5%
_rOwned[0x2a34A7bca44628ec47dA6FA105B9f8E22a5e8FE3] = _rTotal.div(1000).mul(5); // Yaya - Team member - 0.5%
_rOwned[0x571D73e3727ea29211fDaDF9b5560Ec79cCED8bC] = _rTotal.div(1000).mul(5); //  - Team member - 0.5%
_rOwned[0xdb845d0101874425b5bB7AcbFf0BfD7848881847] = _rTotal.div(1000).mul(5); // Mike - Team member - 0.5%
_rOwned[0xfb7a0B3e83Fc0673Bf96302e0b46ebAA75469219] = _rTotal.div(100).mul(5); // Marketing wallet - 5%
_rOwned[0xF908d85578e19BC29F793EEaB46c1E859A2c3054] = _rTotal.div(1000).mul(895); // 89.5%
```

Recommendation:

Please recheck the logic of the tokens distribution. Also see the low severity issue with wrong events!

Medium Severity Issues

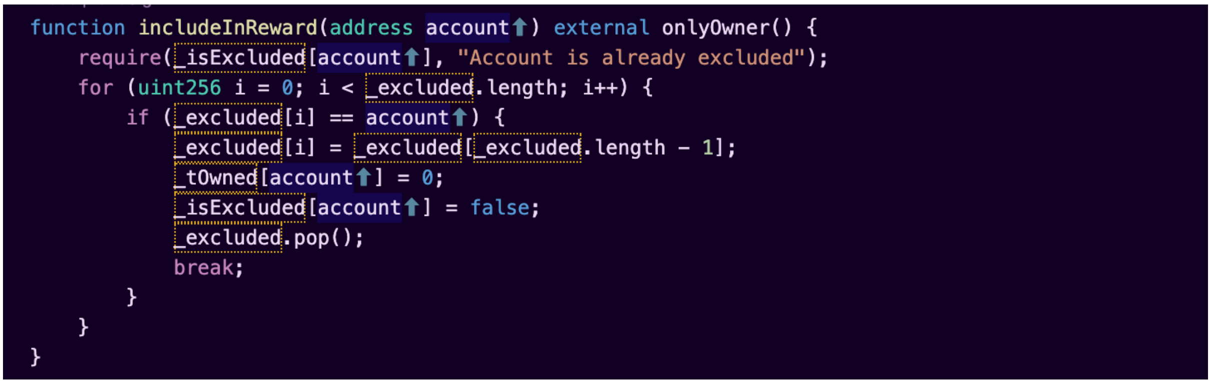
No medium severity issues found.

Low Severity Issues

1. Out of gas

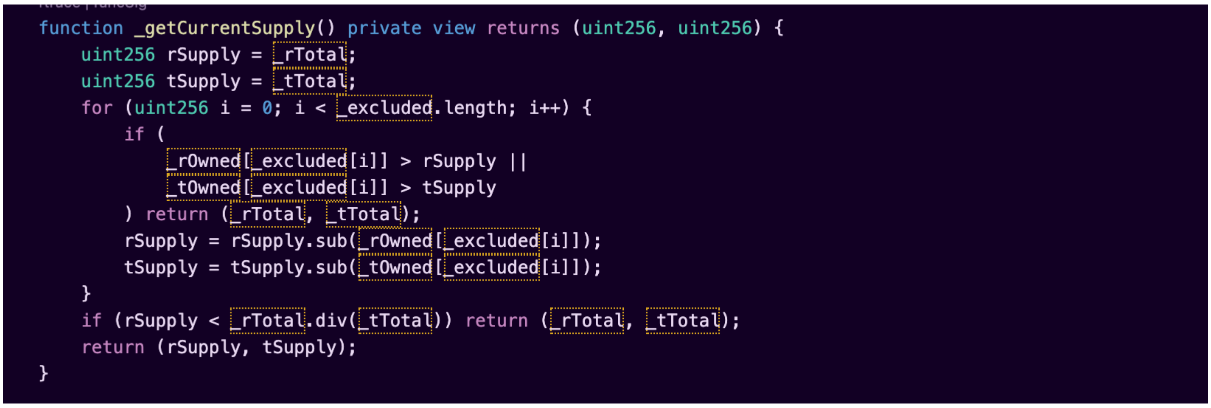
Issue:

❏ 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);
}
```

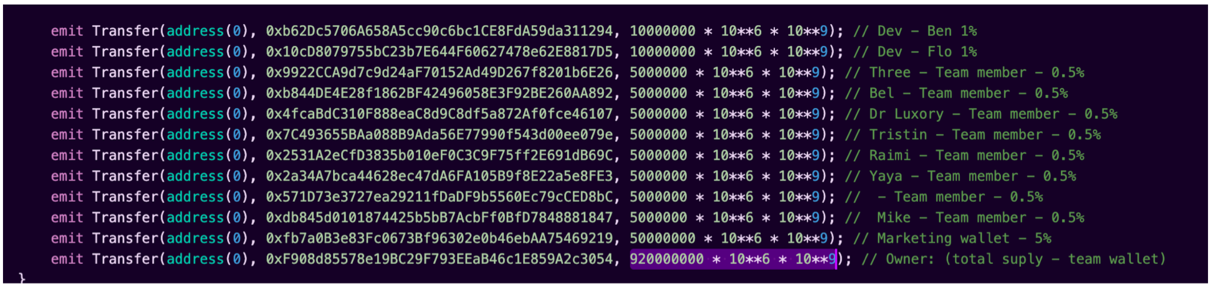
Recommendation:

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

2. Wrong Transfer event

Issue:

There is a wrong Transfer event in the constructor of the contract, where the tokens are distributed through team members and the owner. This event shows that the owner received about 92 percent of the total tokens, but he received only the 89.5 percent which is also wrong (Look HIGH severity issues.)



```
    emit Transfer(address(0), 0xb62Dc5706A658A5cc90c6bc1CE8FdA59da311294, 10000000 * 10**6 * 10**9); // Dev - Ben 1%
    emit Transfer(address(0), 0x10cD8079755bC23b7E644F60627478e62E8817D5, 10000000 * 10**6 * 10**9); // Dev - Flo 1%
    emit Transfer(address(0), 0x9922CCA9d7c9d24aF70152Ad49D267f8201b6E26, 5000000 * 10**6 * 10**9); // Three - Team member - 0.5%
    emit Transfer(address(0), 0xb844DE4E28f1862BF42496058E3F92BE260AA892, 5000000 * 10**6 * 10**9); // Bel - Team member - 0.5%
    emit Transfer(address(0), 0x4fcaBdC310F888eaC8d9C8df5a872Af0fce46107, 5000000 * 10**6 * 10**9); // Dr Luxory - Team member - 0.5%
    emit Transfer(address(0), 0x7C493655BAa088B9Ada56E77990f543d00ee079e, 5000000 * 10**6 * 10**9); // Tristin - Team member - 0.5%
    emit Transfer(address(0), 0x2531A2eCfD3835b010eF0C3C9F75ff2E691dB69C, 5000000 * 10**6 * 10**9); // Raimi - Team member - 0.5%
    emit Transfer(address(0), 0x2a34A7bca44628ec47dA6FA105B9f8E22a5e8FE3, 5000000 * 10**6 * 10**9); // Yaya - Team member - 0.5%
    emit Transfer(address(0), 0x571D73e3727ea29211fDaDF9b5560Ec79cCED8bC, 5000000 * 10**6 * 10**9); //  - Team member - 0.5%
    emit Transfer(address(0), 0xdb845d0101874425b5bB7AcbFf0BfD7848881847, 5000000 * 10**6 * 10**9); //  Mike - Team member - 0.5%
    emit Transfer(address(0), 0xfb7a0B3e83Fc0673Bf96302e0b46ebAA75469219, 50000000 * 10**6 * 10**9); // Marketing wallet - 5%
    emit Transfer(address(0), 0xF908d85578e19BC29F793EEaB46c1E859A2c3054, 920000000 * 10**6 * 10**9); // Owner: (total suply - team wallet)
}
```

Recommendation:

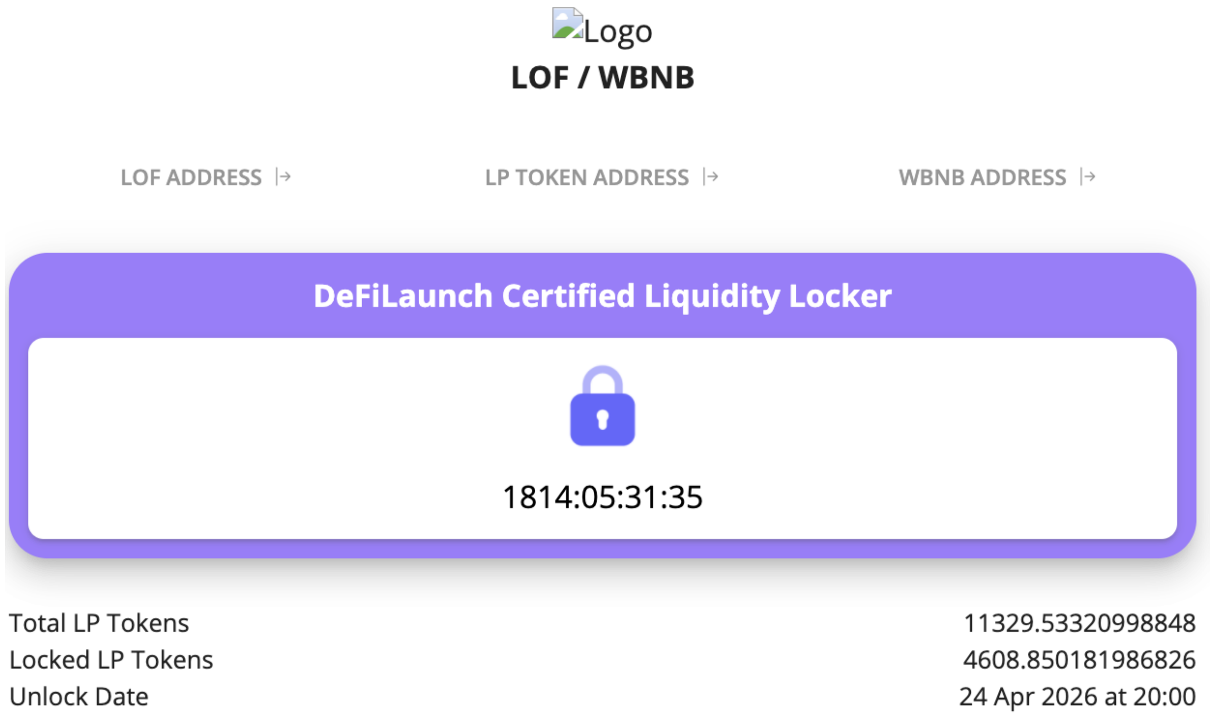
Please recheck the logic of distribution.

Conclusion

Smart contracts contain high severity issues! Lliquidity pair contract's security is not checked.

Sale details on DXSale could be found by the link - https://dxsale.app/app/pages/defipresalev1?saleID=1646&chain=BSC

DXSale locking details could be found by the link - https://dxsale.app/app/pages/dxlockviewv1?id=1646&add=0&type=lpdefi&chain=BSC



Logo

LOF / WBNB

LOF ADDRESS LP TOKEN ADDRESS WBNB ADDRESS

DeFiLaunch Certified Liquidity Locker

1814:05:31:35

Total LP Tokens	11329.53320998848
Locked LP Tokens	4608.850181986826
Unlock Date	24 Apr 2026 at 20:00

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.