

TechRate
May, 2022



SMART CONTRACTS SECURITY AUDIT REPORT



Techrate_audits



Techrate



Techrate1

Audit Details



Audited project

Lil Dragon



Deployer address

0x384695239a0a957674f2c7694c0a683c9c1a86f8



Client contacts:

Lil Dragon 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 Lil Dragon to perform an audit of smart contracts:

<https://bscscan.com/address/0x67BdcD2CAba8F26A37759CeE37B8b922a473C125#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 02.05.2022

Contract name Lil Dragon

Contract address 0x67BdcD2CAba8F26A37759CeE37B8b922a473C125

Total supply 1,000,000,000,000

Token ticker LDG

Decimals 9

Token holders 4

Transactions count 8

Top 100 holders dominance 100.00%

Total fees 0

Liquidity fee 700

Tax fee 200

Uniswap V2 pair 0x9ea7397b59dba369fcd9f257041284169d950aa7

Contract deployer address 0x384695239a0a957674f2c7694c0a683c9c1a86f8

Owner address 0x2f93129b2e56223c3d7a5b549638cd326be9b23a

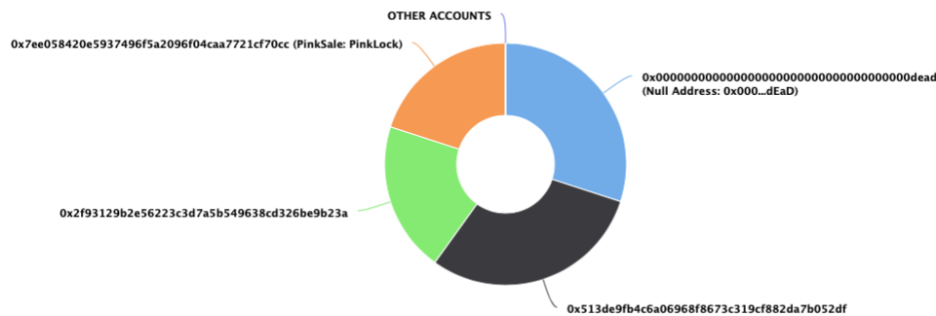
Lil Dragon Token Distribution

The top 100 holders collectively own 100.00% (1,000,000,000,000.00 Tokens) of Lil Dragon

Token Total Supply: 1,000,000,000,000.00 Token | Total Token Holders: 4

Lil Dragon Top 100 Token Holders

Source: BscScan.com



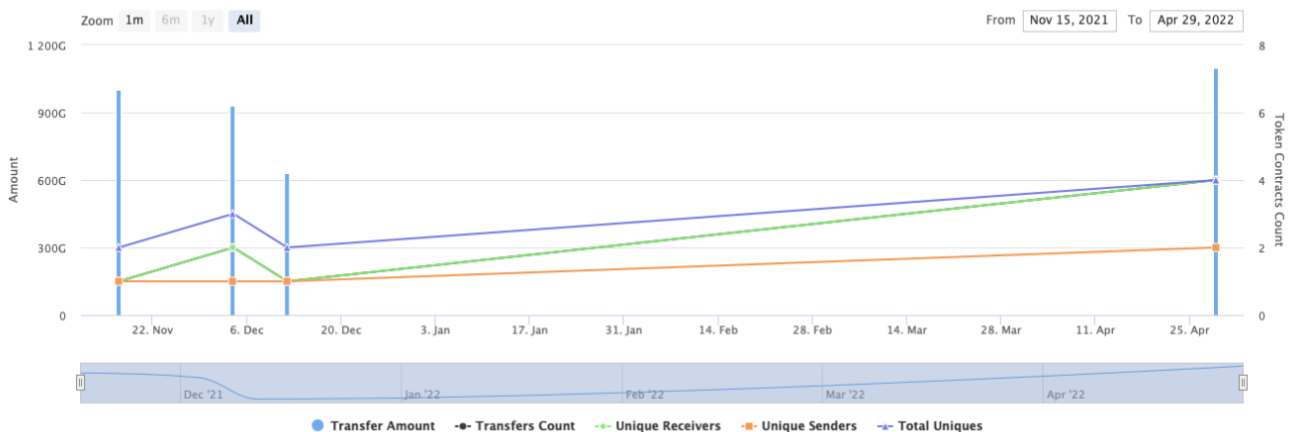
(A total of 1,000,000,000,000.00 tokens held by the top 100 accounts from the total supply of 1,000,000,000,000.00 token)

Lil Dragon Contract Interaction Details

Time Series: Token Contract Overview

Wed 17, Nov 2021 - Fri 29, Apr 2022

Token Contract 0x678dcD2CABa8F26A37759CeE3788b922a473C125 (Lil Dragon)
Source: BscScan.com



Lil Dragon Top 10 Token Holders

| Rank | Address | Quantity (Token) | Percentage |
|------|--|------------------|------------|
| 1 | Null Address: 0x000...dEaD | 300,000,000,000 | 30.0000% |
| 2 | 0x513de9fb4c6a06968f8673c319cf882da7b052df | 299,504,800,000 | 29.9505% |
| 3 | 0x2f93129b2e56223c3d7a5b549638cd326be9b23a | 200,495,200,000 | 20.0495% |
| 4 | PinkSale: PinkLock | 200,000,000,000 | 20.0000% |

Contract functions details

+ [Lib] AddressUpgradeable

- [Int] isContract
- [Int] sendValue #
- [Int] functionCall #
- [Int] functionCall #
- [Int] functionCallWithValue #
- [Int] functionCallWithValue #
- [Int] functionStaticCall
- [Int] functionStaticCall
- [Prv] _verifyCallResult

+ Initializable

- [Prv] _isConstructor

+ ContextUpgradeable (Initializable)

- [Int] __Context_init #
 - modifiers: initializer
- [Int] __Context_init_unchained #
 - modifiers: initializer
- [Int] _msgSender
- [Int] _msgData

+ [Int] IAntiBotLiquidityGeneratorToken

- [Ext] initialize #

+ [Int] IPinkAntiBot

- [Ext] setTokenOwner #
- [Ext] onPreTransferCheck #

+ [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

DF1408

65

76C6

5C780

29C4CAD8

C4

87C9C

31B2A384

- [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 #

- + [Int] IUniswapV2Factory
 - [Ext] feeTo
 - [Ext] feeToSetter
 - [Ext] getPair
 - [Ext] allPairs
 - [Ext] allPairsLength
 - [Ext] createPair #
 - [Ext] setFeeTo #
 - [Ext] setFeeToSetter #

- + [Lib] Address
 - [Int] isContract
 - [Int] sendValue #
 - [Int] functionCall #
 - [Int] functionCall #
 - [Int] functionCallWithValue #
 - [Int] functionCallWithValue #
 - [Int] functionStaticCall
 - [Int] functionStaticCall
 - [Int] functionDelegateCall #
 - [Int] functionDelegateCall #
 - [Prv] _verifyCallResult

- + [Lib] SafeMath
 - [Int] tryAdd
 - [Int] trySub
 - [Int] tryMul
 - [Int] tryDiv
 - [Int] tryMod
 - [Int] add
 - [Int] sub
 - [Int] mul
 - [Int] div
 - [Int] mod
 - [Int] sub
 - [Int] div
 - [Int] mod

- + OwnableUpgradeable (Initializable, ContextUpgradeable)
 - [Int] __Ownable_init #
 - modifiers: initializer
 - [Int] __Ownable_init_unchained #
 - modifiers: initializer
 - [Pub] owner
 - [Pub] renounceOwnership #

- modifiers: onlyOwner
- [Pub] transferOwnership #
 - modifiers: onlyOwner

+ [Int] IERC20Upgradeable

- [Ext] totalSupply
- [Ext] balanceOf
- [Ext] transfer #
- [Ext] allowance
- [Ext] approve #
- [Ext] transferFrom #

+ AntiBotLiquidityGeneratorToken (IERC20Upgradeable, OwnableUpgradeable, IAntiBotLiquidityGeneratorToken)

- [Ext] initialize #
 - modifiers: initializer
- [Ext] setEnableAntiBot #
 - 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
- [Pub] setExcludeFromMaxTx #
 - modifiers: onlyOwner

- [Pub] isExcludedFromMaxTx
- [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] _takeCharityFee #
- [Prv] calculateTaxFee
- [Prv] calculateLiquidityFee
- [Prv] calculateCharityFee
- [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

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.
- 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.

Recommendation:

Check that the excluded array length is not too big.

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

- Owner can enable / disable antibot.
- Owner can include in and exclude from reward.
- Owner can include in and exclude from fees.
- Owner can include in and exclude from the maximum transaction amount limit.
- Owner can change the tax and liquidity fees.
- Owner can change the maximum transaction amount.
- Owner can enable / disable swap and liquify.

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 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.