https://t.me/SolCheck

< SolCheck >

Smart Contract Security Audit

Audit Details

Project:
LemonSwap Token

Deployer Address:
0x161a61bc66f625277da70a38bb7307c89fc92836

Contract Address:
0x86A611fa791C22f91f38E49dEa494A85ae2dCbc0

Blockchain:
Binance Smart Chain (BSC)

Project website:
https://lemonswap.net/

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 SolCheck and its affiliates (including holding companies, shareholders, subsidiaries, employees, directors, officers and other representatives) (SolCheck) owe no duty of care towards you or any other person, nor does SolCheck 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 SolCheck 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, SolCheck hereby excludes all liability and responsibility, and neither you nor any other person shall have any claim against SolCheck, 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

SolCheck performed a free smart contract audit of contract:

https://bscscan.com/address/0x86A611fa791C22f91f38E49dEa494A85ae2dCbc0

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.

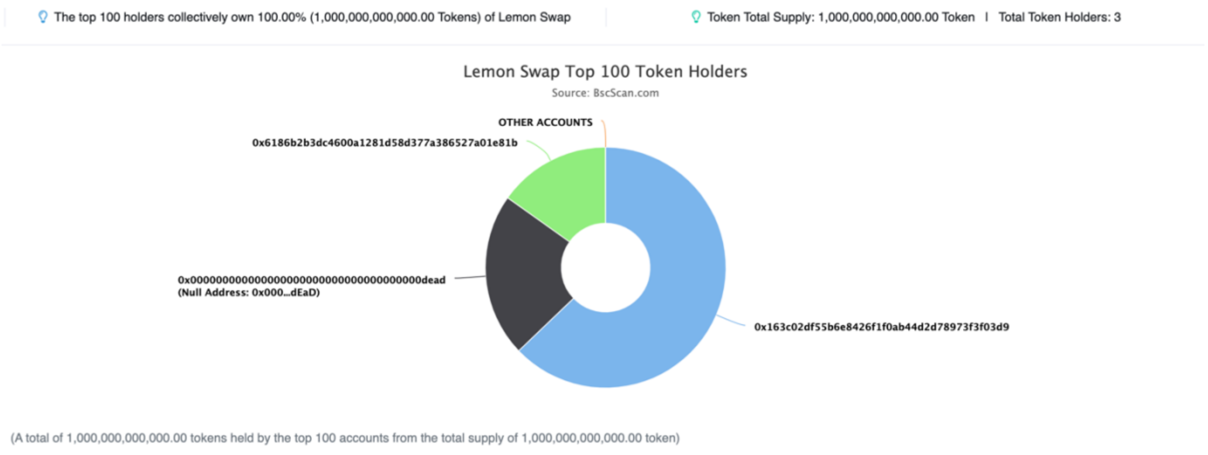
The information in this report should be used to understand the risk exposure of the smart contract, and as a guide to improve the security posture of the smart contract by remediating the issues that were identified.

Contract Details

Contract details for 22.01.2022

Contract Name	Lemon Swap
Contract Address	0x86A611fa791C22f91f38E49dEa494A85ae2dCbc0
Total Supply	1,000,000,000,000
Token Symbol	Lemon
Decimals	18
Token holders	3
Transactions count	4
Top 100 holders dominance	100%
Contract Deployer address	0x161a61BC66f625277DA70A38Bb7307C89fc92836
Contract’s current owner address	0x6186B2b3Dc4600a1281d58D377A386527a01E81B

Lemon Token Distribution



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

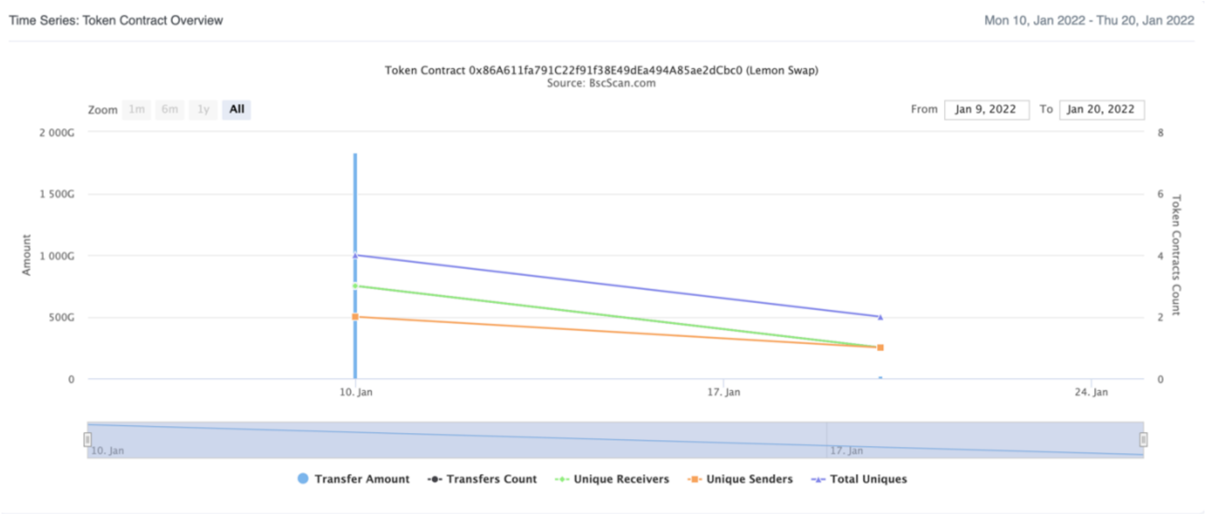
Token Total Supply: 1,000,000,000,000.00 Token | Total Token Holders: 3

Lemon Swap 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)

Contract Interaction Details



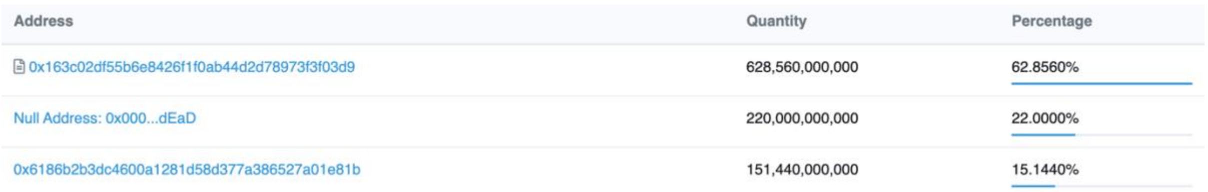
Time Series: Token Contract Overview

Mon 10, Jan 2022 - Thu 20, Jan 2022

Token Contract 0x86A611fa791C22f91f38E49dEa494A85ae2dCbc0 (Lemon Swap)

Source: BscScan.com

NAME Top 100 Holders



Address	Quantity	Percentage
0x163c02df55b6e8426f1f0ab44d2d78973f3f03d9	628,560,000,000	62.8560%
Null Address: 0x000...dEaD	220,000,000,000	22.0000%
0x6186b2b3dc4600a1281d58d377a386527a01e81b	151,440,000,000	15.1440%

Contract Functions Details

+ **Contract**
    - [Int]
    - [Ext]
    - [Pub]
    - [Prv]
+ **[Lib]**
+ **[Int]**

+ **Context**
    - [Int] <Constructor>
    - [Int] _msgSender
    - [Int] _msgData
+ **Ownable (Context)**
    - [Int] <Constructor>
    - [Pub] owner
    - [Pub] renounceOwnership #
    - [Pub] transferOwnership #
    - [Int] _transferOwnership
+ [Int] **IERC20**
    - [Ext] totalSupply
    - [Ext] balanceOf
    - [Ext] transfer
    - [Ext] allowance
    - [Ext] approve
    - [Ext] transferFrom
+ [Int] **IERC20Metadata**
    - [Ext] name
    - [Ext] symbol
    - [Ext] decimals
+ **ERC20**
    - [Int] <Constructor>
    - [Pub] name
    - [Pub] symbol
    - [Pub] decimals
    - [Pub] totalSupply
    - [Pub] balanceOf
    - [Pub] transfer
    - [Pub] allowance
    - [Pub] approve
    - [Pub] transferFrom
    - [Pub] increaseAllowance
    - [Pub] decreaseAllowance
    - [Int] _transfer
    - [Int] _mint
    - [Int] _burn
    - [Int] _approve
    - [Int] _beforeTokenTransfer
    - [Int] _afterTokenTransfer
+ [Lib] **SafeMath**
    - [Int] add

- [Int] sub
- [Int] sub
- [Int] mul
- [Int] div
- [Int] div
- [Int] mod
- [Int] mod

+ [Lib] **SafeMathInt**
  - [Int] mul
  - [Int] div
  - [Int] sub
  - [Int] add
  - [Int] abs
  - [Int] toUnit256Safe

+ [Lib] **SafeMathUint**
  - [Int] toInt256Safe

+ [Int] **DividendPayingTokenInterface**
  - [Ext] dividendOf
  - [Ext] distributeDividends $
  - [Ext] withdrawDividend

+ [Int] **DividendPayingTokenOptionalInterface**
  - [Ext] withdrawableDividendOf
  - [Ext] withdrawDividendOf
  - [Ext] accumulateDividendOf

+ **DividendPayingToken (ERC20, DividendPayingTokenInterface, DividendPayingTokenOptionalInterface)**
  - [Int] <Constructor>
  - [Ext] receive $
  - [Pub] distributeDividends $
  - [Pub] withdrawDividend
  - [Int] _withdrawDividendOfUser
  - [Pub] dividendOf
  - [Pub] withdrawableDividendOf
  - [Pub] withdrawnDividendOf
  - [Pub] accumulativeDividendOf
  - [Int] _transfer
  - [Int] _mint
  - [Int] _burn
  - [int] _setBalance

+ [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] 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
+ [Lib] **IterableMapping**
  - [Int] get
  - [Int] getIndexOfKey

```
          - [Int] getKeyAtIndex
          - [Int] size
          - [Int] set
          - [Int] remove
+ LemonSwapDividendTracker (DividendPayingToken, Ownable)
          - [Int] <Constructor>
          - [Pub] decimals
          - [Int] _transfer
          - [Pub] getAllowCustomTokens
          - [Ext] setAllowCustomTokens #
          - [Ext] excludeFromDividends #
          - [Pub] isExcludedFromDividends
          - [Ext] updateClaimWait #
          - [Ext] updateMinimumTokenBalanceForDividends #
          - [Ext] getLastProcessedIndex
          - [Ext] getNumberOfTokenHolders
          - [Pub] getAccount
          - [Pub] getAccountAtIndex
          - [Prv] canAutoClaim
          - [Ext] setBalance #
          - [Pub] process
          - [Pub] processAccount #
          - [Pub] updateUniswapV2Router #
          - [Pub] updatePayoutToken #
          - [Pub] getPayoutToken
          - [Pub] updateAllowTokens #
          - [Pub] getAllowTokens
          - [Int] _withdrawDividendOfUser
+ LemonSwap (ERC20, Ownable)
          - [Int] <Constructor>
          - modifiers: antiWhale
          - [Pub] decimals
          - [Pub] SetMaxWalletRate #
          - [Ext] receive $
          - [Ext] setSwapTokensAtAmount #
          - [Pub] updateDividendTracker #
          - [Pub] updateUniswapV2Router #
          - [Pub] excludeFromFees #
          - [Pub] excludeMultipleAccountsFromFees #
          - [Ext] updateMarketingWallet #
          - [Ext] updateDevWallet #
          - [Int] isFeeAcceptable
          - [Ext] setMarketingSellFee #
          - [Ext] setMarketingBuyFee #
          - [Ext] setDevSellFee #
          - [Ext] setDevBuyFee #
          - [Ext] setLiquiditySellFee #
          - [Ext] setLiquidityBuyFee #
          - [Ext] setReflectionSellFee #
          - [Ext] setReflectionBuyFee #
          - [Pub] setAutomatedMarketMakerPair #
          - [Prv] _setAutomatedMarketMakerPair
```

- [Pub] updateGasForProcessing #
- [Ext] updateClaimWait #
- [Ext] getClaimWait
- [Ext] updateMinimumTokenBalanceForDividends #
- [Ext] getMinimumTokenBalanceForDividends
- [Ext] getTotalDividendsDistributed
- [Pub] isExcludedFromFees
- [Pub] withdrawableDividendOf
- [Pub] dividendTokenBalanceOf
- [Ext] excludeFromDividends #
- [Pub] isExcludedFromDividends
- [Ext] getAccountDividendsInfo
- [Ext] getAccountDividendsInfoAtIndex
- [Ext] processDividendTracker
- [Ext] claim
- [Ext] claimFor
- [Ext] getNumberOfDividendTokenHolders
- [Int] _transfer
    - modifiers: antiWhale
- [Prv] swapAndLiquify
- [Prv] swapAndSendDividendsMarketingDev
- [Prv] swapTokensForEth
- [Prv] addLiquidity
- [Pub] setAntiBotSystemEnable #
- [Pub] setBotSettingTime #
- [Pub] setBotFeeMultiplicator #
- [Pub] excludeAntibot #
- [Pub] isBot
- [Pub] setEnableAntiwhale #
- [Pub] maxTransferAmount
- [Pub] setMaxTransferAmountRate #
- [Pub] updatePayoutToken
- [Pub] getPayoutToken
- [Pub] updateAllowTokens #
- [Pub] getAllowTokens
- [Pub] enableSwapAndLiquify #
- [Pub] setSwapTokensAmountMax #
- [Ext] getNativeBalance
- [Ext] getCountOfFeesToSwap
- [Ext] transferERC20Token #
- [Pub] setExcludeAntiwhale #
- [Pub] setExcludeMaxWallet #

* $ - payable function
** # - modifier: onlyOwner

Issues Checking Status

Issue Description	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.	Passed
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 Checks

✓ High Severity Issues

No high severity issues found

✓ Medium Severity Issues

No medium severity issues found

✓ Low Severity Issues

No low severity issues found

Owner Abilities

- ⚠ Change swapTokensAtAmount
- ⚠ Change Dividend Tracker address
- ⚠ Change Uniswap Router address
- ⚠ Exclude from Fees
- ⚠ Change Marketing Wallet address
- ⚠ Change Dev Wallet address
- ⚠ Change Marketing Sell Fee
- ⚠ Change Marketing Buy Fee
- ⚠ Change Dev Sell Fee
- ⚠ Change Dev Buy Fee
- ⚠ Change Liquidity Sell Fee
- ⚠ Change Liquidity Buy Fee
- ⚠ Change Reflection Sell Fee
- ⚠ Change Reflection Buy Fee
- ⚠ Set Automated Market Maker Pairs
- ⚠ Change Gas for Processing
- ⚠ Change Claim Wait
- ⚠ Change Minimum token balance for dividends
- ⚠ Exclude from Dividends
- ⚠ Enable / Disable Antibot system
- ⚠ Change Antibot setting time (max. 5 minutes)
- ⚠ Change Bot Fee Multiplicator
- ⚠ Exclude from Antibot
- ⚠ Enable / Disable Antiwhale
- ⚠ Change Max transfer amount
- ⚠ Change tokens allowed to claim dividends with
- ⚠ Enable / Disable swap and liquify
- ⚠ Change swap and liquify at amount
- ⚠ Withdraw any IERC20 token from the contract
- ⚠ Exclude / Include from / in Antiwhale
- ⚠ Exclude / Include from / in Max Wallet

Conclusion

Although this ERC20-compatible token smart contract does not have any severe security issues, owner has a lot of control over token functionality. Until ownership is renounces, addresses could be potentially banned from swapping and transferring tokens. SolCheck advises to check with project's whitepaper to check whether the listed functionality is required to avoid potential scams.

SolCheck 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.