Cyberscope

Audit Report
DoctorCat

April 2022

Type	BEP20
Network	BSC
Address	0xe6acb4761b9171ce8240ce83d31e63e73b67f82b
Audited by	© cyberscope

Table of Contents

Contract Review

Contract Name	DoctorCat
Compiler Version	v0.8.13+commit.abaa5c0e
Optimization	200 runs
Licence	MIT
Explorer	https://bscscan.com/token/0xe6acb4761b9171ce8240ce83d31e63e73b67f82b
Symbol	DCAT
Decimals	18
Total Supply	1,000,000,000
Domain	doctorcat.finance

Source Files

Filename	**SHA256**
contract.sol	f5a4b8c6fcacc963e1c413ea0b0c1a589872e5ef1edd88d148bbb2fcdc10b33a

Audit Updates

Initial Audit	18th 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
●	FSA	Fixed Swap Address
●	CO	Code Optimization
●	L01	Public Function could be Declared External
●	L04	Conformance to Solidity Naming Conventions
●	L09	Dead Code Elimination
●	L11	Unnecessary Boolean equality

FSA - Fixed Swap Address

Criticality	minor
Location	contract.sol#L1154

Description

The swap address is assigned once in the constructor and it can not be changed. The decentralized swaps sometimes create a new swap version or abandon the current. A contract that cannot change the swap address may not be able to catch-up the upgrade.

```
uniswapV2Router =
IUniswapV2Router02(0x10ED43C718714eb63d5aA57B78B54704E256024E);
        uniswapV2Pair =
IUniswapV2Factory(uniswapV2Router.factory()).createPair(address(this),
uniswapV2Router.WETH());
```

Recommendation

It could be better to allow the swap address mutation in case of future swap updates.

CO - Code Optimization

Criticality	minor
Location	contract.sol#L1145, 1175, 1192

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. Liquidity and burn fees are fixed to 0, so calculations will have no effect on the amount.

```
uint256 public constant liquiditySellFee = 0;
uint256 public constant liquidityBuyFee = 0;
uint256 public constant burnSellFee = 0;
uint256 public constant burnBuyFee = 0;
```

```
uint256 _LiquidityFee = amount.mul(liquiditySellFee).div(100);
uint256 _BurnFee = amount.mul(burnSellFee).div(100);

super._transfer(sender, marketingAddress, _MarketingFee);
super._transfer(sender, uniswapV2Pair, _LiquidityFee);
super._burn(sender, _BurnFee);

amount = amount.sub(_MarketingFee.add(_BurnFee).add(_LiquidityFee));
```

```
uint256 _LiquidityFee = amount.mul(liquidityBuyFee).div(100);
uint256 _BurnFee = amount.mul(burnBuyFee).div(100);

super._transfer(sender, marketingAddress, _MarketingFee);
super._burn(sender, _BurnFee);

amount = amount.sub(_MarketingFee.add(_BurnFee).add(_LiquidityFee));
```

Recommendation

Remove `liquiditySellFee`, `liquidityBuyFee` , `burnSellFee` and `burnBuyFee` definitions and usage so the runtime will be more performant.

L01 - Public Function could be Declared External

Criticality	minor
Location	contract.sol#L800,808

Description

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

```
transferOwnership
renounceOwnership
```

Recommendation

Use the external attribute for functions never called from the contract

L04 - Conformance to Solidity Naming Conventions

Criticality	minor
Location	contract.sol#L27,1140,1143,1144,1145,1146,1147,1148,1149

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.

```
marketingAddress
burnBuyFee
burnSellFee
liquidityBuyFee
liquiditySellFee
marketingBuyFee
marketingSellFee
maxSupply
WETH
```

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#L350,360,379,393,439,449,412,422,301,325 and 2 more

Description

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

```
_burnFrom
verifyCallResult
sendValue
isContract
functionStaticCall
functionDelegateCall
functionCallWithValue
functionCall
...
```

Recommendation

Remove unused functions.

L11 - Unnecessary Boolean equality

Criticality	minor
Location	contract.sol#L1167

Description

The comparison to boolean constants is redundant. Boolean constants can be used directly and do not need to be compared to true or false.

```
taxStatus == true
```

Recommendation

Remove the equality to the boolean constant.

Contract Functions

Contract	Type	Bases		
	Function Name	**Visibility**	**Mutability**	**Modifiers**
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	✓	-
	swapExactETHForTokensSupportingFeeOnTransferTokens	External	Payable	-
	swapExactTokensForETHSupportingFeeOnTransferTokens	External	✓	-
IERC20	Interface			
	totalSupply	External		-
	decimals	External		-
	symbol	External		-
	name	External		-
	getOwner	External		-
	balanceOf	External		-
	transfer	External	✓	-
	allowance	External		-
	approve	External	✓	-
	transferFrom	External	✓	-
Address	Library			
	isContract	Internal		
	sendValue	Internal	✓	
	functionCall	Internal	✓	
	functionCall	Internal	✓	
	functionCallWithValue	Internal	✓	
	functionCallWithValue	Internal	✓	
	functionStaticCall	Internal		

	functionStaticCall	Internal		
	functionDelegateCall	Internal	✓	
	functionDelegateCall	Internal	✓	
	verifyCallResult	Internal		
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		
Ownable	Implementation	Context		
	<Constructor>	Public	✓	-
	owner	Public		-
	renounceOwnership	Public	✓	onlyOwner
	transferOwnership	Public	✓	onlyOwner
	_transferOwnership	Internal	✓	
ERC20	Implementation	Context, IERC20, Ownable		
	<Constructor>	Public	✓	-
	getOwner	External		-

	name	External		-
	decimals	External		-
	symbol	External		-
	totalSupply	External		-
	balanceOf	External		-
	transfer	External	✓	-
	allowance	External		-
	approve	External	✓	-
	transferFrom	External	✓	-
	increaseAllowance	External	✓	-
	decreaseAllowance	External	✓	-
	_transfer	Internal	✓	
	_mint	Internal	✓	
	_burn	Internal	✓	
	_approve	Internal	✓	
	_burnFrom	Internal	✓	
DoctorCat	Implementation	ERC20		
	<Constructor>	Public	✓	ERC20
	setTax	External	✓	onlyOwner
	addExcludeFee	External	✓	onlyOwner
	_transfer	Internal	✓	

Contract Flow

Domain Info

Domain Name	doctorcat.finance
Registry Domain ID	65d838b54c1c4f6da9c749e47994d5ae-DONUTS
Creation Date	2022-04-14T15:59:32Z
Updated Date	2022-04-19T16:01:27Z
Registry Expiry Date	2023-04-14T15:59:32Z
Registrar WHOIS Server	whois.namecheap.com
Registrar URL	https://www.namecheap.com/
Registrar	NameCheap, Inc.
Registrar IANA ID	1068

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

Summary

DoctorCat is an interesting project that has a friendly and growing community. 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 fees are fixed 5% on selling, 3% on buying and can not be changed.

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