Cyberscope

# Audit Report

# CZ Luna

July 2022

| | |
|---|---|
| Type | BEP20 |
| Network | BSC |
| Address | 0x39DdcF0fd3A4F29Dc40E41E88A32331F715836ED |
| Audited by | © cyberscope |

# Table of Contents

# Contract Review

| | |
|---|---|
| **Contract Name** | CZLunaToken |
| **Compiler Version** | v0.8.4+commit.c7e474f2 |
| **Optimization** | 200 runs |
| **Licence** | MIT |
| **Explorer** | https://bscscan.com/token/0x39DdcF0fd3A4F29Dc40E41E88A32331F715836ED |
| **Symbol** | LUNCZ |
| **Decimals** | 18 |
| **Total Supply** | 10,000,000,000,000 |
| **Domain** | czluna.io |

# Source Files

| **Filename** | SHA256 |
|---|---|
| **contract.sol** | 9b31e101bdbf6484396ba4168b8495c257e878c9aaf0910b6084a5fbbf076a18 |

# Audit Updates

| | |
|---|---|
| **Initial Audit** | 13th June 2022 |
| **Corrected phase 1** | 25th June 2022 |
| **Corrected phase 2** | 5th July 2022 |

# Contract Analysis

● Critical ● Medium ● Minor ● Pass

| Severity | Code | Description |
|---|---|---|
| ● | ST | Contract Owner is not able to stop or pause transactions |
| ● | OCTD | Contract Owner is not able to transfer tokens from specific address |
| ● | OTUT | Owner Transfer User's Tokens |
| ● | ELFM | Contract Owner is not able to increase fees more than a reasonable percent (25%) |
| ● | ULTW | Contract Owner is not able to increase the amount of liquidity taken by dev wallet more than a reasonable percent |
| ● | MT | Contract Owner is not able to mint new tokens |
| ● | BT | Contract Owner is not able to burn tokens from specific wallet |
| ● | BC | Contract Owner is not able to blacklist wallets from selling |

# BC - Blacklisted Contracts

| | |
|---|---|
| **Criticality** | critical |
| **Location** | contract.sol#L708 |

## Description

The contract owner has the authority to stop contracts from transactions. The owner may take advantage of it by calling the `addBotToBlackList` function.

```
require(!_isBlacklisted[from] && !_isBlacklisted[to], "This address is blacklisted");
```

## Recommendation

The team should carefully manage the private keys of the owner’s account. We strongly recommend a powerful security mechanism that will prevent a single user from accessing the contract admin functions. That risk can be prevented by temporarily locking the contract or renouncing ownership.

# Contract Diagnostics

Critical Medium Minor

| Severity | Code | Description |
|---|---|---|
| | L01 | Public Function could be Declared External |
| | L02 | State Variables could be Declared Constant |
| | L04 | Conformance to Solidity Naming Conventions |
| | L07 | Missing Events Arithmetic |
| | L09 | Dead Code Elimination |
| | L14 | Uninitialized Variables in Local Scope |

# L01 - Public Function could be Declared External

| | |
|---|---|
| **Criticality** | minor |
| **Location** | contract.sol#L180,184,432,449,452,455,458,465,469,473,477,482,486,490,493,534,542,693 |

## Description

Public functions that are never called by the contract should be declared external to save gas.

```
isExcludedFromFee
reflectionFromToken
deliver
totalFees
isExcludedFromReward
decreaseAllowance
increaseAllowance
transferFrom
approve
...
```

## Recommendation

Use the external attribute for functions never called from the contract.

# L02 - State Variables could be Declared Constant

| | |
|---|---|
| **Criticality** | minor |
| **Location** | contract.sol#L387,394,417,392,393,389,402,403,401,418 |

## Description

Constant state variables should be declared constant to save gas.

```
numTokensSellToAddToLiquidity
maxTaxFee
maxLiquidityFee
maxDevWalletFee
_tTotal
_symbol
_name
_maxTxAmount
_decimals
...
```

## Recommendation

Add the constant attribute to state variables that never change.

# L04 - Conformance to Solidity Naming Conventions

| | |
|---|---|
| **Criticality** | minor |
| **Location** | contract.sol#L215,216,230,248,598,606,664,669,674,387,395,397,399,417,815 |

## Description

Solidity defines a naming convention that should be followed. Rule exceptions:

- Allow constant variable name/symbol/decimals to be lowercase.
- Allow _ at the beginning of the mixed_case match for private variables and unused parameters.

```
_isBlacklisted
_maxTxAmount
_liquidityFee
_DevWalletFee
_taxFee
_DevWalletWalletAddress
_amount
_enabled
DevWalletFee
...
```

## Recommendation

Follow the Solidity naming convention.
https://docs.soliditylang.org/en/v0.4.25/style-guide.html#naming-conventions.

# L07 - Missing Events Arithmetic

| | |
|---|---|
| **Criticality** | minor |
| **Location** | contract.sol#L594,598,602 |

## Description

Detected missing events for critical arithmetic parameters. There are functions that have no event emitted, so it is difficult to track off-chain changes.

```
_liquidityFee = liquidityFee
_DevWalletFee = DevWalletFee
_taxFee = taxFee
```

## Recommendation

Emit an event for critical parameter changes.

# L09 - Dead Code Elimination

| | |
|---|---|
| **Criticality** | minor |
| **Location** | contract.sol#L150,119,122,125,128,142,145,134,137,109,114,472 |

## Description

Functions that are not used in the contract, and make the code's size bigger.

```
_beforeTokenTransfer
sendValue
isContract
functionStaticCall
functionDelegateCall
functionCallWithValue
functionCall
_verifyCallResult
...
```

## Recommendation

Remove unused functions.

# L14 - Uninitialized Variables in Local Scope

| | |
|---|---|
| **Criticality** | minor |
| **Location** | contract.sol#L819 |

## Description

The are variables that are defined in the local scope and are not initialized.

```
i
```

## Recommendation

All the local scoped variables should be initialized.

# Contract Functions

| Contract | Type | Bases | | |
|---|---|---|---|---|
| | Function Name | Visibility | Mutability | Modifiers |
| | | | | |
| IERC20 | Interface | | | |
| | totalSupply | External | | - |
| | balanceOf | External | | - |
| | transfer | External | ✓ | - |
| | allowance | External | | - |
| | approve | External | ✓ | - |
| | transferFrom | External | ✓ | - |
| | | | | |
| SafeMath | Library | | | |
| | tryAdd | Internal | | |
| | trySub | Internal | | |
| | tryMul | Internal | | |
| | tryDiv | Internal | | |
| | tryMod | Internal | | |
| | add | Internal | | |
| | sub | Internal | | |
| | mul | Internal | | |
| | div | Internal | | |
| | mod | Internal | | |
| | sub | Internal | | |
| | div | Internal | | |
| | mod | Internal | | |
| | | | | |
| Context | Implementation | | | |
| | _msgSender | Internal | | |
| | _msgData | Internal | | |
| | | | | |
| Address | Library | | | |
| | isContract | Internal | | |

| | | | | |
|---|---|---|---|---|
| | sendValue | Internal | ✓ | |
| | functionCall | Internal | ✓ | |
| | functionCall | Internal | ✓ | |
| | functionCallWithValue | Internal | ✓ | |
| | functionCallWithValue | Internal | ✓ | |
| | functionStaticCall | Internal | | |
| | functionStaticCall | Internal | | |
| | functionDelegateCall | Internal | ✓ | |
| | functionDelegateCall | Internal | ✓ | |
| | _verifyCallResult | Private | | |
| | | | | |
| **Ownable** | Implementation | Context | | |
| | <Constructor> | Public | ✓ | - |
| | owner | Public | | - |
| | renounceOwnership | Public | ✓ | onlyOwner |
| | transferOwnership | Public | ✓ | onlyOwner |
| | | | | |
| **IUniswapV2Factory** | Interface | | | |
| | feeTo | External | | - |
| | feeToSetter | External | | - |
| | getPair | External | | - |
| | allPairs | External | | - |
| | allPairsLength | External | | - |
| | createPair | External | ✓ | - |
| | setFeeTo | External | ✓ | - |
| | setFeeToSetter | External | ✓ | - |
| | | | | |
| **IUniswapV2Pair** | Interface | | | |
| | name | External | | - |
| | symbol | External | | - |
| | decimals | External | | - |
| | totalSupply | External | | - |
| | balanceOf | External | | - |
| | allowance | External | | - |

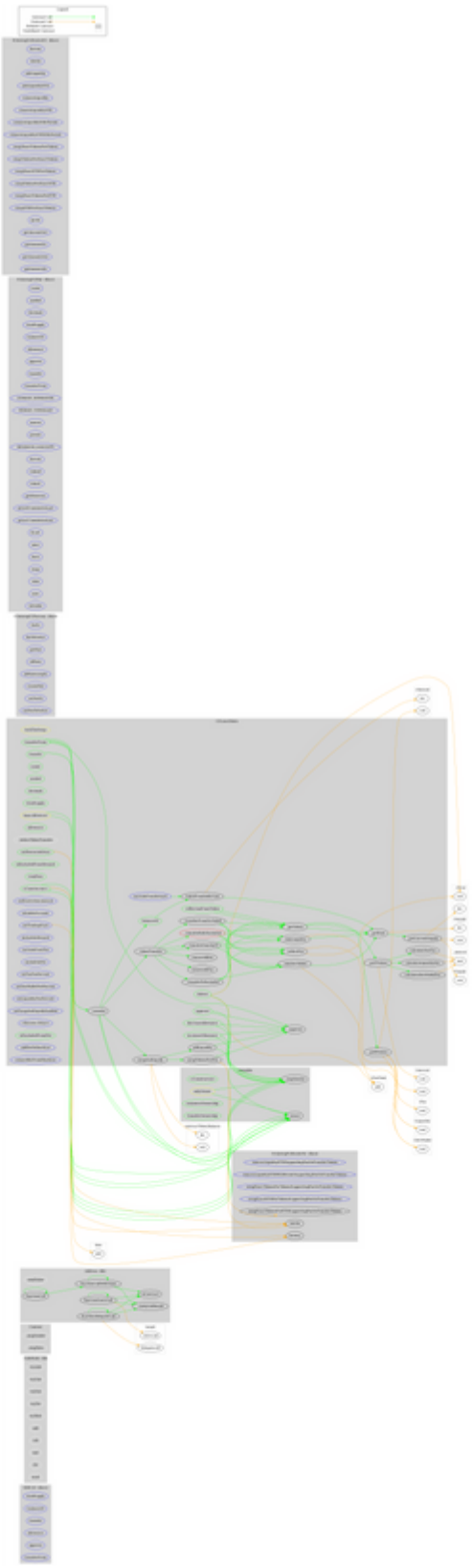
| | | | | |
|---|---|---|---|---|
| | approve | External | ✓ | - |
| | transfer | External | ✓ | - |
| | transferFrom | External | ✓ | - |
| | DOMAIN_SEPARATOR | External | | - |
| | PERMIT_TYPEHASH | External | | - |
| | nonces | External | | - |
| | permit | External | ✓ | - |
| | MINIMUM_LIQUIDITY | External | | - |
| | factory | External | | - |
| | token0 | External | | - |
| | token1 | External | | - |
| | getReserves | External | | - |
| | price0CumulativeLast | External | | - |
| | price1CumulativeLast | External | | - |
| | kLast | External | | - |
| | mint | External | ✓ | - |
| | burn | External | ✓ | - |
| | swap | External | ✓ | - |
| | skim | External | ✓ | - |
| | sync | External | ✓ | - |
| | initialize | External | ✓ | - |
| | | | | |
| **IUniswapV2Router01** | Interface | | | |
| | factory | External | | - |
| | WETH | External | | - |
| | addLiquidity | External | ✓ | - |
| | addLiquidityETH | External | Payable | - |
| | removeLiquidity | External | ✓ | - |
| | removeLiquidityETH | External | ✓ | - |
| | removeLiquidityWithPermit | External | ✓ | - |
| | removeLiquidityETHWithPermit | External | ✓ | - |
| | swapExactTokensForTokens | External | ✓ | - |
| | swapTokensForExactTokens | External | ✓ | - |
| | swapExactETHForTokens | External | Payable | - |
| | swapTokensForExactETH | External | ✓ | - |

| | | | | |
|---|---|---|---|---|
| | swapExactTokensForETH | External | ✓ | - |
| | swapETHForExactTokens | External | Payable | - |
| | quote | External | | - |
| | getAmountOut | External | | - |
| | getAmountIn | External | | - |
| | getAmountsOut | External | | - |
| | getAmountsIn | External | | - |
| | | | | |
| **IUniswapV2Router02** | Interface | IUniswapV2Router01 | | |
| | removeLiquidityETHSupportingFeeOnTransferTokens | External | ✓ | - |
| | removeLiquidityETHWithPermitSupportingFeeOnTransferTokens | External | ✓ | - |
| | swapExactTokensForTokensSupportingFeeOnTransferTokens | External | ✓ | - |
| | swapExactETHForTokensSupportingFeeOnTransferTokens | External | Payable | - |
| | swapExactTokensForETHSupportingFeeOnTransferTokens | External | ✓ | - |
| | | | | |
| **CZLunaToken** | Implementation | Context, IERC20, Ownable | | |
| | setRouterAddress | Public | ✓ | onlyOwner |
| | <Constructor> | Public | ✓ | - |
| | name | Public | | - |
| | symbol | Public | | - |
| | decimals | Public | | - |
| | totalSupply | Public | | - |
| | balanceOf | Public | | - |
| | transfer | Public | ✓ | - |
| | allowance | Public | | - |
| | _beforeTokenTransfer | Internal | ✓ | |
| | approve | Public | ✓ | - |
| | transferFrom | Public | ✓ | - |
| | increaseAllowance | Public | ✓ | - |
| | decreaseAllowance | Public | ✓ | - |

| | | | | |
|---|---|---|---|---|
| | isExcludedFromReward | Public | | - |
| | totalFees | Public | | - |
| | setTradingStart | External | ✓ | onlyOwner |
| | setRestrictionAmount | External | ✓ | onlyOwner |
| | whitelistAccount | External | ✓ | onlyOwner |
| | deliver | Public | ✓ | - |
| | reflectionFromToken | Public | | - |
| | tokenFromReflection | Public | | - |
| | excludeFromReward | External | ✓ | onlyOwner |
| | includeInReward | External | ✓ | onlyOwner |
| | _transferBothExcluded | Private | ✓ | |
| | excludeFromFee | External | ✓ | onlyOwner |
| | includeInFee | External | ✓ | onlyOwner |
| | setTaxFeePercent | External | ✓ | onlyOwner |
| | setDevWalletFeePercent | External | ✓ | onlyOwner |
| | setLiquidityFeePercent | External | ✓ | onlyOwner |
| | setSwapAndLiquifyEnabled | External | ✓ | onlyOwner |
| | <Receive Ether> | External | Payable | - |
| | _reflectFee | Private | ✓ | |
| | _getValues | Private | | |
| | _getTValues | Private | | |
| | _getRValues | Private | | |
| | _getRate | Private | | |
| | _getCurrentSupply | Private | | |
| | _takeLiquidity | Private | ✓ | |
| | _takeDevWallet | Private | ✓ | |
| | calculateTaxFee | Private | | |
| | calculateDevWalletFee | Private | | |
| | calculateLiquidityFee | Private | | |
| | removeAllFee | Private | ✓ | |
| | restoreAllFee | Private | ✓ | |
| | isExcludedFromFee | Public | | - |
| | _approve | Private | ✓ | |
| | _transfer | Private | ✓ | |
| | swapAndLiquify | Private | ✓ | lockTheSwap |

| | | | | |
|---|---|---|---|---|
| | swapTokensForEth | Private | ✓ | |
| | addLiquidity | Private | ✓ | |
| | _tokenTransfer | Private | ✓ | |
| | _transferStandard | Private | ✓ | |
| | _transferToExcluded | Private | ✓ | |
| | _transferFromExcluded | Private | ✓ | |
| | addBotToBlackList | External | ✓ | onlyOwner |
| | removeBotFromBlackList | External | ✓ | onlyOwner |

# Contract Flow



# Domain Info

| | |
|---|---|
| **Domain Name** | czluna.io |
| **Registry Domain ID** | 3942f3a2b06940c4b9907a12cfbc8038-DONUTS |
| **Creation Date** | 2022-06-01T07:05:25Z |
| **Updated Date** | 2022-06-06T07:05:29Z |
| **Registry Expiry Date** | 2023-06-01T07:05:25Z |
| **Registrar WHOIS Server** | whois.namecheap.com |
| **Registrar URL** | https://www.namecheap.com/ |
| **Registrar** | NameCheap, Inc. |
| **Registrar IANA ID** | 1068 |

The domain has been created in 12 months before the creation of the audit.

There is no public billing information, the creator is protected by the privacy settings.

# Summary

The Smart Contract analysis reported one critical severity issue. The contract owner has the authority to massively blacklist addresses. A multi-wallet signing pattern will provide security against potential hacks. Temporarily locking the contract or renouncing ownership will eliminate all the contract threats. There is also a limit of max 25% fees.

# Disclaimer

All the content provided in this document is for general information only and should not be used as financial advice or a reason to buy any investment.

Cyberscope team provides no guarantees against the sale of team tokens or the removal of liquidity by the project audited in this document. Always Do your own research and protect yourselves from being scammed.

The Cyberscope team has audited this project for general information and only expresses their opinion based on similar projects and checks from popular diagnostic tools. Under no circumstances did Cyberscope receive a payment to manipulate those results or change the awarding badge that we will be adding in our website.

Always Do your own research and protect yourselves from scams. This document should not be presented as a reason to buy or not buy any particular token.

The Cyberscope team disclaims any liability for the resulting losses.

# About Cyberscope

Coinscope audit and K.Y.C. service has been rebranded to Cyberscope.

Coinscope is the leading early coin listing, voting and auditing authority firm. The audit process is analyzing and monitoring many aspects of the project. That way, it gives the community a good sense of security using an informative report and a generic score.

Cyberscope and Coinscope are aiming to make crypto discoverable and efficient globally. They provide all the essential tools to assist users draw their own conclusions.

The Cyberscope team

https://www.cyberscope.io