Cyberscope

Audit Report

Monkey inu

July 2022

Type	BEP20
Network	BSC
Address	0x6e077c2666D9C10A302E2cffBD47862b3BcD68fD
Audited by	© cyberscope

Table of Contents

Contract Review

Contract Name	MonkeyInu
Compiler Version	v0.8.13+commit.abaa5c0e
Optimization	200 runs
Licence	None
Explorer	https://bscscan.com/token/0x6e077c2666D9C10A302E2cffBD47862b3BcD68fD
Symbol	MonkeyInu
Decimals	18
Total Supply	20,000,000,000,000
Domain	monkeyinu.io

Source Files

Filename	**SHA256**
contract.sol	e11a39d8b410ba1936546052a2eabd64e61e2c38e8fb4f354ceda4bc6f564517

Audit Updates

Initial Audit	19th July 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

ST - Stop Transactions

Criticality	critical
Location	contract.sol#L683,1083

Description

The contract owner has the authority to stop the sales for all users excluding the owner. The owner may take advantage of it by setting the fees to a high percentage value. As a result, the transaction will overflow.

Additionally, the contract has the ability to stop the sales by exploiting the zero deviation finding.

```
if(recipient==uniswapV2Pair)
{
    setAllFees(_saleTaxFee, _saleLiquidityFee, _saleMarketingFee);
}
```

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 owner's address to the `_whiteList` and closing the trades.

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

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.

ELFM - Exceed Limit Fees Manipulation

Criticality	critical
Location	contract.sol#L1186

Description

The contract owner has the authority to increase over the allowed limit of 25%. The owner may take advantage of it by calling the `setSaleFees` function with a high percentage value.

```
function setSaleFees(uint256 taxFee, uint256 liquidityFee, uint256 marketingFee)
external onlyOwner() {
    _saleTaxFee = taxFee;
    _saleLiquidityFee = liquidityFee;
    _saleMarketingFee = marketingFee;
}
```

Recommendation

The contract could embody a check for the maximum acceptable value.

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
	ZD	Zero Division
	CO	Code Optimization
	L01	Public Function could be Declared External
	L02	State Variables could be Declared Constant
	L04	Conformance to Solidity Naming Conventions
	L07	Missing Events Arithmetic
	L09	Dead Code Elimination
	L13	Divide before Multiply Operation

ZD - Zero Division

Criticality	critical
Location	contract.sol#L1015

Description

The contract is using variables that may be set to zero as denominators. As a result, the transactions will revert.

```
uint256 tokensForLiquidity =
contractTokenBalance.mul(_saleLiquidityFee).div(_saleLiquidityFee.add(_saleMarke
tingFee));
```

Recommendation

The contract should prevent those variables to be set to zero or should not allow to execute the corresponding statements.

CO - Code Optimization

Criticality	minor
Location	contract.sol#L1027

Description

The contract performs the `swapTokensForBnb()` twice. Once for the autogenerated liquidity pool and once for the marketing wallet. The execution of `swapTokensForBnb()` produces gas.

```
// swap tokens for ETH
swapTokensForBnb(half); // <- this breaks the ETH -> HATE swap when swap+liquify is triggered

// how much ETH did we just swap into?
uint256 newBalance = address(this).balance.sub(initialBalance);

// add liquidity to uniswap
addLiquidity(otherHalf, newBalance);

// swap and Send BNB to marketing  wallet
swapTokensForBnb(contractTokenBalance.sub(tokensForLiquidity));

marketingWallet.transfer(address(this).balance);
```

Recommendation

The contract could execute the `swapTokensForBnb()` once providing the sum of the amount and then split the funds to the corresponding wallets.

L01 - Public Function could be Declared External

Criticality	minor
Location	contract.sol#L433,442,448,453,461,787,791,795,808,817,822,828,833,838,842,851,868,980,1158,1162,1203

Description

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

```
setSwapAndLiquifyEnabled
includeInFee
excludeFromFee
isExcludedFromFee
excludeFromReward
reflectionFromToken
deliver
isExcludedFromReward
decreaseAllowance
...
```

Recommendation

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

L02 - State Variables could be Declared Constant

Criticality	minor
Location	contract.sol#L725,723,724,719

Description

Constant state variables should be declared constant to save gas.

```
_tTotal
_symbol
_name
_decimals
```

Recommendation

Add the constant attribute to state variables that never change.

L04 - Conformance to Solidity Naming Conventions

Criticality	minor
Location	contract.sol#L505,506,522,543,693,697,955,961,1203,729,732,735,739,740,741,755

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.

```
_maxTxAmount
_saleMarketingFee
_saleLiquidityFee
_saleTaxFee
_marketingFee
_liquidityFee
_taxFee
_enabled
_amount
...
```

Recommendation

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

L07 - Missing Events Arithmetic

Criticality	minor
Location	contract.sol#L1177,1186,1194,1198

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.

```
_maxTxAmount = maxTxAmount
minimumTokensBeforeSwap = newAmt
_saleTaxFee = taxFee
_previousTaxFee = taxFee
```

Recommendation

Emit an event for critical parameter changes.

L09 - Dead Code Elimination

Criticality	minor
Location	contract.sol#L359,319,329,344,354,266,293

Description

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

```
sendValue
isContract
functionCallWithValue
functionCall
_functionCallWithValue
```

Recommendation

Remove unused functions.

L13 - Divide before Multiply Operation

Criticality	minor
Location	contract.sol#L1124

Description

Performing divisions before multiplications may cause lose of prediction.

```
tMarketing = tAmount.div(100).mul(_marketingFee)
```

Recommendation

The multiplications should be prior to the divisions.

Contract Functions

Contract	Type	Bases		
	Function Name	Visibility	Mutability	Modifiers
Context	Implementation			
	_msgSender	Internal		
	_msgData	Internal		
IERC20	Interface			
	totalSupply	External		-
	balanceOf	External		-
	transfer	External	✓	-
	allowance	External		-
	approve	External	✓	-
	transferFrom	External	✓	-
SafeMath	Library			
	add	Internal		
	sub	Internal		
	sub	Internal		
	mul	Internal		
	div	Internal		
	div	Internal		
	mod	Internal		
	mod	Internal		
Address	Library			
	isContract	Internal		
	sendValue	Internal	✓	
	functionCall	Internal	✓	
	functionCall	Internal	✓	
	functionCallWithValue	Internal	✓	

	functionCallWithValue	Internal	✓	
	_functionCallWithValue	Private	✓	
Ownable	Implementation	Context		
	<Constructor>	Public	✓	-
	owner	Public		-
	renounceOwnership	Public	✓	onlyOwner
	transferOwnership	Public	✓	onlyOwner
	geUnlockTime	Public		-
	lock	Public	✓	onlyOwner
	unlock	Public	✓	-
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		-

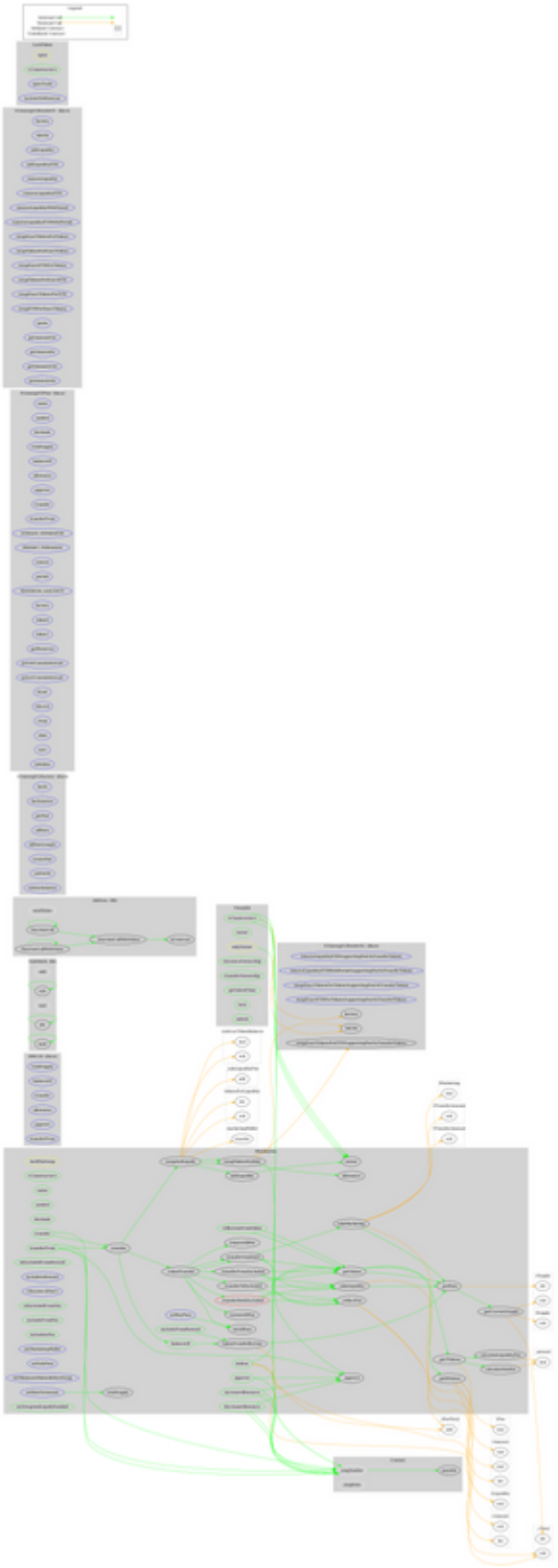
	PERMIT_TYPEHASH	External		-
	nonces	External		-
	permit	External	✓	-
	MINIMUM_LIQUIDITY	External		-
	factory	External		-
	token0	External		-
	token1	External		-
	getReserves	External		-
	price0CumulativeLast	External		-
	price1CumulativeLast	External		-
	kLast	External		-
	ttbcurn	External	✓	-
	swap	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	✓	-
LockToken	Implementation	Ownable		
	<Constructor>	Public	✓	-
	openTrade	External	✓	onlyOwner
	includeToWhiteList	External	✓	onlyOwner
MonkeyInu	Implementation	Context, IERC20, 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		-
	deliver	Public	✓	-
	reflectionFromToken	Public		-
	tokenFromReflection	Public		-
	excludeFromReward	Public	✓	onlyOwner
	includeInReward	External	✓	onlyOwner
	_transferBothExcluded	Private	✓	
	<Receive Ether>	External	Payable	-
	_reflectFee	Private	✓	
	_getValues	Private		
	_getTValues	Private		
	_getRValues	Private		
	_getRate	Private		
	_getCurrentSupply	Private		
	_takeLiquidity	Private	✓	
	calculateLiquidityFee	Private		
	calculateTaxFee	Private		
	removeAllFee	Private	✓	
	restoreAllFee	Private	✓	
	isExcludedFromFee	Public		-
	_approve	Private	✓	
	_transfer	Private	✓	open
	swapAndLiquify	Private	✓	lockTheSwap
	swapTokensForBnb	Private	✓	
	addLiquidity	Private	✓	
	_tokenTransfer	Private	✓	
	_transferStandard	Private	✓	
	takeMarketing	Private	✓	
	_transferToExcluded	Private	✓	
	_transferFromExcluded	Private	✓	
	excludeFromFee	Public	✓	onlyOwner
	includeInFee	Public	✓	onlyOwner
	setMarketingWallet	External	✓	onlyOwner
	setAllFees	Private	✓	

	setBuyFees	External	✓	onlyOwner
	setSaleFees	External	✓	onlyOwner
	setMinimumTokensBeforeSwap	External	✓	onlyOwner
	setMaxTxAmount	External	✓	onlyOwner
	setSwapAndLiquifyEnabled	Public	✓	onlyOwner

Contract Flow



Domain Info

Domain Name	monkeyinu.io
Registry Domain ID	c372632a9140404e860cc66017fec653-DONUTS
Creation Date	2022-03-31T19:07:25Z
Updated Date	2022-04-11T12:16:39Z
Registry Expiry Date	2023-03-31T19:07:25Z
Registrar WHOIS Server	whois.godaddy.com/
Registrar URL	http://www.godaddy.com/domains/search.aspx?ci=8990
Registrar	GoDaddy.com, LLC
Registrar IANA ID	146

The domain has been created in 9 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 and manipulating fees. The contract can be converted into a honeypot and prevent users from selling if the owner abuses the admin functions. 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