Cyberscope

Audit Report

Futuball

November 2022

Type	BEP20
Network	BSC
Address	0xBB4BbeEa97Ec14406Fb75aa43AaB02D7ef6b35b4
Audited by	© cyberscope

Table of Contents

Contract Review

Contract Name	FutuballToken
Compiler Version	v0.8.4+commit.c7e474f2
Optimization	1 runs
Explorer	https://bscscan.com/token/0xBB4BbeEa97Ec14406Fb75aa43AaB02D7ef6b35b4
Symbol	FB
Decimals	18
Total Supply	100,000,000
Domain	futuball.io

Source Files

Filename	**SHA256**
contract.sol	d7a9f1edd9b1a9349cd9a28dd7b35df278e9c4b07c1164f174337d675ddf56e3

Audit Updates

Initial Audit	5th November 2022
Corrected	

Contract Analysis

● Critical ● Medium ● Minor / Informative ● Pass

Severity	Code	Description	Status
●	ST	Stops Transactions	Unresolved
●	OCTD	Transfers Contract's Tokens	Passed
●	OTUT	Transfers User's Tokens	Passed
●	ELFM	Exceeds Fees Limit	Unresolved
●	ULTW	Transfers Liquidity to Team Wallet	Passed
●	MT	Mints Tokens	Passed
●	BT	Burns Tokens	Passed
●	BC	Blacklists Addresses	Passed

ST - Stops Transactions

Criticality	critical
Location	contract.sol#L955,926
Status	Unresolved

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 `buyTaxFee` to a high value. As a result, the contract may operate as a honeypot.

```
if(sender == pairAddress) {
    taxFee = amount.mul(buyTaxFee).div(10000);
}
```

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

```
if (!(addLPaddress[sender] || addLPaddress[recipient]))
        { require(amount <= antiBotAmount, "antiBot"); }
```

Recommendation

The contract could embody a check for not allowing setting the ‘antiBotAmount’ 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.

Read more about the fees manipulation.

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 - Exceeds Fees Limit

Criticality	critical
Location	contract.sol#L731
Status	Unresolved

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 `setTax` function with a high percentage value.

```
function setTax(uint256 _sellTaxFee, uint256 _buyTaxFee) public onlyOwner{
    sellTaxFee = _sellTaxFee;
    buyTaxFee = _buyTaxFee;
}
```

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 / Informative

Severity	Code	Description	Status
●	TSD	Total Supply Diversion	Unresolved
●	L02	State Variables could be Declared Constant	Unresolved
●	L04	Conformance to Solidity Naming Conventions	Unresolved
●	L07	Missing Events Arithmetic	Unresolved

TSD - Total Supply Diversion

Criticality	critical
Location	contract.sol#L976
Status	Unresolved

Description

The taxed amount is added to the contract's address but it is not subtracted from the recipient's amount. As a result, the sum of balances is diverted from the total supply and the contract's balance is violated.

```
taxFee = amount.mul(buyTaxFee).div(10000);
...
_balances[address(this)] = _balances[address(this)].add(taxFee);
...
_balances[recipient] = _balances[recipient].add(amount);
```

Recommendation

The sum of balances should always be equal with the total supply.

L02 - State Variables could be Declared Constant

Criticality	minor / informative
Location	contract.sol#L650,651,652
Status	Unresolved

Description

Constant state variables should be declared constant to save gas.

```
_name
_symbol
_initSupply
```

Recommendation

Add the constant attribute to state variables that never change.

L04 - Conformance to Solidity Naming Conventions

Criticality	minor / informative
Location	contract.sol#L708,731,696,434,727,670
Status	Unresolved

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.

```
_amount
_buyTaxFee
_sellTaxFee
_duration
_address
WETH
_taxAddress
_router
```

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 / informative
Location	contract.sol#L708,731
Status	Unresolved

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.

```
antiBotAmount = _amount
sellTaxFee = _sellTaxFee
```

Recommendation

Emit an event for critical parameter changes.

Contract Functions

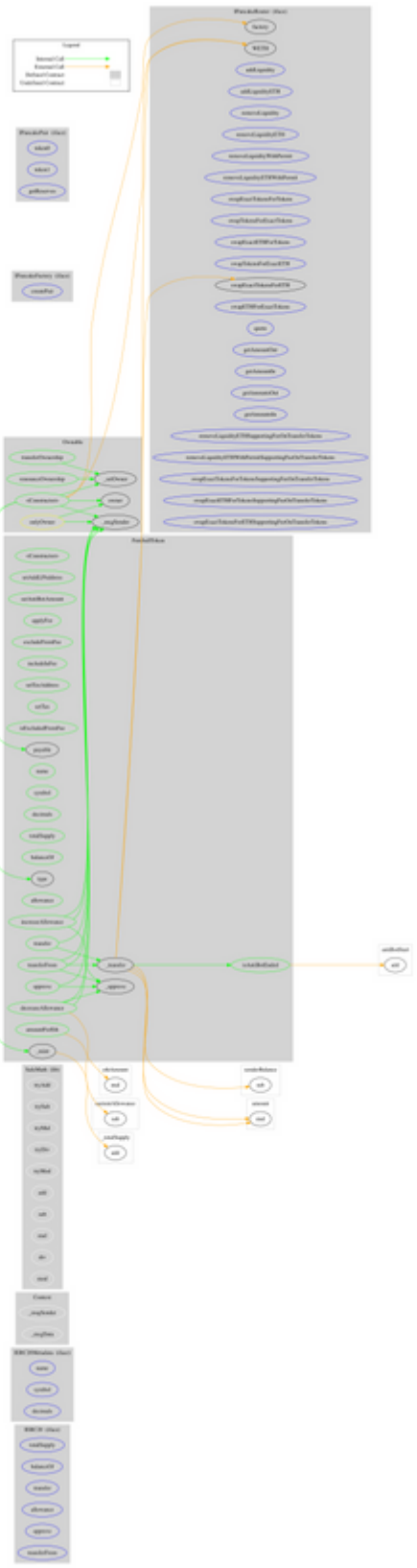
Contract	Type	Bases		
	Function Name	Visibility	Mutability	Modifiers
IERC20	Interface			
	totalSupply	External		-
	balanceOf	External		-
	transfer	External	✓	-
	allowance	External		-
	approve	External	✓	-
	transferFrom	External	✓	-
IERC20Metadata	Interface	IERC20		
	name	External		-
	symbol	External		-
	decimals	External		-
Context	Implementation			
	_msgSender	Internal		
	_msgData	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		
Ownable	Implementation	Context		
	<Constructor>	Public	✓	-
	owner	Public		-
	renounceOwnership	Public	✓	onlyOwner
	transferOwnership	Public	✓	onlyOwner
	_setOwner	Private	✓	
IPancakeFactory	Interface			
	createPair	External	✓	-
IPancakeRouter	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		-

	removeLiquidityETHSupportingFeeOnTransferTokens	External	✓	-
	removeLiquidityETHWithPermitSupportingFeeOnTransferTokens	External	✓	-
	swapExactTokensForTokensSupportingFeeOnTransferTokens	External	✓	-
	swapExactETHForTokensSupportingFeeOnTransferTokens	External	Payable	-
	swapExactTokensForETHSupportingFeeOnTransferTokens	External	✓	-
IPancakePair	Interface			
	token0	External		-
	token1	External		-
	getReserves	External		-
FutuballToken	Implementation	Context, IERC20, IERC20Metadata, Ownable		
	<Constructor>	Public	✓	-
	setAddLPAddress	Public	✓	onlyOwner
	isAntiBotEnded	Public		-
	setAntiBotAmount	Public	✓	onlyOwner
	applyFee	Public	✓	onlyOwner
	excludeFromFee	Public	✓	onlyOwner
	includeInFee	Public	✓	onlyOwner
	setTaxAddress	Public	✓	onlyOwner
	setTax	Public	✓	onlyOwner
	isExcludedFromFee	Public		-
	amountForEth	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	✓	
	_approve	Internal	✓	

Contract Flow



Domain Info

Domain Name	futuball.io
Registry Domain ID	4e2a25d6eadd46f29da4688e7ba1dd52-DONUTS
Creation Date	2022-09-19T15:30:04Z
Updated Date	2022-09-24T15:30:18Z
Registry Expiry Date	2023-09-19T15:30:04Z
Registrar WHOIS Server	whois.namecheap.com
Registrar URL	https://www.namecheap.com/
Registrar	NameCheap, Inc.
Registrar IANA ID	1068

The domain was created about 2 months before the creation of the audit. It will expire in 11 months.

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 some of the potential hacks. Temporarily locking the contract or renouncing ownership will eliminate some of 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