Cyberscope

Audit Report

DollarBack

August 2022

Type	BEP20
Network	BSC
Address	0xF2cAaBf67f99D3AC5D0A4529722cFB874c9b35Bf
Audited by	© cyberscope

Table of Contents

Contract Review

Contract Name	TOKEN
Compiler Version	v0.8.13+commit.abaa5c0e
Optimization	200 runs
Licence	MIT
Explorer	https://bscscan.com/token/0xF2cAaBf67f99D3AC5D0A4529722cFB874c9b35Bf
Symbol	$BACK
Decimals	9
Total Supply	300,000,000,000
Domain	http://dollarback.io

Source Files

Filename	**SHA256**
contract.sol	65d15f163cf781639abea2aa7c369d163febc364dfd69457b39c9096b806479f

Audit Updates

Initial Audit	19th March 2022
Corrected Phase 1	21th March 2022
Corrected Phase 2	12th June 2022
Corrected Phase 3	10th August 2022

Contract Analysis

Critical Medium Minor Pass

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

ST - Stop Transactions

Criticality	medium
Location	contract.sol#L1339,1350

Description

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

```
if (from != owner() && to != owner())
    require( _isExcludedFromMaxTnxLimit[from] ||
_isExcludedFromMaxTnxLimit[to] ||
        amount <= _maxTxAmount,
        "Transfer amount exceeds the maxTxAmount."
    );
```

The contract owner has the authority to stop transactions for all users excluding the owner. The owner may take advantage of it by setting the `isOpen` to false with the method `openTrade`.

```
modifier open(address from, address to) {
            require(isOpen || _whiteList[from] || _whiteList[to], " Trading is
not Open");
            _;
}
```

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

```
if (
    from != owner() &&
    to != address(this) &&
    to != _burnAddress &&
    to != uniswapV2Pair )
{
    uint256 currentBalance = balanceOf(to);
    require(_isExcludedFromMaxWallet[to] || (currentBalance + amount <=
_maxWalletBalance),
            "BEP20: Reached max wallet holding");
}
```

Recommendation

The contract could embody a check for not allowing setting the _maxTxAmount and _maxWalletBalance 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 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.

OCTD - Owner Contract Tokens Drain

Criticality	minor
Location	contract.sol#L1135

Description

The contract owner has the authority to claim all the balance of the contract. The owner may take advantage of it by calling the `withdrawStuckedTokens` function.

```
function withdrawStuckedTokens(address tokenAddress, uint256 tokens) external
onlyOwner returns (bool success){
    return IBEP20(tokenAddress).transfer(msg.sender, tokens);
}
```

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.

ULTW - Unlimited Liquidity to Team Wallet

Criticality	minor
Location	contract.sol#L1126

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 `withdrawStuckedFunds` methods.

```
function withdrawStuckedFunds(uint256 amount) external onlyOwner {
    // This is the current recommended method to use.
    (bool sent, ) = _owner.call{value: amount}("");
    require(sent, "Failed to send BNB");
}
```

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.

BC - Blacklisted Contracts

Criticality	medium
Location	contract.sol#L1054

Description

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

```
function addToBlackList(address account) external onlyOwner {
    require(account != owner(),"Owner address can not blacklisted");
    _isBlacklisted[account] = true;
}
```

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
	STC	Succeeded Transfer Check
	L01	Public Function could be Declared External
	L02	State Variables could be Declared Constant
	L04	Conformance to Solidity Naming Conventions
	L05	Unused State Variable
	L07	Missing Events Arithmetic
	L09	Dead Code Elimination
	L13	Divide before Multiply Operation

STC - Succeeded Transfer Check

Criticality	minor
Location	contract.sol#L1126

Description

According to the ERC20 specification, the transfer methods should be checked if the result is successful. Otherwise, the contract may wrongly assume that the transfer has been established.

```
function withdrawStuckedTokens(address tokenAddress, uint256 tokens) external
onlyOwner returns (bool success){
    return IBEP20(tokenAddress).transfer(msg.sender, tokens);
}
```

Recommendation

The contract should check if the result of the transfer methods is successful.

L01 - Public Function could be Declared External

Criticality	minor
Location	contract.sol#L904,1018,317,1030,856,1022,838,874,847,928,322,1034,826,830,865,1026,891,920,924,1014,1307

Description

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

```
isExcludedFromFee
excludeFromFee
totalFees
isExcludedFromReward
increaseAllowance
isExcludedFromMaxTnxLimit
approve
symbol
name
...
```

Recommendation

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

L02 - State Variables could be Declared Constant

Criticality	minor
Location	contract.sol#L296,717,725

Description

Constant state variables should be declared constant to save gas.

```
_totalFees
_burnAddress
_previousOwner
```

Recommendation

Add the constant attribute to state variables that never change.

L04 - Conformance to Solidity Naming Conventions

Criticality	minor
Location	contract.sol#L1268,757,758,421,452,742,350,419,1272,716,1113,717,743,295,1091,715,712,1280,744,498,1095,741

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.

```
_taxFee
_trueFalse
_addr
WETH
_charityFee
_amount
_isBlacklisted
_marketingWalletAddress
_owner
...
```

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
Location	contract.sol#L725,296

Description

There are segments that contain unused state variables.

```
_previousOwner
_totalFees
```

Recommendation

Remove unused state variables.

L07 - Missing Events Arithmetic

Criticality	minor
Location	contract.sol#L1055,1042,1073,1099,1038

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.

```
_maxWalletBalance = maxBalancePercent * 10 ** decimals()
numTokensSellToAddToLiquidity = amount * 10 ** _decimals
_buyTaxFee = tFee
_maxTxAmount = maxTxAmount * 10 ** decimals()
_sellTaxFee = tFee
```

Recommendation

Emit an event for critical parameter changes.

L09 - Dead Code Elimination

Criticality	minor
Location	contract.sol#L171,198,264,252,212,229,274,163,190,242,183

Description

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

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

Recommendation

Remove unused functions.

L13 - Divide before Multiply Operation

Criticality	minor
Location	contract.sol#L1392

Description

Performing divisions before multiplications may cause lose of prediction.

```
marketingTokens = contractBalance.mul(_marketingFee).div(1000)
charityTokens = contractBalance.mul(_charityFee).div(1000)
tokensForLiquidity = contractBalance.mul(_liquidityFee).div(1000)
```

Recommendation

The multiplications should be prior to the divisions.

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		
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
LockToken	Implementation	Ownable		
	<Constructor>	Public	✓	-
	openTrade	External	✓	onlyOwner
	includeToWhiteList	External	✓	onlyOwner
IUniswapV2Factory	Interface			
	feeTo	External		-
	feeToSetter	External		-
	getPair	External		-
	allPairs	External		-
	allPairsLength	External		-
	createPair	External	✓	-
	setFeeTo	External	✓	-
	setFeeToSetter	External	✓	-
IUniswapV2Pair	Interface			

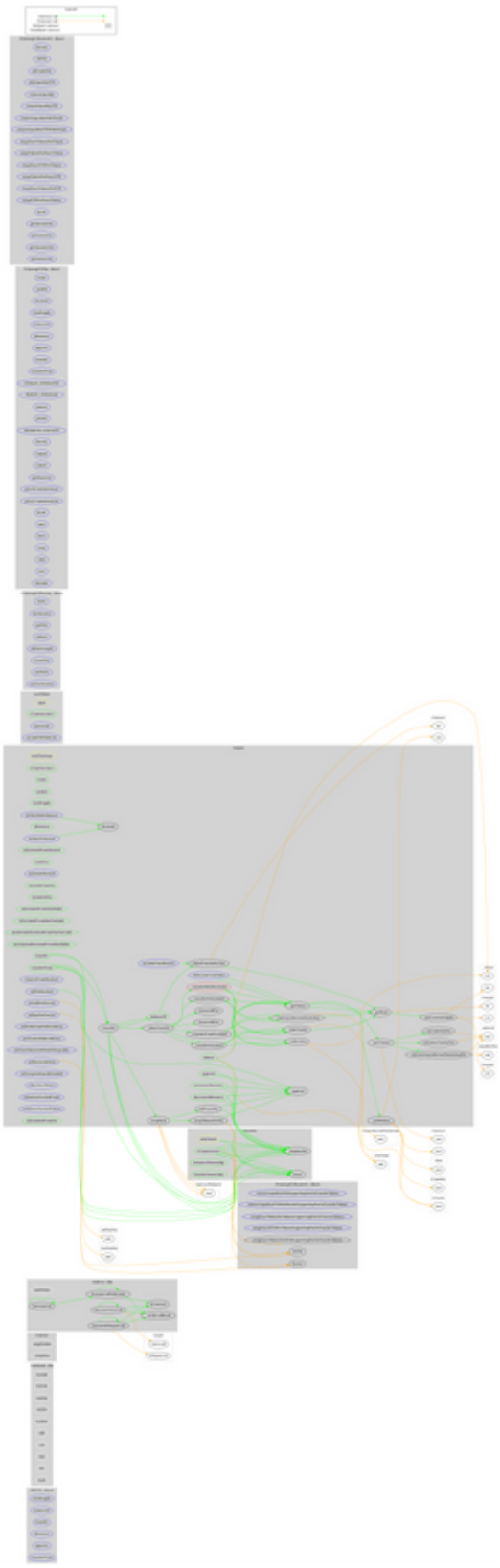
	name	External		-
	symbol	External		-
	decimals	External		-
	totalSupply	External		-
	balanceOf	External		-
	allowance	External		-
	approve	External	✓	-
	transfer	External	✓	-
	transferFrom	External	✓	-
	DOMAIN_SEPARATOR	External		-
	PERMIT_TYPEHASH	External		-
	nonces	External		-
	permit	External	✓	-
	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	✓	-
TOKEN	Implementation	Context, IBEP20, Ownable, LockToken		
	<Constructor>	Public	✓	-
	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	External		-
	tokenFromReflection	Public		-
	excludeFromReward	External	✓	onlyOwner
	includeInReward	External	✓	onlyOwner
	_transferBothExcluded	Private	✓	
	excludeFromFee	Public	✓	onlyOwner
	includeInFee	Public	✓	onlyOwner
	isExcludedFromMaxWallet	Public		-
	isExcludedFromMaxTnxLimit	Public		-
	includeAndExcludedFromMaxTnxLimit	Public	✓	onlyOwner
	includeAndExcludedFromMaxWallet	Public	✓	onlyOwner
	setMaxWalletBalance	External	✓	onlyOwner
	setMaxTxAmount	External	✓	onlyOwner
	removeFromBlackList	External	✓	onlyOwner
	addToBlackList	External	✓	onlyOwner
	setSellFeePercent	External	✓	onlyOwner
	setBuyFeePercent	External	✓	onlyOwner
	setMarketingWalletAddress	External	✓	onlyOwner
	setCharityWalletAddress	External	✓	onlyOwner
	setNumTokensSellToAddToLiquidity	External	✓	onlyOwner
	setRouterAddress	External	✓	onlyOwner
	setSwapAndLiquifyEnabled	External	✓	onlyOwner
	<Receive Ether>	External	Payable	-
	withdrawStuckedFunds	External	✓	onlyOwner
	withdrawStuckedTokens	External	✓	onlyOwner

	_reflectFee	Private	✓	
	_getValues	Private		
	_getTValues	Private		
	_getRValues	Private		
	_getRate	Private		
	_getCurrentSupply	Private		
	_takeLiquidityAndMarketing	Private	✓	
	_takeCharity	Private	✓	
	calculateTaxFee	Private		
	calculateCharityFee	Private		
	calculateLiquidityAndMarketingFee	Private		
	removeAllFee	Private	✓	
	restoreAllFee	Private	✓	
	isExcludedFromFee	Public		-
	_approve	Private	✓	
	_transfer	Private	✓	open
	swapBack	Private	✓	lockTheSwap
	swapTokensForEth	Private	✓	
	addLiquidity	Private	✓	
	_tokenTransfer	Private	✓	
	_transferStandard	Private	✓	
	_transferToExcluded	Private	✓	
	_transferFromExcluded	Private	✓	

Contract Flow



Domain info

Domain Name	dollarback.io
Registry Domain ID	086c34a20aa04c3480e8eca7c17f042a-DONUTS
Creation Date	2022-06-07T14:14:11Z
Updated Date	2022-06-15T18:27:57Z
Registry Expiry Date	2023-06-07T14:14:11Z
Registrar WHOIS Server	whois.ionos.com
Registrar URL	https://www.ionos.com
Registrar	IONOS SE
Registrar IANA ID	83

The domain has been created in 10 months before the creation of the audit.

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

Summary

There are some functions that can be abused by the owner like stopping transactions, transferring tokens to the team's wallet, transferring funds to the team's wallet and blacklisting 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 20% fees both for buys and sales.

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