Cyberscope

Audit Report

Right Coin

September 2022

Type	BEP20
Network	BSC
Address	0x99DE5611BC1f5b8e3D8876EF567b65f94C5a2ca3
Audited by	© cyberscope

Table of Contents

Contract Review

Contract Name	RightContract
Compiler Version	v0.8.7+commit.e28d00a7
Optimization	200 runs
Licence	MIT
Explorer	https://bscscan.com/token/0x99DE5611BC1f5b8e3D8876EF567b65f94C5a2ca3
Symbol	RHC
Decimals	18
Total Supply	100,000,000
Domain	https://rightcoin.com.br

Audit Updates

Initial Audit	24th September 2022
Corrected	

Source Files

Filename	SHA256
Authorized.sol	92fc8a8c2d7c543a452e05a164302f3e357a4d7009fc5030ed6b5ede699fab2b
Context.sol	91bb853b4716bea8540722c7b13af34e2f24b01a3654cadd68246a72e6c759b8
ERC20.sol	adea8d6813eba55020be787c8a9bef8a71f90c96fd5c75544bc4ac1bccbd51ab
IERC20.sol	4ad9e1338842c0a911ed1994774827c17eea117751a56f1111193d0bc4c0006e
IERC20Metadata.sol	aa7bbf621cc23ca80abde64c64ff6f9503aceae5592f8e3ed2d0ab0a345e09e6
IPancake.sol	ce5cedde1004c8768e88974c30f9d386f0e4f56f084d03e1397a5c8a2a274aa9
Ownable.sol	4a0c4ca403220345b36b1a2e02b5fe041c0e93aa5603a964344c4b3f2c3a8a36
RightCoin.sol	59e8a3a9e10a5bda9fe5db938b78900546f62b0d23865dea6c5a425c29fc763f
Strings.sol	958c2a94731d0ceaaa0830b457842ec11471197f894c2afd6facd7709275f8ac
SwapHelper.sol	82a1d3af307e1561dcfe9844cd83421b3ed372b3dd6fa638810397df4326542d

Solidity Assembly MethodId Analysis

MethodId	Method Name
0x70a08231	balanceOf(address)
0x022c0d9f	swap(uint256, uint256, address, bytes)
0x23b872dd	transferFrom(address, address, uint256)
0xa9059cbb	transfer(address, uint256)
0x0dfe1681	token0( )
0x0902f1ac	getReserves( )

Contract Analysis

● Critical ● Medium ● Minor / Informative ● Pass

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

ULTW - Transfers Liquidity to Team Wallet

Criticality	minor / informative
Location	contract.sol#L373,266
Status	Unresolved

Description

The contract owner has the authority to transfer funds without limit to the team wallet. These funds have been accumulated from fees collected from the contract. The owner may take advantage of it by calling the safeOtherTokens and buyBackWithDecimals methods.

```
function safeOtherTokens(address token, address payable receiv, uint amount) external
isAuthorized(0) {
    if(token == address(0)) { receiv.transfer(amount); } else { IERC20(token).transfer(receiv, amount);
}
  }

if (destAddress == address(0)) {
      swapToken(pairBnbRightCoin, reversed ? igtAmount : 0, reversed ? 0 : igtAmount,
swapHelperAddress);
      _burn(swapHelperAddress, igtAmount);
      totalBurned += igtAmount;
    } else {
      swapToken(pairBnbRightCoin, reversed ? igtAmount : 0, reversed ? 0 : igtAmount,
destAddress);
    }
```

Recommendation

The contract could embody a check for the maximum amount of funds that can be swapped. Since a huge amount may volatile the token's price.

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
●	PTFE	Paired Token Fees Exempt	Unresolved
●	MFEA	Misleading Fees Exempt Assumption	Unresolved
●	SAD	Swapped Amount Diversion	Unresolved
●	L01	Public Function could be Declared External	Unresolved
●	L04	Conformance to Solidity Naming Conventions	Unresolved
●	L09	Dead Code Elimination	Unresolved

PTFE - Paired Token Fees Exempt

Criticality	minor / informative
Location	contract.sol#L207
Status	Unresolved

Description

The contract assumes that during the swap of the BNB/Token pair, the contract should not tax the transfer. That means that the pairWbnbToken address should not be excluded from the exemptFee structure.

```
uint256 wbnbAmount = getAmountOut(feeTokenAmount, reserve1, reserve0);
    swapToken(pairBnbRightCoin, reversed ? 0 : wbnbAmount, reversed ? wbnbAmount : 0,
swapHelperAddress);
    uint256 wbnbBalanceNew = getTokenBalanceOf(wbnbAddress, swapHelperAddress);
    require(wbnbBalanceNew == wbnbBalanceBefore + wbnbAmount, "Wrong amount of
swapped on WBNB");
```

Recommendation

The contract should not allow the address pairWbnbToken to be removed from the exemptFee.

MFEA - Misleading Fees Exempt Assumption

Criticality	minor / informative
Location	contract.sol#L207,222
Status	Unresolved

Description

The contract is based on the fact that the external tokens WBNB and BUSD will never add fees in their transfer functionality.

```
uint256 wbnbAmount = getAmountOut(feeTokenAmount, reserve1, reserve0);
    swapToken(pairBnbRightCoin, reversed ? 0 : wbnbAmount, reversed ? wbnbAmount : 0,
swapHelperAddress);
    uint256 wbnbBalanceNew = getTokenBalanceOf(wbnbAddress, swapHelperAddress);
    require(wbnbBalanceNew == wbnbBalanceBefore + wbnbAmount, "Wrong amount of
swapped on WBNB");


uint256 busdBalanceBefore = getTokenBalanceOf(busdAddress, address(this));
      tokenTransferFrom(wbnbAddress, swapHelperAddress, pairWbnbBusd, wbnbAmount);
      uint256 busdAmount = getAmountOut(wbnbAmount, reserve0, reserve1);
      swapToken(pairWbnbBusd, reversed ? busdAmount : 0, reversed ? 0 : busdAmount,
address(this));
      uint256 busdBalanceNew = getTokenBalanceOf(busdAddress, address(this));
      require(busdBalanceNew == busdBalanceBefore + busdAmount, "Wrong amount swapped
on BUSD");
```

Recommendation

Since it is an external factor that can be changed, the implementation could be more tolerant.

SAD - Swapped Amount Diversion

Criticality	minor
Location	contract.sol#L242
Status	Unresolved

Description

The `_burn` function should take into consideration the tokens that have been swapped and not the fixed number.

```
  tokenTransfer(WBNB, pairBnbRightCoin, wbnbAmount);

    uint256 igtAmount = getAmountOut(wbnbAmount, reserve0, reserve1);
    if (destAddress == address(0)) {
      swapToken(pairBnbRightCoin, reversed ? igtAmount : 0, reversed ? 0 : igtAmount,
swapHelperAddress);
      _burn(swapHelperAddress, igtAmount);
      totalBurned += igtAmount;
    } else {
      swapToken(pairBnbRightCoin, reversed ? igtAmount : 0, reversed ? 0 : igtAmount,
destAddress);
    }
    exemptFee[RIGHTCOIN_POOL] = previousExemptFeeState;
```

Recommendation

The team is advised to carefully check if the implementation follows the expected business logic.

L01 - Public Function could be Declared External

Criticality	minor / informative
Location	RightCoin.sol#L96,93,97,84,138,88,92,94
Status	Unresolved

Description

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

```
setExemptStaker
setExemptFeeReceiver
setAdministrationWallet
activeTxLimit
decimals
desactiveTxLimit
setExemptFee
setExemptTxLimit
```

Recommendation

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

L04 - Conformance to Solidity Naming Conventions

Criticality	minor / informative
Location	RightCoin.sol#L378,74,54,52,379,377,73,55,380,56,53,57
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.

```
setWBNB_BUSD_Pair
RIGHTCOIN_POOL
_name
decimal
getRIGHTCOIN_POOL
setRIGHTCOIN_POOL
WBNB_BUSD_PAIR
_symbol
getWBNB_BUSD_Pair
...
```

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 / informative
Location	RightCoin.sol#L370
Status	Unresolved

Description

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

```
walletHolder
```

Recommendation

Remove unused functions.

Contract Functions

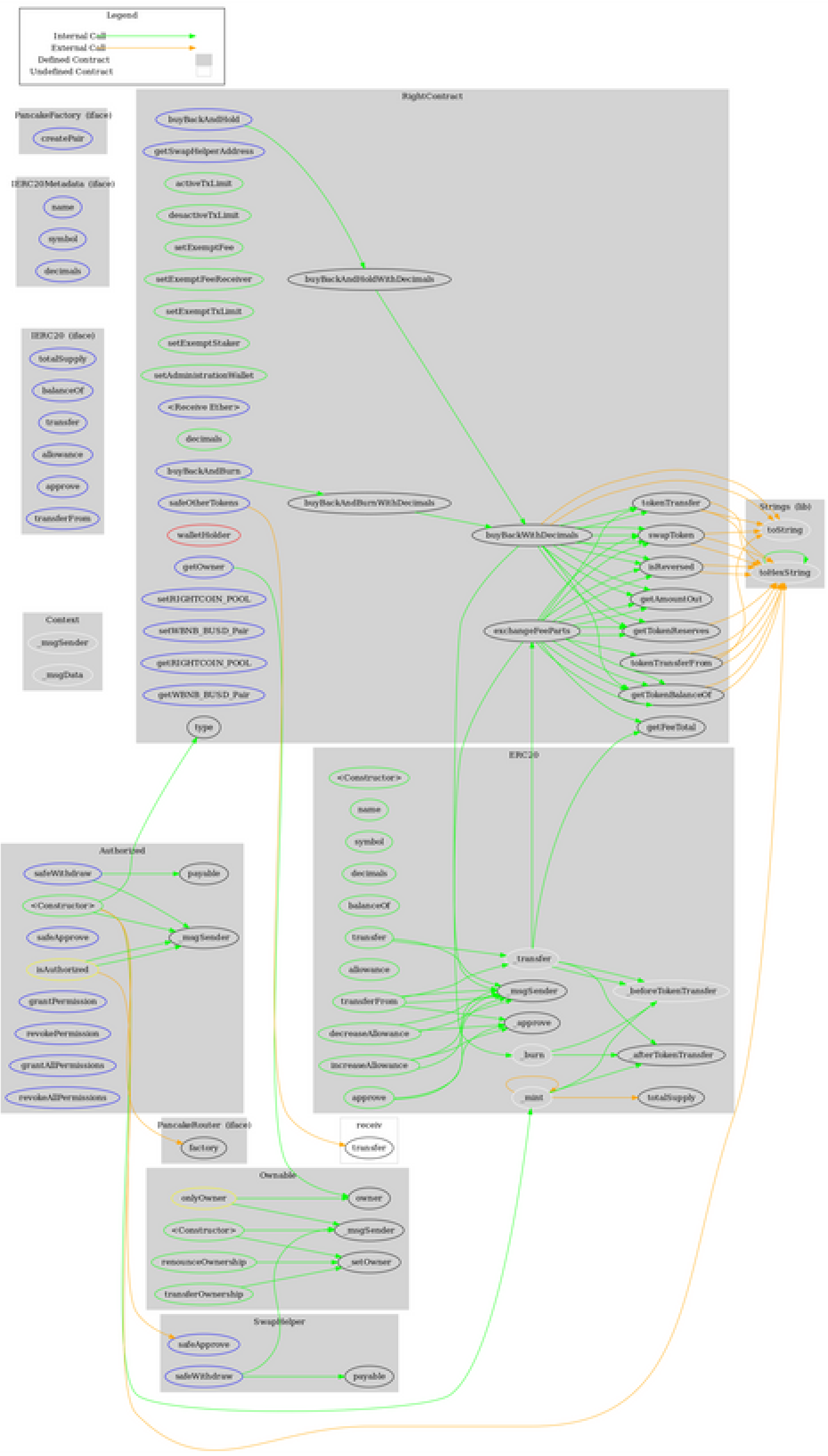
Contract	Type	Bases		
	Function Name	**Visibility**	**Mutability**	**Modifiers**
Authorized	Implementation	Ownable		
	<Constructor>	Public	✓	-
	safeApprove	External	✓	isAuthorized
	safeWithdraw	External	✓	isAuthorized
	grantPermission	External	✓	isAuthorized
	revokePermission	External	✓	isAuthorized
	grantAllPermissions	External	✓	isAuthorized
	revokeAllPermissions	External	✓	isAuthorized
Context	Implementation			
	_msgSender	Internal		
	_msgData	Internal		
ERC20	Implementation	Context, IERC20, IERC20Metadata		
	<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	✓	
	_beforeTokenTransfer	Internal	✓	
	_afterTokenTransfer	Internal	✓	
IERC20	Interface			
	totalSupply	External		-
	balanceOf	External		-
	transfer	External	✓	-
	allowance	External		-
	approve	External	✓	-
	transferFrom	External	✓	-
IERC20Metadata	Interface	IERC20		
	name	External		-
	symbol	External		-
	decimals	External		-
PancakeFactory	Interface			
	createPair	External	✓	-
PancakeRouter	Interface			
	factory	External		-
Ownable	Implementation	Context		
	<Constructor>	Public	✓	-
	owner	Public		-
	renounceOwnership	Public	✓	onlyOwner
	transferOwnership	Public	✓	onlyOwner
	_setOwner	Private	✓	

RightContract	Implementation	Authorized, ERC20		
	getOwner	External		-
	getFeeTotal	Public		-
	getSwapHelperAddress	External		-
	activeTxLimit	Public	✓	isAuthorized
	desactiveTxLimit	Public	✓	isAuthorized
	setExemptFee	Public	✓	isAuthorized
	setExemptFeeReceiver	Public	✓	isAuthorized
	setExemptTxLimit	Public	✓	isAuthorized
	setExemptStaker	Public	✓	isAuthorized
	setAdministrationWallet	Public	✓	isAuthorized
	<Receive Ether>	External	Payable	-
	<Constructor>	Public	✓	ERC20
	decimals	Public		-
	_mint	Internal	✓	
	_beforeTokenTransfer	Internal		
	_transfer	Internal	✓	
	exchangeFeeParts	Private	✓	
	buyBackAndHold	External	✓	isAuthorized
	buyBackAndHoldWithDecimals	Public	✓	isAuthorized
	buyBackAndBurn	External	✓	isAuthorized
	buyBackAndBurnWithDecimals	Public	✓	isAuthorized
	buyBackWithDecimals	Private	✓	
	getAmountOut	Internal		
	isReversed	Internal		
	tokenTransfer	Internal	✓	
	tokenTransferFrom	Internal	✓	
	swapToken	Internal	✓	
	getTokenBalanceOf	Internal		
	getTokenReserves	Internal		
	walletHolder	Private		
	safeOtherTokens	External	✓	isAuthorized
	setRIGHTCOIN_POOL	External	✓	isAuthorized
	setWBNB_BUSD_Pair	External	✓	isAuthorized

	getRIGHTCOIN_POOL	External		-
	getWBNB_BUSD_Pair	External		-
Strings	Library			
	toString	Internal		
	toHexString	Internal		
	toHexString	Internal		
SwapHelper	Implementation	Ownable		
	<Constructor>	Public	✓	-
	safeApprove	External	✓	onlyOwner
	safeWithdraw	External	✓	onlyOwner

Contract Flow



Domain Info

Domain Name	rightcoin.com.br
Creation Date	2022-06-10 00:15:05 UTC
Updated Date	2022-07-26 01:27:03 UTC
Registry Expiry Date	2023-06-10 00:15:05 UTC
Registrar Name	ENDURANCE-BRASIL

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

Summary

The Smart Contract analysis reported one minor severity issue. The contract owner has the authority to transfer funds to the team's wallet. Other than that, the contract owner can access some admin functions that can not be used in a malicious way to disturb the users' transactions. There is also a fixed fee of 10%.

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