Cyberscope

Audit Report

ButterFinance

August 2022

Type	BEP20
Network	BSC
Address	0xCE5D85177feCC3d7c824Dbf0790B4eaC1A472BCe
Audited by	© cyberscope

Table of Contents

Contract Review

Contract Name	ButterToken
Compiler Version	v0.8.4+commit.c7e474f2
Optimization	200 runs
Explorer	https://bscscan.com/token/0xCE5D85177feCC3d7c824Dbf0790B4eaC1A472BCe
Symbol	BUTTER
Decimals	18
Total Supply	10,000,000
Domain	butterfinance.io

Audit Updates

Initial Audit	23rd August 2022
Corrected	

Source Files

Filename	SHA256
@openzeppelin/contracts/access/Ownable.sol	75e3c97011e75627ffb36f4a2799a4e887e1a3e27ed427490e82d7b6f51cc5c9
@openzeppelin/contracts/token/ERC20/ERC20.sol	bea6ecb4a800d648b1f77708cbb12a7e86a5547965a0a4e041925dbff07d13e9
@openzeppelin/contracts/token/ERC20/extensions/ERC20Burnable.sol	046d05ab1bd0452f2a5abed929383c4b29e0b69fda9e1f1c4d5e7d31ccf99637
@openzeppelin/contracts/token/ERC20/extensions/IERC20Metadata.sol	af5c8a77965cc82c33b7ff844deb9826166689e55dc037a7f2f790d057811990
@openzeppelin/contracts/token/ERC20/IERC20.sol	6eacf8ca56b41b7636489c0996d8f9608b4d298879a1fd5d876f21ad7a6711f1
@openzeppelin/contracts/utils/Context.sol	1458c260d010a08e4c20a4a517882259a23a4baa0b5bd9add9fb6d6a1549814a
contracts/ButterToken.sol	fb71d001f691ba4a926e4d9d24bf52344d6f30b0dbd70ddefef778a0a55447aa

Contract Analysis

● Critical   ● Medium   ● Minor / Informative   ● Pass

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

Contract Diagnostics

● Critical   ● Medium   ● Minor / Informative

Severity	Code	Description	Status
●	L01	Public Function could be Declared External	Unresolved
●	L04	Conformance to Solidity Naming Conventions	Unresolved
●	L07	Missing Events Arithmetic	Unresolved
●	L08	Tautology or Contradiction	Unresolved
●	L11	Unnecessary Boolean equality	Unresolved
●	L13	Divide before Multiply Operation	Unresolved

L01 - Public Function could be Declared External

Criticality	minor / informative
Location	contracts/ButterToken.sol#L49,58,21,32,40,28
Status	Unresolved

Description

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

```
toggleTaxExemptionOnTo
toggleTaxExemptionOnFrom
changeFees
toggleLiqPools
toggleTaxExemption
changeFeeAddress
```

Recommendation

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

L04 - Conformance to Solidity Naming Conventions

Criticality	minor / informative
Location	contracts/ButterToken.sol#L15,14,12,10,11,13
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.

```
_liqPools
_taxExemptionFrom
_taxExemption
TaxFee
FeeAddress
_taxExemptionTo
```

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	contracts/ButterToken.sol#L21
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.

```
TaxFee = tax
```

Recommendation

Emit an event for critical parameter changes.

L08 - Tautology or Contradiction

Criticality	minor / informative
Location	contracts/ButterToken.sol#L21
Status	Unresolved

Description

Detects expressions that are tautologies or contradictions. For instance, an uint variable will always be greater than or equal to zero.

```
require(bool,string)(tax >= 0,You cannot set the fee below 0%)
```

Recommendation

Fix the incorrect comparison by changing the value type or the comparison.

L11 - Unnecessary Boolean equality

Criticality	minor / informative
Location	contracts/ButterToken.sol#L66
Status	Unresolved

Description

The comparison to boolean constants is redundant. Boolean constants can be used directly and do not need to be compared to true or false.

```
_taxExemptionFrom[from] == false
_taxExemptionTo[to] == false
_taxExemption[to] == false
```

Recommendation

Remove the equality to the boolean constant.

L13 - Divide before Multiply Operation

Criticality	minor / informative
Location	contracts/ButterToken.sol#L66
Status	Unresolved

Description

Performing divisions before multiplications may cause lose of prediction.

```
taxamount = amount / 1000 * TaxFee
```

Recommendation

The multiplications should be prior to the divisions.

Contract Functions

Contract	Type	Bases		
	Function Name	**Visibility**	**Mutability**	**Modifiers**
Ownable	Implementation	Context		
	<Constructor>	Public	✓	-
	owner	Public		-
	renounceOwnership	Public	✓	onlyOwner
	transferOwnership	Public	✓	onlyOwner
	_transferOwnership	Internal	✓	
ERC20	Implementation	Context, IERC20, IERC20Metadata		
	<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	✓	
	_afterTokenTransfer	Internal	✓	

ERC20Burnable	Implementation	Context, ERC20		
	burn	Public	✓	-
	burnFrom	Public	✓	-
IERC20Metadata	Interface	IERC20		
	name	External		-
	symbol	External		-
	decimals	External		-
IERC20	Interface			
	totalSupply	External		-
	balanceOf	External		-
	transfer	External	✓	-
	allowance	External		-
	approve	External	✓	-
	transferFrom	External	✓	-
Context	Implementation			
	_msgSender	Internal		
	_msgData	Internal		
ButterToken	Implementation	ERC20, ERC20Burnable, Ownable		
	<Constructor>	Public	✓	ERC20
	changeFees	Public	✓	onlyOwner
	changeFeeAddress	Public	✓	onlyOwner
	toggleLiqPools	Public	✓	onlyOwner
	toggleTaxExemption	Public	✓	onlyOwner
	toggleTaxExemptionOnTo	Public	✓	onlyOwner
	toggleTaxExemptionOnFrom	Public	✓	onlyOwner
	_afterTokenTransfer	Internal	✓	

Contract Flow
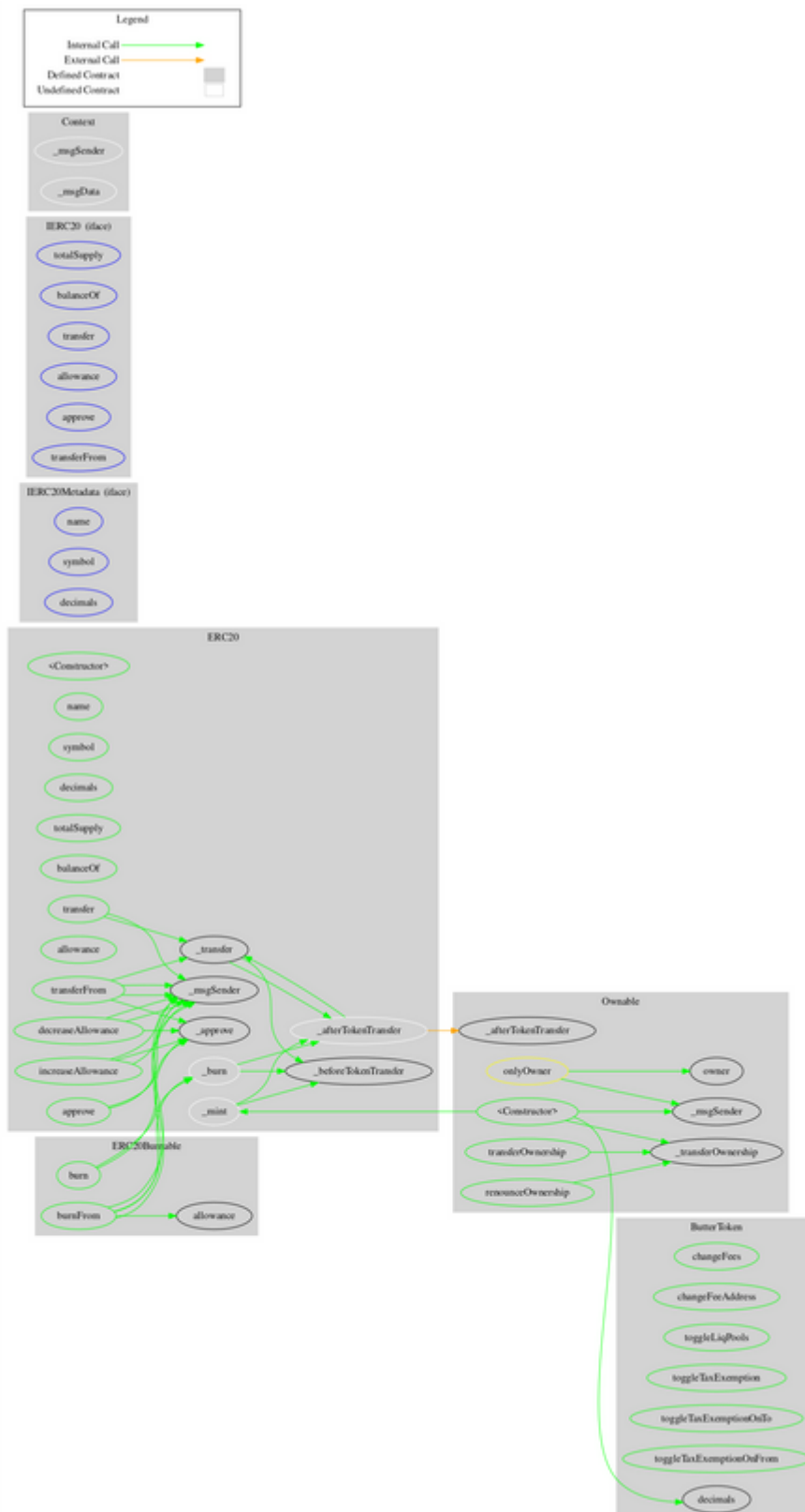
Domain Info

Domain Name	butterfinance.io
Registry Domain ID	539fd7c1c13743d29d0e210b5b84e7cf-DONUTS
Creation Date	2022-04-07T17:32:16Z
Updated Date	2022-04-12T17:32:47Z
Registry Expiry Date	2023-04-07T17:32:16Z
Registrar WHOIS Server	whois.namecheap.com
Registrar URL	https://www.namecheap.com/
Registrar	NameCheap, Inc.
Registrar IANA ID	1068

The domain was created 5 months before the creation of the audit. It will expire in 8 months.

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

Summary

ButterFinance is an interesting project that has a friendly and growing community. The Smart Contract analysis reported no compiler error or critical issues. The contract Owner can access some admin functions that can not be used in a malicious way to disturb the users' transactions. There is also a limit of max 10% 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