Cyberscope

Audit Report

Betswamp

March 2022

Type	BEP20
Network	BSC
Address	0xa8614ae1c909331B67C564fE0c05826714bd300E
Audited by	© cyberscope

Table of Contents

Contract Review

Contract Name	BetSwampERC20Token
Compiler Version	v0.7.5+commit.eb77ed08
Optimization	200 runs
Licence	Unknown
Explorer	https://bscscan.com/token/0xa8614ae1c909331B67C564fE0c05826714bd300E
Symbol	BETS
Decimals	9
Total Supply	1,140,000
Domain	betswamp.com

Source Files

Filename	**SHA256**
contract.sol	3549cb9b56c5f278067bce2b951ac97794b4681b47dd2eed9b00b44189660897

Audit Updates

Initial Audit	8th March 2022
Corrected	28th June 2022

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#L1363

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 `tradingActive` to false.

```
if(!tradingActive){
    require(_isExcludedFromFees[from] || _isExcludedFromFees[to], "Trading is
not active.");
  }
```

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.

MT - Mint Tokens

Criticality	critical
Location	contract.sol#L1229

Description

The contract owner has the authority to mint tokens. The owner may take advantage of it by calling the `mint` function. As a result the contract tokens will be highly inflated.

```
function mint(address account_, uint256 amount_) external onlyVault() {
      if(msg.sender == _vault)
      _mint(account_, amount_);
  }
```

Recommendation

The owner should carefully manage the credentials of the owner's account. We advised considering an extra-strong security mechanism that the actions may be quarantined by many users instead of one. The owner could also renounce the contract ownership for a period of time or pass the access to the zero address.

BC - Blacklisted Contracts

Criticality	critical
Location	contract.sol#L1273

Description

The contract owner has the authority to stop contracts from selling. The owner may take advantage of it by calling the `blacklistAddress` function while the burn fee is very high value. This will result in burning the tokens instead of selling them.

```
    function blackListAddresses(address[] memory addrs) external onlyOwner
returns (bool) {
        require(block.timestamp <= tradingActiveBlock + 28800, "Option
expired!");
        for(uint256 i = 0; i < addrs.length; i++) {
            _blackListAddr[addrs[i]] = true;
        }
        return 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
	CO	Code Optimization
	L01	Public Function could be Declared External
	L04	Conformance to Solidity Naming Conventions
	L05	Unused State Variable
	L06	Missing Events Access Control
	L07	Missing Events Arithmetic
	L09	Dead Code Elimination
	L15	Local Scope Variable Shadowing

CO - Code Optimization

Criticality	minor
Location	contract.sol#L1386

Description

Variable `swapping` will be always assigned to *false* inside the `if` statement

```
if(
    !swapping &&
    !automatedMarketMakerPairs[from] &&
    !_isExcludedFromFees[from] &&
    !_isExcludedFromFees[to]
) {
    swapping = true;
    swapping = false;
}

bool takeFee = !swapping;

// if any account belongs to _isExcludedFromFee account then remove the fee
if(_isExcludedFromFees[from] || _isExcludedFromFees[to]) {
    takeFee = false;
}
bool takeFee = !_isExcludedFromFees[from] && !_isExcludedFromFees[to]
```

Recommendation

The above code segment could be rewritten into the below:

```
bool takeFee = !_isExcludedFromFees[from] && !_isExcludedFromFees[to]
```

L01 - Public Function could be Declared External

Criticality	minor
Location	contract.sol#L774,778,782,790,799,804,810,815,922,945,969,978,1000,1234,1238,1329,1333

Description

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

```
setAutomatedMarketMakerPair
isExcludedFromFees
burnFrom
burn
vault
renounceOwnership
owner
nonces
permit
...
```

Recommendation

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

L04 - Conformance to Solidity Naming Conventions

Criticality	minor
Location	contract.sol#L747,750,753,756,759,762,903,960,992,1029,1293,1345,1171,1184

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.

```
_isExcludedMaxTransactionAmount
deadAddress
_burnFrom
_fee
WETH
_vault
_owner
DOMAIN_SEPARATOR
_decimals
...
```

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#L744

Description

There are segments that contain unused state variables.

```
ERC20TOKEN_ERC1820_INTERFACE_ID
```

Recommendation

Remove unused state variables.

L06 - Missing Events Access Control

Criticality	minor
Location	contract.sol#L994

Description

Detected missing events for critical access control parameters. There are functions that have no event emitted, so it is difficult to track off-chain changes.

```
_vault = vault_
```

Recommendation

Emit an event for critical parameter changes.

L07 - Missing Events Arithmetic

Criticality	minor
Location	contract.sol#L1293,1299,1304,1309,1314

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.

```
burnFeeOnBuy = newBurnFeeOnBuy
burnFeeOnSell = newBurnFeeOnSell
maxWallet = newNum
maxTransactionAmount = newNum
blackListFee = _fee
```

Recommendation

Emit an event for critical parameter changes.

L09 - Dead Code Elimination

Criticality	minor
Location	contract.sol#L551,511,521,536,546,458,485,875,29,105,84,110,119,91,47,306,239,175,432,380,285,218,154,411,359,314,243,179,325,253,187,292,225,161,418,366,278,211,147,404,352,725,734,713,721,730,700,717

Description

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

```
substractPercentage
sqrrt
quadraticPricing
percentageOfTotal
percentageAmount
bondingCurve
average
remove
length
...
```

Recommendation

Remove unused functions.

L15 - Local Scope Variable Shadowing

Criticality	minor
Location	contract.sol#L1210

Description

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

```
totalSupply
```

Recommendation

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

Contract Functions

Contract	Type	Bases		
	Function Name	Visibility	Mutability	Modifiers
EnumerableSet	Library			
	_add	Private	✓	
	_remove	Private	✓	
	_contains	Private		
	_length	Private		
	_at	Private		
	_getValues	Private		
	_insert	Private	✓	
	add	Internal	✓	
	remove	Internal	✓	
	contains	Internal		
	length	Internal		
	at	Internal		
	getValues	Internal		
	insert	Internal	✓	
	add	Internal	✓	
	remove	Internal	✓	
	contains	Internal		
	length	Internal		
	at	Internal		
	getValues	Internal		
	insert	Internal	✓	
	add	Internal	✓	
	remove	Internal	✓	
	contains	Internal		
	length	Internal		
	at	Internal		
	getValues	Internal		

	insert	Internal	✓	
	add	Internal	✓	
	remove	Internal	✓	
	contains	Internal		
	length	Internal		
	at	Internal		
	add	Internal	✓	
	remove	Internal	✓	
	contains	Internal		
	length	Internal		
	at	Internal		
Address	Library			
	isContract	Internal		
	sendValue	Internal	✓	
	functionCall	Internal	✓	
	functionCall	Internal	✓	
	functionCallWithValue	Internal	✓	
	functionCallWithValue	Internal	✓	
	_functionCallWithValue	Private	✓	
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		

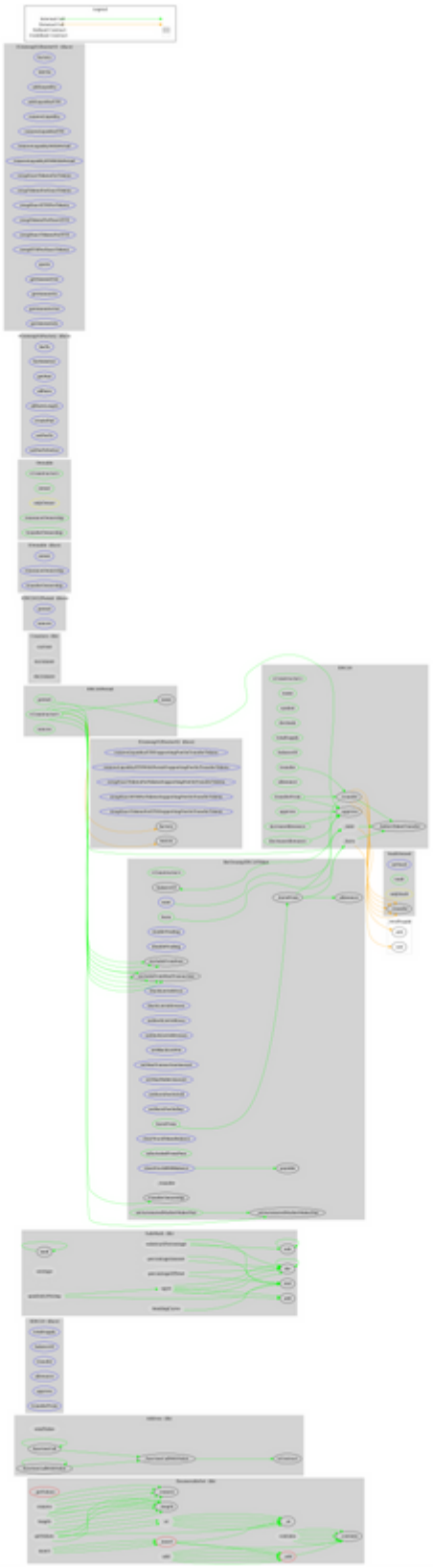
	div	Internal		
	mod	Internal		
	mod	Internal		
	sqrrt	Internal		
	percentageAmount	Internal		
	substractPercentage	Internal		
	percentageOfTotal	Internal		
	average	Internal		
	quadraticPricing	Internal		
	bondingCurve	Internal		
ERC20	Implementation	IERC20		
	<Constructor>	Public	✓	-
	name	Public		-
	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	✓	
Counters	Library			
	current	Internal		
	increment	Internal	✓	
	decrement	Internal	✓	

IERC2612Permit	Interface			
	permit	External	✓	-
	nonces	External		-
ERC20Permit	Implementation	ERC20, IERC2612Permit		
	<Constructor>	Public	✓	-
	permit	Public	✓	-
	nonces	Public		-
IOwnable	Interface			
	owner	External		-
	renounceOwnership	External	✓	-
	transferOwnership	External	✓	-
Ownable	Implementation	IOwnable		
	<Constructor>	Public	✓	-
	owner	Public		-
	renounceOwnership	Public	✓	onlyOwner
	transferOwnership	Public	✓	onlyOwner
VaultOwned	Implementation	Ownable		
	setVault	External	✓	onlyOwner
	vault	Public		-
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	✓	-

BetSwampERC20Token	Implementation	IERC20, ERC20Permit, VaultOwned		
	<Constructor>	Public	✓	ERC20
	mint	External	✓	onlyVault
	burn	Public	✓	-
	burnFrom	Public	✓	-
	enableTrading	External	✓	onlyOwner
	disableTrading	External	✓	onlyOwner
	excludeFromFees	Public	✓	onlyOwner
	excludeFromMaxTransaction	Public	✓	onlyOwner
	blackListAddress	External	✓	onlyOwner
	blackListAddresses	External	✓	onlyOwner
	unblackListAddress	External	✓	onlyOwner
	unblackListAddresses	External	✓	onlyOwner
	setBlackListFee	External	✓	onlyOwner
	setMaxTransactionAmount	External	✓	onlyOwner
	setMaxWalletAmount	External	✓	onlyOwner
	setBurnFeeOnSell	External	✓	onlyOwner
	setBurnFeeOnBuy	External	✓	onlyOwner
	clearStuckBNBBalance	External	✓	onlyOwner
	clearStuckTokenBalance	External	✓	onlyOwner
	isExcludedFromFees	Public		-
	setAutomatedMarketMakerPair	Public	✓	onlyOwner
	_setAutomatedMarketMakerPair	Private	✓	
	_burnFrom	Public	✓	-
	_transfer	Internal	✓	

Contract Flow



Domain Info

Domain Name	betswamp.com
Registry Domain ID	2624723449_DOMAIN_COM-VRSN
Creation Date	2021-07-06T10:54:28.00Z
Updated Date	0001-01-01T00:00:00.00Z
Registry Expiry Date	
Registrar WHOIS Server	whois.namecheap.com
Registrar URL	http://www.namecheap.com
Registrar	NAMECHEAP INC
Registrar IANA ID	1068

The domain has been created 8 months before the creation of the audit.

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

Summary

Betswamp is an interesting project that has a friendly and growing community. There are some functions that can be abused by the owner, like minting tokens, stopping transactions and mass blacklisting wallets from selling. 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 provides all the essential tools to assist users draw their own conclusions.

The Cyberscope team

https://www.cyberscope.io