Cyberscope

Audit Report

Luzion Protocol

April 2022

Github	https://github.com/RevoluzionToken/Luzion-Protocol
Commit	32ecac3ee0bc439b049edc9d496a3f429e385463
Audited by	© cyberscope

Table of Contents

Contract Review

Github	https://github.com/RevoluzionToken/Luzion-Protocol
Commit	32ecac3ee0bc439b049edc9d496a3f429e385463
File	LuzionProtocol.sol
Domain	luzion.io

Source Files

Filename	**SHA256**
contract.sol	c66ff180356d2892e56608df0a9240c31f67289918754dbed3125f956e436632

Audit Updates

Initial Audit	11th April 2022
Corrected	

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

Contract Diagnostics

Critical Medium Minor

Severity	Code	Description
	MTS	Manipulate Total Supply
	CO	Code Optimization
	L01	Public Function could be Declared External
	L04	Conformance to Solidity Naming Conventions
	L09	Dead Code Elimination
	L13	Divide before Multiply Operation
	L15	Local Scope Variable Shadowing

MTS - Manipulate Total Supply

Criticality	minor
Location	contract.sol#L1529

Description

Owner is able to manipulate total supply. This change will have a direct impact on the token price and Market Cap.

```
for (uint256 i = 0; i < times; i++) {
    supplyTotal =
supplyTotal.mul((10**rateDecimals).add(rebaseRate)).div(10**rateDecimals);
}
```

Recommendation

The contract owner should carefully manage the adjustment of the circulating supply (increases or decreases), according to the token’s price fluctuations.

CO - Code Optimization

Criticality	minor
Location	contract.sol#L1519

Description

There are code segments that could be optimized. A segment may be optimized so that it becomes a smaller size, consumes less memory, executes more rapidly, or performs fewer operations.

```
if (deltaTimeFromInit < (365 days)) {
    rebaseRate = 2355;
} else if (deltaTimeFromInit >= (365 days) && deltaTimeFromInit < ((15 * 365
days) / 10)) {
    rebaseRate = 211;
} else if (deltaTimeFromInit >= ((15 * 365 days) / 10) && deltaTimeFromInit < (7
* 365 days)) {
    rebaseRate = 14;
} else if (deltaTimeFromInit >= (7 * 365 days)) {
    rebaseRate = 2;
}
```

Recommendation

If the `if` statements are reversed, then the result will be the same but the total expressions will be decreased.

1. If `deltaTimeFromInit < (365 days)`
2. If `deltaTimeFromInit >= (7 * 365 days)`
3. If `deltaTimeFromInit >= ((15 * 365 days) / 10)`
4. else

L01 - Public Function could be Declared External

Criticality	minor
Location	contract.sol#L338,345,352,370,378,562,570,587,594,613,636,658,677,697,1936,1943

Description

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

```
setDividendDistributor
distributorInitialization
decreaseAllowance
increaseAllowance
transferFrom
approve
transfer
totalSupply
decimals
...
```

Recommendation

Use the external attribute for functions never called from the contract

L04 - Conformance to Solidity Naming Conventions

Criticality	minor
Location	contract.sol#L890,892,906,959,1097,1120,1128,1052,1435,1444,1467,1479,1491,1499,1545,1680,1689,1696,1715,1728,1739,1865,1903,1952,1991,2003,1333,1334,1335,1336,1337

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.

```
_allowedFragments
_gonBalances
_isDividendExempt
_isFeeExempt
_blacklistBotContract
_denominator
_target
_flag
_minDistribution
...
```

Recommendation

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

L09 - Dead Code Elimination

Criticality	minor
Location	contract.sol#L859,803,843,773,750,819,722

Description

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

```
_transfer
_spendAllowance
_mint
_burn
_beforeTokenTransfer
_approve
_afterTokenTransfer
```

Recommendation

Remove unused functions.

L13 - Divide before Multiply Operation

Criticality	minor
Location	contract.sol#L1358,1491,1508,1625,1983

Description

Performing divisions before multiplications may cause lose of prediction.

```
liquidityBalance = _gonBalances[pair].div(gonsPerFragment)
autoLiquidityAmount = _gonBalances[address(this)].div(gonsPerFragment)
times = deltaTime.div(900)
gonSwapThreshold = gonsTotal.div(_denominator).mul(_numerator)
gonSwapThreshold = gonsTotal.div(10000).mul(10)
```

Recommendation

The multiplications should be prior to the divisions.

L15 - Local Scope Variable Shadowing

Criticality	minor
Location	contract.sol#L1689

Description

The are variables that are defined in the local scope containing the same name from an upper scope.

```
_owner
```

Recommendation

The local variables should have different names from the upper scoped variables.

Contract Functions

Contract	Type	Bases		
	Function Name	Visibility	Mutability	Modifiers
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		
	_msgValue	Internal		
Ownable	Implementation	Context		
	<Constructor>	Public	✓	-
	owner	Public		-
	authorize	Public	✓	onlyOwner
	unauthorize	Public	✓	onlyOwner
	isOwner	Public		-
	isAuthorized	Public		-
	renounceOwnership	Public	✓	onlyOwner
	transferOwnership	Public	✓	onlyOwner

	_transferOwnership	Internal	✓	
IERC20Extended	Interface			
	name	External		-
	symbol	External		-
	decimals	External		-
	totalSupply	External		-
	balanceOf	External		-
	transfer	External	✓	-
	allowance	External		-
	approve	External	✓	-
	transferFrom	External	✓	-
ERC20	Implementation	Context, IERC20Extended		
	<Constructor>	Public	✓	-
	name	Public		-
	symbol	Public		-
	decimals	Public		-
	totalSupply	Public		-
	balanceOf	Public		-
	transfer	Public	✓	-
	allowance	Public		-
	approve	Public	✓	-
	transferFrom	Public	✓	-
	increaseAllowance	Public	✓	-
	decreaseAllowance	Public	✓	-
	_transfer	Internal	✓	
	_mint	Internal	✓	
	_burn	Internal	✓	
	_approve	Internal	✓	
	_spendAllowance	Internal	✓	
	_beforeTokenTransfer	Internal	✓	
	_afterTokenTransfer	Internal	✓	

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	✓	-
IUniswapV2Factory	Interface			
	feeTo	External		-
	feeToSetter	External		-
	getPair	External		-

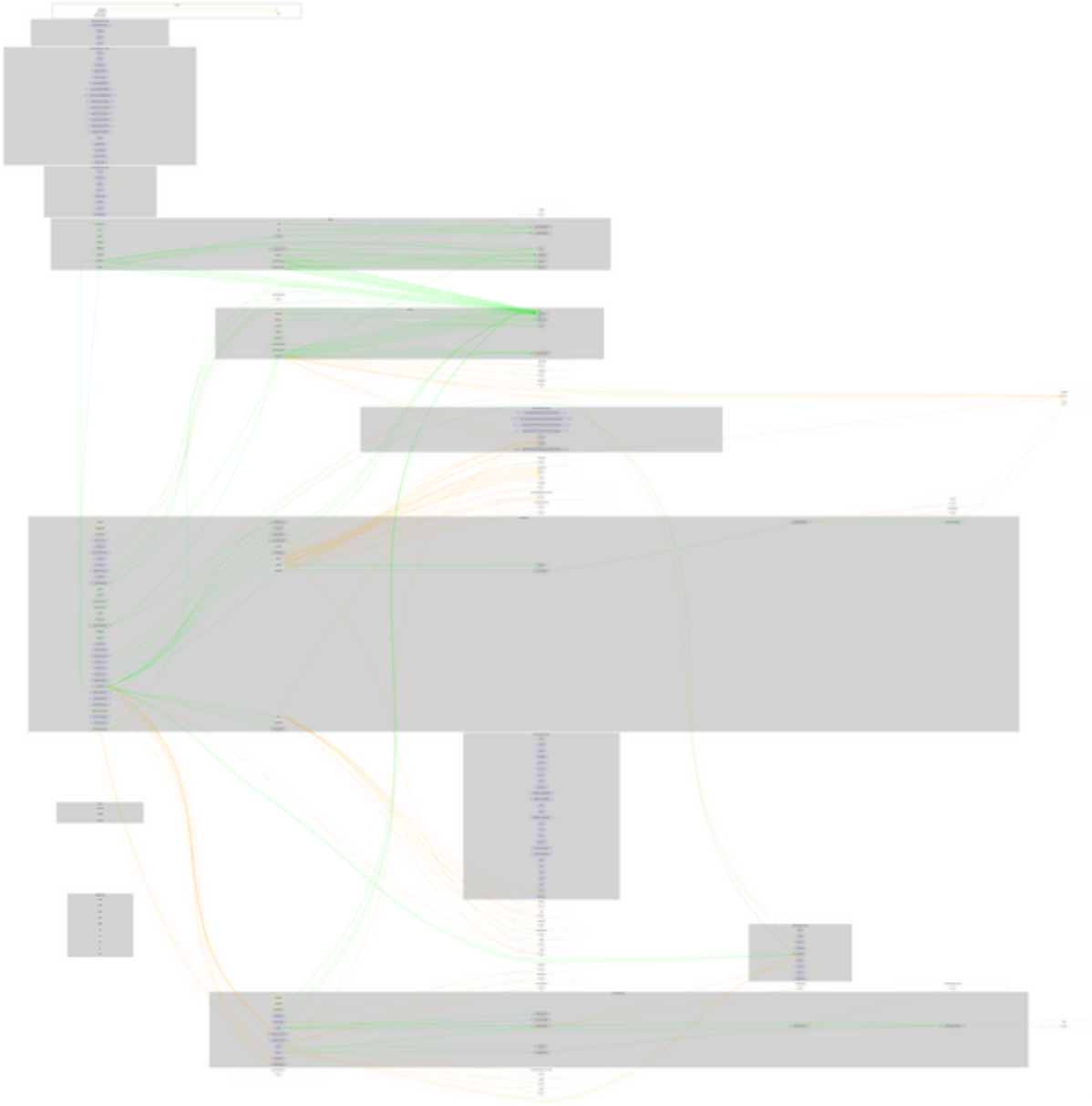
	allPairs	External		-
	allPairsLength	External		-
	createPair	External	✓	-
	setFeeTo	External	✓	-
	setFeeToSetter	External	✓	-
IUniswapV2Router01	Interface			
	factory	External		-
	WETH	External		-
	addLiquidity	External	✓	-
	addLiquidityETH	External	Payable	-
	removeLiquidity	External	✓	-
	removeLiquidityETH	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	✓	-
	swapExactETHForTokensSupportingF	External	Payable	-

	eeOnTransferTokens			
	swapExactTokensForETHSupportingFeeOnTransferTokens	External	✓	-
IDividendDistributor	Interface			
	setDistributionCriteria	External	✓	-
	setShare	External	✓	-
	deposit	External	Payable	-
	process	External	✓	-
DividendDistributor	Implementation	IDividendDistributor, Ownable		
	<Constructor>	Public	✓	-
	changeRouter	External	✓	authorized
	unInitialized	External	✓	authorized
	setTokenAddress	External	✓	initializer authorized
	setDistributionCriteria	External	✓	authorized
	changeRewardToken	External	✓	authorized
	setShare	External	✓	onlyToken
	deposit	External	Payable	authorized
	process	External	✓	authorized
	shouldDistribute	Internal		
	distributeDividend	Internal	✓	
	getCumulativeDividends	Internal		
	getUnpaidEarnings	Public		-
	addShareholder	Internal	✓	
	removeShareholder	Internal	✓	
	claimDividend	External	✓	-
LuzionProtocol	Implementation	ERC20, Ownable		
	<Constructor>	Public	✓	ERC20
	<Receive Ether>	External	Payable	-
	changeRouter	External	✓	authorized

	changePairContract	External	✓	authorized
	manualSync	External	✓	-
	getCirculatingSupply	Public		-
	setAutoRebase	External	✓	authorized
	setBotBlacklist	External	✓	authorized
	setSwapBackSettings	External	✓	authorized
	rescueToken	External	✓	authorized
	rebase	Internal	✓	
	takeFee	Internal	✓	
	swapBack	Internal	✓	swapping
	addLiquidity	Internal	✓	swapping
	buyTokens	Internal	✓	swapping
	approve	Public	✓	-
	allowance	Public		-
	decreaseAllowance	Public	✓	-
	increaseAllowance	Public	✓	-
	transfer	Public	✓	validRecipient
	transferFrom	Public	✓	validRecipient
	_basicTransfer	Internal	✓	
	_transferFrom	Internal	✓	
	totalSupply	Public		-
	balanceOf	Public		-
	shouldTakeFee	Internal		
	shouldRebase	Internal		
	shouldAddLiquidity	Internal		
	shouldSwapBack	Internal		
	isOverLiquified	Public		-
	isNotInSwap	External		-
	checkFeeExempt	External		-
	checkSwapThreshold	External		-
	isContract	Internal		
	_initializeFeeReceivers	Internal	✓	
	setFeeReceivers	External	✓	authorized
	_setFeeReceivers	Internal	✓	
	setIsFeeExempt	External	✓	authorized

	_initializeDistributor	Internal	✓	
	distributorInitialization	Public	✓	authorized
	setDividendDistributor	Public	✓	authorized
	setDistributionCriteria	External	✓	authorized
	setDistributorSettings	External	✓	authorized
	setIsDividendExempt	External	✓	authorized
	getLiquidityBacking	Public		-
	setAutoAddLiquidity	External	✓	authorized
	setTargetLiquidity	External	✓	authorized
	triggerZeusBuyback	External	✓	authorized

Contract Flow



Domain Info

Domain Name	luzion.io
Registry Domain ID	03de6f68973e4a6d965ee5cba83b025e-DONUTS
Creation Date	2022-04-05T18:43:57Z
Updated Date	2022-04-10T18:44:17Z
Registry Expiry Date	2023-04-05T18:43:57Z
Registrar WHOIS Server	http://www.hostinger.com
Registrar URL	http://www.hostinger.com
Registrar	Hostinger, UAB
Registrar IANA ID	1636

The domain has been created 5 days before the creation of the audit. It will expire in 12 months.

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

Summary

The Smart Contract analysis reported no compiler error or critical issues. The contract Owner can access some admin functions that can not be used in a malicious way to disturb the users' transactions. The transaction fees are fixed to 12% for buys and 16% for sales. The contract can blacklist addresses that are contracts. The contract increases the total supply and the corresponding holdings proportionally to the time that has elapsed.

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 provides all the essential tools to assist users draw their own conclusions.

The Cyberscope team

https://www.cyberscope.io