Cyberscope

Audit Report

GOLDEN REGENT İNVESTMENT

November 2022

Type	BEP20
Network	BSC
Address	0x781a900Effca0F373e76b2DCE1DB92969A217Fa2
Audited by	© cyberscope

Table of Contents

Contract Review

Contract Name	GRIcoin
Compiler Version	v0.8.17+commit.8df45f5f
Optimization	200 runs
Licence	None
Explorer	https://bscscan.com/token/0x781a900Effca0F373e76b2DCE1DB92969A217Fa2
Symbol	GRI
Decimals	18
Total Supply	500,000,000
Domain	coingri.com

Source Files

Filename	**SHA256**
contract.sol	5d62c8d1bcf15f8b3e1d1f900d04b6e5fc051594a42e718e5cddb27aade5e4de

Audit Updates

Initial Audit	5th November 2022
Corrected	

Contract Analysis

● Critical ● Medium ● Minor / Informative ● Pass

Severity	Code	Description	Status
●	ST	Stops Transactions	Unresolved
●	OCTD	Transfers Contract's Tokens	Passed
●	OTUT	Transfers User's Tokens	Passed
●	ELFM	Exceeds Fees Limit	Passed
●	ULTW	Transfers Liquidity to Team Wallet	Passed
●	MT	Mints Tokens	Passed
●	BT	Burns Tokens	Passed
●	BC	Blacklists Addresses	Passed

ST - Stops Transactions

Criticality	medium
Location	contract.sol#L933,887
Status	Unresolved

Description

The contract owner has the authority to stop the transactions for all users excluding the owner. The owner may take advantage of it by setting the `_percentageOfLiquidityForMarketing` to a value greater than 100.

```
uint256 marketingFee =
newBalance.mul(_percentageOfLiquidityForMarketing).div(100);
```

The contract owner has the authority to stop the purchases for all users excluding the owner. The owner may take advantage of it by setting the `maxWalletToken` to zero.

```
uint256 contractBalanceRecepient = balanceOf(to);
require(
    contractBalanceRecepient + amount <= maxWalletToken,
    "Exceeds maximum wallet token amount."
);
```

Recommendation

The contract could embody a check for not allowing setting the maxWalletToken less than a reasonable amount. A suggested implementation could check that the maximum amount should be more than a fixed percentage of the total supply. The maximum value of `_percentageOfLiquidityForMarketing` should be 100.

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 / Informative

Severity	Code	Description	Status
●	CO	Code Optimization	Unresolved
●	L02	State Variables could be Declared Constant	Unresolved
●	L04	Conformance to Solidity Naming Conventions	Unresolved
●	L05	Unused State Variable	Unresolved
●	L07	Missing Events Arithmetic	Unresolved
●	L09	Dead Code Elimination	Unresolved

CO - Code Optimization

Criticality	minor / informative
Location	contract.sol#L574
Status	Unresolved

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. The state variable `_maxTxAmount` is initialized by the total supply and can never be changed. As a result, the conditions that are using it will never be truth.

```
uint256 public  _maxTxAmount     = _tTotal;
...
if (from != owner() && to != owner()) {
    require(amount <= _maxTxAmount, "Transfer amount exceeds the maxTxAmount.");
}
...
if (contractTokenBalance >= _maxTxAmount) {
    contractTokenBalance = _maxTxAmount;
}
```

Recommendation

Rewrite some code segments so the runtime will be more performant.

L02 - State Variables could be Declared Constant

Criticality	minor / informative
Location	contract.sol#L307,562,558,308,564,563
Status	Unresolved

Description

Constant state variables should be declared constant to save gas.

```
_previousOwner
_name
_tTotal
_lockTime
_decimals
_symbol
```

Recommendation

Add the constant attribute to state variables that never change.

L04 - Conformance to Solidity Naming Conventions

Criticality	minor / informative
Location	contract.sol#L580,579,574,372,566,389,371,568,555,578,554,581,567,409,551,766
Status	Unresolved

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.

```
_uniswapV2Router
_inSwapAndLiquify
_maxTxAmount
PERMIT_TYPEHASH
_taxFee
MINIMUM_LIQUIDITY
DOMAIN_SEPARATOR
_percentageOfLiquidityForMarketing
_investingWallet
...
```

Recommendation

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

L05 - Unused State Variable

Criticality	minor / informative
Location	contract.sol#L308,307,224
Status	Unresolved

Description

There are segments that contain unused state variables.

```
_lockTime
_previousOwner
MAX_INT256
```

Recommendation

Remove unused state variables.

L07 - Missing Events Arithmetic

Criticality	minor / informative
Location	contract.sol#L746,766,758,753,763
Status	Unresolved

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.

```
_minTokenBalance = minimumToken
maxWalletToken = _maxToken
_liquidityFee = liquidityFee
_taxFee = taxFee
_percentageOfLiquidityForMarketing = marketingFee
```

Recommendation

Emit an event for critical parameter changes.

L09 - Dead Code Elimination

Criticality	minor / informative
Location	contract.sol#L270,283,276
Status	Unresolved

Description

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

```
abs
toInt256Safe
toUint256Safe
```

Recommendation

Remove unused functions.

Contract Functions

Contract	Type	Bases		
	Function Name	**Visibility**	**Mutability**	**Modifiers**
IBEP20	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		
SafeMathInt	Library			
	mul	Internal		
	div	Internal		
	sub	Internal		
	add	Internal		
	abs	Internal		

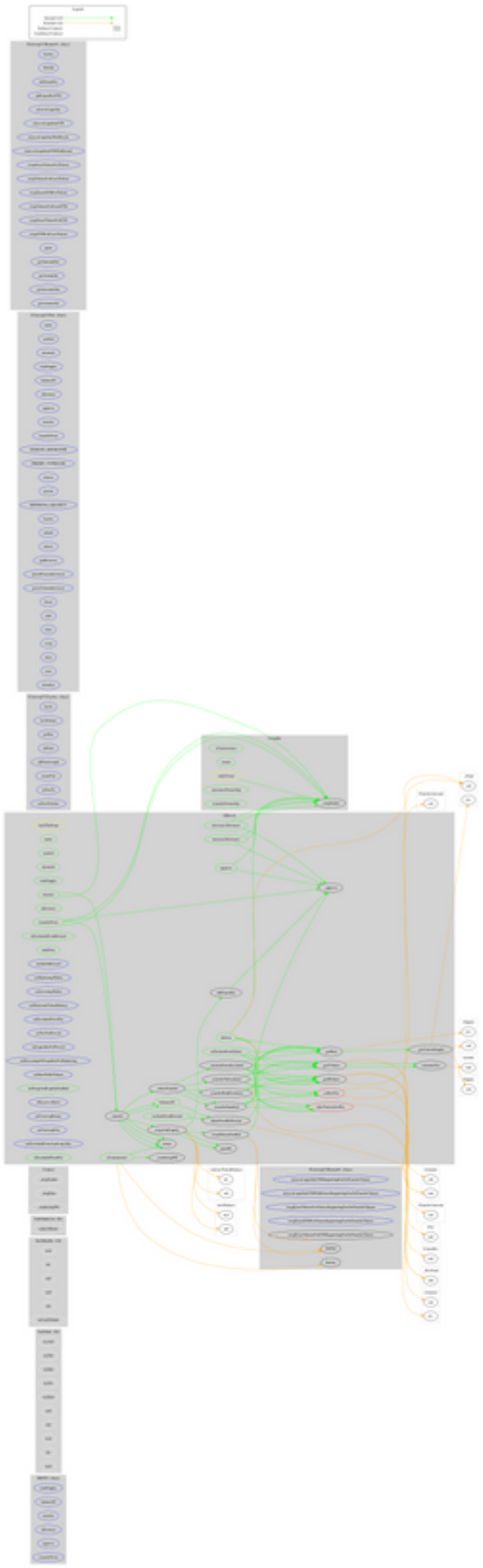
	toUint256Safe	Internal		
SafeMathUint	Library			
	toInt256Safe	Internal		
Context	Implementation			
	_msgSender	Internal		
	_msgData	Internal		
	_marketingWlt	Internal		
Ownable	Implementation	Context		
	<Constructor>	Public	✓	-
	owner	Public		-
	renounceOwnership	Public	✓	onlyOwner
	transferOwnership	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	✓	-
GRIcoin	Implementation	Context, IBEP20, Ownable		
	<Constructor>	Public	✓	Ownable
	name	Public		-
	symbol	Public		-
	decimals	Public		-
	totalSupply	Public		-
	balanceOf	Public		-
	transfer	Public	✓	-
	allowance	Public		-
	approve	Public	✓	-
	transferFrom	Public	✓	-
	increaseAllowance	Public	✓	-
	decreaseAllowance	Public	✓	-
	isExcludedFromReward	Public		-
	totalFees	Public		-
	deliver	Public	✓	-

	reflectionFromToken	Public		-
	tokenFromReflection	Public		-
	excludeFromReward	Public	✓	onlyOwner
	includeInReward	External	✓	onlyOwner
	setMarketingWallet	External	✓	onlyOwner
	setInvestingWallet	External	✓	onlyOwner
	setMinimumTokenBalance	External	✓	onlyOwner
	setExcludedFromFee	External	✓	onlyOwner
	setTaxFeePercent	External	✓	onlyOwner
	setLiquidityFeePercent	External	✓	onlyOwner
	setPercentageOfLiquidityForMarketing	External	✓	onlyOwner
	setMaxWalletTokens	External	✓	onlyOwner
	setSwapAndLiquifyEnabled	Public	✓	onlyOwner
	<Receive Ether>	External	Payable	-
	setUniswapRouter	External	✓	onlyOwner
	setUniswapPair	External	✓	onlyOwner
	setExcludedFromAutoLiquidity	External	✓	onlyOwner
	_reflectFee	Private	✓	
	_getTValues	Private		
	_getRValues	Private		
	_getRate	Private		
	_getCurrentSupply	Private		
	takeTransactionFee	Private	✓	
	calculateFee	Private		
	isExcludedFromFee	Public		-
	_approve	Private	✓	
	_transfer	Private	✓	
	swapAndLiquify	Private	✓	lockTheSwap
	swapTokensForBnb	Private	✓	
	addLiquidity	Private	✓	
	_tokenTransfer	Private	✓	
	_transferStandard	Private	✓	
	_transferBothExcluded	Private	✓	
	_transferToExcluded	Private	✓	
	_transferFromExcluded	Private	✓	

Contract Flow



Domain Info

Domain Name	coingri.com
Registry Domain ID	7229015
Creation Date	2021-12-13T13:23:29Z
Updated Date	2022-05-26T18:27:02Z
Registry Expiry Date	2023-12-13T13:23:29Z
Registrar WHOIS Server	whois.bluehost.com
Registrar URL	http://www.bluehost.com/
Registrar	FastDomain Inc.
Registrar IANA ID	1154

The domain was created 11 months before the creation of the audit. It will expire in about 1 year.

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

Summary

The Smart Contract analysis reported one medium severity issue. The contract may stop the transactions if the configuration is abused. A multi-wallet signing pattern will provide security against potential hacks. Temporarily locking the contract or renouncing ownership will eliminate all the contract threats.

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