Cyberscope

Audit Report

Basenji Inu

August 2022

Type	BEP20
Network	BSC
Address	0x3dc5c2cb81e8814ecd69175fa8a96c1da370410f
Audited by	© cyberscope

Table of Contents

Contract Review

Contract Name	Basenji
Compiler Version	v0.8.15+commit.e14f2714
Optimization	200 runs
Licence	MIT
Explorer	https://bscscan.com/token/0x3dc5c2cb81e8814ecd69175fa8a96c1da370410f
Symbol	BASENJI
Decimals	9
Total Supply	1,000,000,000
Domain	https://basenjiinu.com

Source Files

Filename	**SHA256**
contract.sol	5c7b3657c4ea2de3073af9f833438bbc1ae58abc9bcca2670ccdde75539dc0fb

Audit Updates

Initial Audit	17th August 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	medium
Location	contract.sol#L406

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 launchTimestamp to the maximum amount.

```
function transferWithFee(
        address sender,
        address recipient,
        uint amount
    ) private {
        require(block.timestamp >= launchTimestamp);
```

Recommendation

The contract could embody a check for not allowing setting the launchTimestamp less than a reasonable amount. A suggested implementation could not allow launchTimestamp to be updated after the launch.

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#L604

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 `swapContractToken` methods.

```
function swapContractToken(uint treshold) external onlyOwner {
    uint prevTreshold = _swapTreshold;

    _swapTreshold = treshold;

    _swapContractToken(true);

    _swapTreshold = prevTreshold;
}
```

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

Severity	Code	Description
	STC	Succeeded Transfer Check
	FSA	Fixed Swap Address
	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
	L13	Divide before Multiply Operation
	L15	Local Scope Variable Shadowing

STC - Succeeded Transfer Check

Criticality	minor
Location	contract.sol#L188,809

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.

```
WETH.transfer(address(pair), WETH.balanceOf(address(this)));

IBEP20(token).transfer(
        msg.sender,
        IBEP20(token).balanceOf(address(this))
);
```

Recommendation

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

FSA - Fixed Swap Address

Criticality	minor
Location	contract.sol#L317

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.

```
constructor() {
    address tokenAddress=address(this);
    address WETH=pancakeRouter.WETH();
    dexPair = IPancakeFactory(pancakeRouter.factory()).createPair(
        tokenAddress,
        WETH
    );
```

Recommendation

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

L01 - Public Function could be Declared External

Criticality	minor
Location	contract.sol#L784,119,679,753,668,802,128,579

Description

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

```
isOverLiquified
transferOwnership
RescueTokens
setExcludedFromFee
getInfo
setLaunchInSeconds
renounceOwnership
LockLiquidityForSeconds
```

Recommendation

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

L02 - State Variables could be Declared Constant

Criticality	minor
Location	contract.sol#L438

Description

Constant state variables should be declared constant to save gas.

```
MemeswapDiscount
```

Recommendation

Add the constant attribute to state variables that never change.

L04 - Conformance to Solidity Naming Conventions

Criticality	minor
Location	contract.sol#L646,231,159,247,77,235,168,212,169,282,152,278,643,249,160,353,438,459,644,214,253,802,519,208,219,439,202,210,81,146,642,450,153,223,149,276,198,200,740,145,257,641,645,245,194,216,632,227,591,784,243,788,164,523,683

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.

```
Timestamp
ListToken
SharesFromTokens
SetMarketingWallet
SetUnlockTimestamp
DividentMagnifier
LockLiquidityForSeconds
ReflectTokens
_liquifyTreshold
...
```

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#L269

Description

There are segments that contain unused state variables.

```
_pancakeRouter
```

Recommendation

Remove unused state variables.

L07 - Missing Events Arithmetic

Criticality	minor
Location	contract.sol#L600,160

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.

```
MarketingTax = MarketingTax_
_swapTreshold = treshold
```

Recommendation

Emit an event for critical parameter changes.

L13 - Divide before Multiply Operation

Criticality	minor
Location	contract.sol#L402,640

Description

Performing divisions before multiplications may cause lose of prediction.

```
maxTax = (TAX_DENOMINATOR / 100) * 11
TaxedAmount = (amount * tax) / TAX_DENOMINATOR
```

Recommendation

The multiplications should be prior to the divisions.

L15 - Local Scope Variable Shadowing

Criticality	minor
Location	contract.sol#L643

Description

The are variables that are defined in the local scope containing the same name from an upper scope.

```
Transfer
```

Recommendation

The local variables should have different names from the upper scoped variables.

Contract Functions

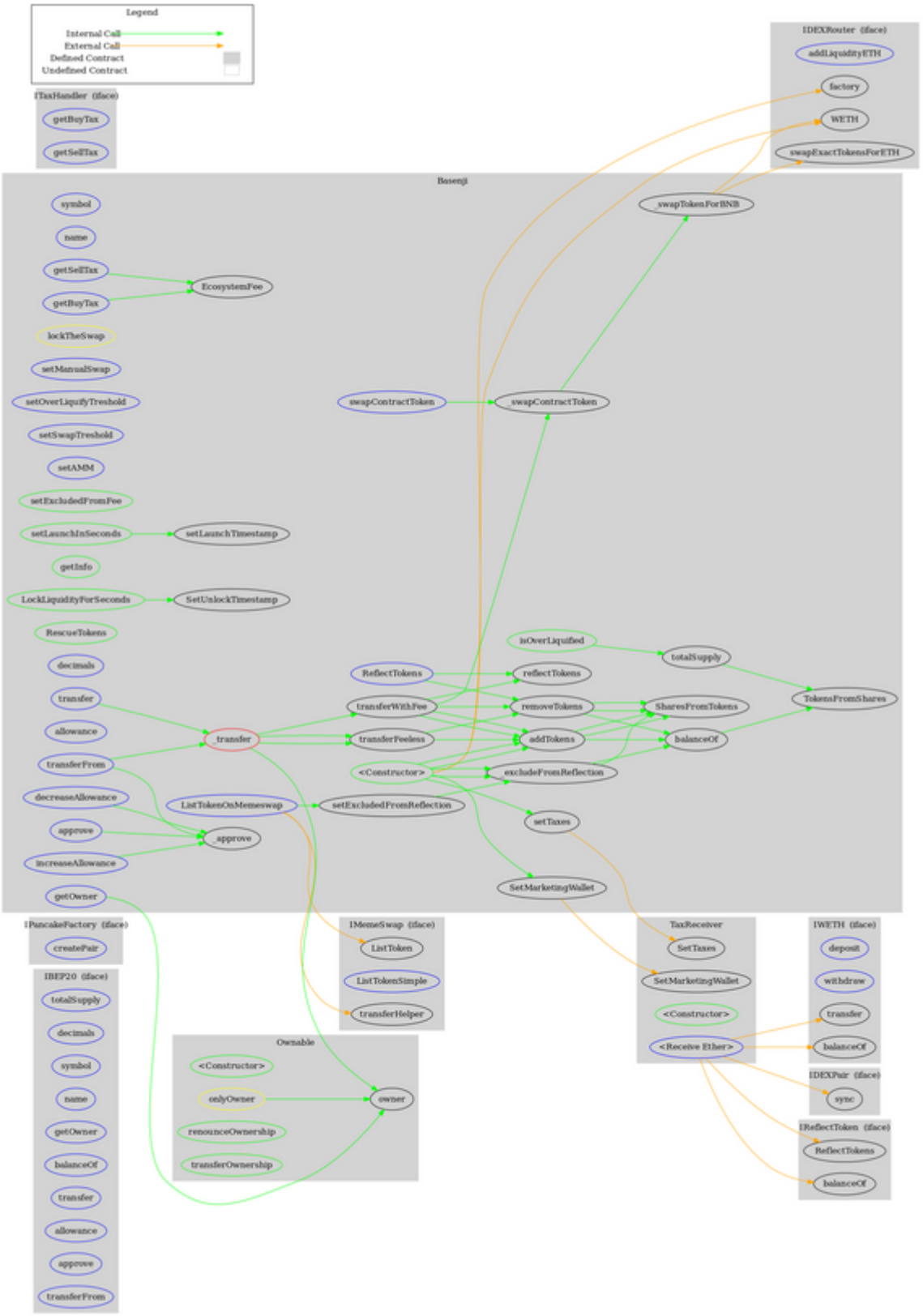
Contract	Type	Bases		
	Function Name	Visibility	Mutability	Modifiers
IBEP20	Interface			
	totalSupply	External		-
	decimals	External		-
	symbol	External		-
	name	External		-
	getOwner	External		-
	balanceOf	External		-
	transfer	External	✓	-
	allowance	External		-
	approve	External	✓	-
	transferFrom	External	✓	-
IPancakeFactory	Interface			
	createPair	External	✓	-
IDEXRouter	Interface			
	addLiquidityETH	External	Payable	-
	swapExactTokensForETH	External	✓	-
	factory	External		-
	WETH	External		-
Ownable	Implementation			
	<Constructor>	Public	✓	-
	owner	Public		-
	renounceOwnership	Public	✓	onlyOwner
	transferOwnership	Public	✓	onlyOwner
IWETH	Interface	IBEP20		

	deposit	External	Payable	-
	withdraw	External	✓	-
IDEXPair	Interface			
	sync	External	✓	-
ITaxHandler	Interface			
	getBuyTax	External		-
	getSellTax	External		-
IReflectToken	Interface	IBEP20		
	ReflectTokens	External	✓	-
IMemeSwap	Interface			
	ListToken	External	✓	-
	ListTokenSimple	External	✓	-
	transferHelper	External		-
TaxReceiver	Implementation			
	SetTaxes	External	✓	-
	SetMarketingWallet	External	✓	-
	<Constructor>	Public	✓	-
	<Receive Ether>	External	Payable	-
Basenji	Implementation	Ownable, IBEP20, ITaxHandler		
	symbol	External		-
	name	External		-
	<Constructor>	Public	✓	-
	ListTokenOnMemeswap	External	✓	onlyOwner
	_transfer	Private	✓	
	transferFeeless	Private	✓	
	transferWithFee	Private	✓	
	getBuyTax	External		-

	getSellTax	External		-
	EcosystemFee	Private		
	addTokens	Private	✓	
	removeTokens	Private	✓	
	reflectTokens	Private	✓	
	TokensFromShares	Public		-
	SharesFromTokens	Public		-
	_swapContractToken	Private	✓	lockTheSwap
	_swapTokenForBNB	Private	✓	
	isOverLiquified	Public		-
	ReflectTokens	External	✓	-
	swapContractToken	External	✓	onlyOwner
	setManualSwap	External	✓	onlyOwner
	setOverLiquifyTreshold	External	✓	onlyOwner
	setSwapTreshold	External	✓	onlyOwner
	setAMM	External	✓	onlyOwner
	setTaxes	Public	✓	onlyOwner
	setExcludedFromFee	Public	✓	onlyOwner
	setLaunchInSeconds	Public	✓	onlyOwner
	setLaunchTimestamp	Public	✓	onlyOwner
	setExcludedFromReflection	Public	✓	onlyOwner
	_excludeFromReflection	Private	✓	
	SetMarketingWallet	Public	✓	onlyOwner
	getInfo	Public		-
	LockLiquidityForSeconds	Public	✓	onlyOwner
	SetUnlockTimestamp	Public	✓	onlyOwner
	RescueTokens	Public	✓	onlyOwner
	decimals	External		-
	getOwner	External		-
	balanceOf	Public		-
	totalSupply	Public		-
	allowance	External		-
	approve	External	✓	-
	_approve	Private	✓	

	transfer	External	✓	-
	transferFrom	External	✓	-
	increaseAllowance	External	✓	-
	decreaseAllowance	External	✓	-

Contract Flow



Domain Info

Domain Name	
Registry Domain ID	2715796800_DOMAIN_COM-VRSN
Creation Date	2022-08-03T19:57:14.00Z
Updated Date	0001-01-01T00:00:00.00Z
Registry Expiry Date	2023-08-03T19:57:14.00Z
Registrar WHOIS Server	whois.namecheap.com
Registrar URL	http://www.namecheap.com
Registrar	NAMECHEAP INC
Registrar IANA ID	1068

The domain has been created in 12 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 transferring funds to the team’s wallet. 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 11% fees.

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