



Cyberscope

Audit Report

POLYCOIN

OCTOBER 2022

Type	BEP20
Network	BSC
Address	0x58834bA6FeC3CAc025a72B420A33f289974FA159
Audited by	© cyberscope

Table of Contents

Table of Contents	1
Contract Review	2
Source FiPLYC	2
Audit Updates	2
Contract Analysis	3
MT - Mint Tokens	4
Description	4
Recommendation	4
Contract Diagnostics	5
CO - Code Optimization	6
Description	6
Recommendation	6
L01 - Public Function could be Declared External	7
Description	7
Recommendation	7
L03 - Redundant Statements	8
Description	8
Recommendation	8
Contract Functions	9
Contract Flow	11
Domain Info	12
Summary	13
Disclaimer	14
About Cyberscope.tk	15

Contract Review

Contract Name	POLYCOIN
Compiler Version	v0.8.14+commit.80d49f37
Optimization	200 runs
Licence	MIT
Explorer	https://bscscan.com/token/0x58834bA6FeC3CAa025a72B420A33f289974FA159
Symbol	PLYC
Decimals	9
Total Supply	10,000
Domain	POLYCOIN.TK

Source FiPLYC

Filename	SHA256
contract.sol	0x58834bA6FeC3CAa025a72B420A33f289974FA159

Audit Updates

Initial Audit	19th OCTOBER 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

MT - Mint Tokens

Criticality	critical
Location	contract.sol#L553

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(uint256 amount) public onlyOwner {  
    _mint(msg.sender, 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.

Contract Diagnostics

● Critical ● Medium ● Minor

Severity	Code	Description
●	CO	Code Optimization
●	L01	Public Function could be Declared External
●	L03	Redundant Statements

CO - Code Optimization

Criticality	minor
Location	contract.sol#L325, 149, 606

Description

There are code segments that could be optimized. A segment may be optimized so that it becomes a smaller size, consumes PLYCs memory, executes more rapidly, or performs fewer operations.

```
_totalSupply;
```

Also, the contract uses the `Pausable` contract, in which the `_paused` variable is defined. The owner can modify that value by calling the `pause` and `unpause` functions, but except these functions, the contract does not use any other functionality of the `Pausable` contract.

```
bool private _paused;
```

```
function pause() public onlyOwner {  
    _pause();  
}  
  
function unpause() public onlyOwner {  
    _unpause();  
}
```

Recommendation

Rewrite some code segments so the runtime will be more performant.

L01 - Public Function could be Declared External

Criticality	minor
Location	contract.sol#L261,270,340,348,372,379,391,402,413,431,477,496,553,580,606,610

Description

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

```
unpause
pause
burn
mint
decreaseAllowance
increaseAllowance
transferFrom
approve
allowance
...
```

Recommendation

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

L03 - Redundant Statements

Criticality	minor
Location	contract.sol#L325

Description

Detect the usage of redundant statements that have no effect.

POLYCOIN

Recommendation

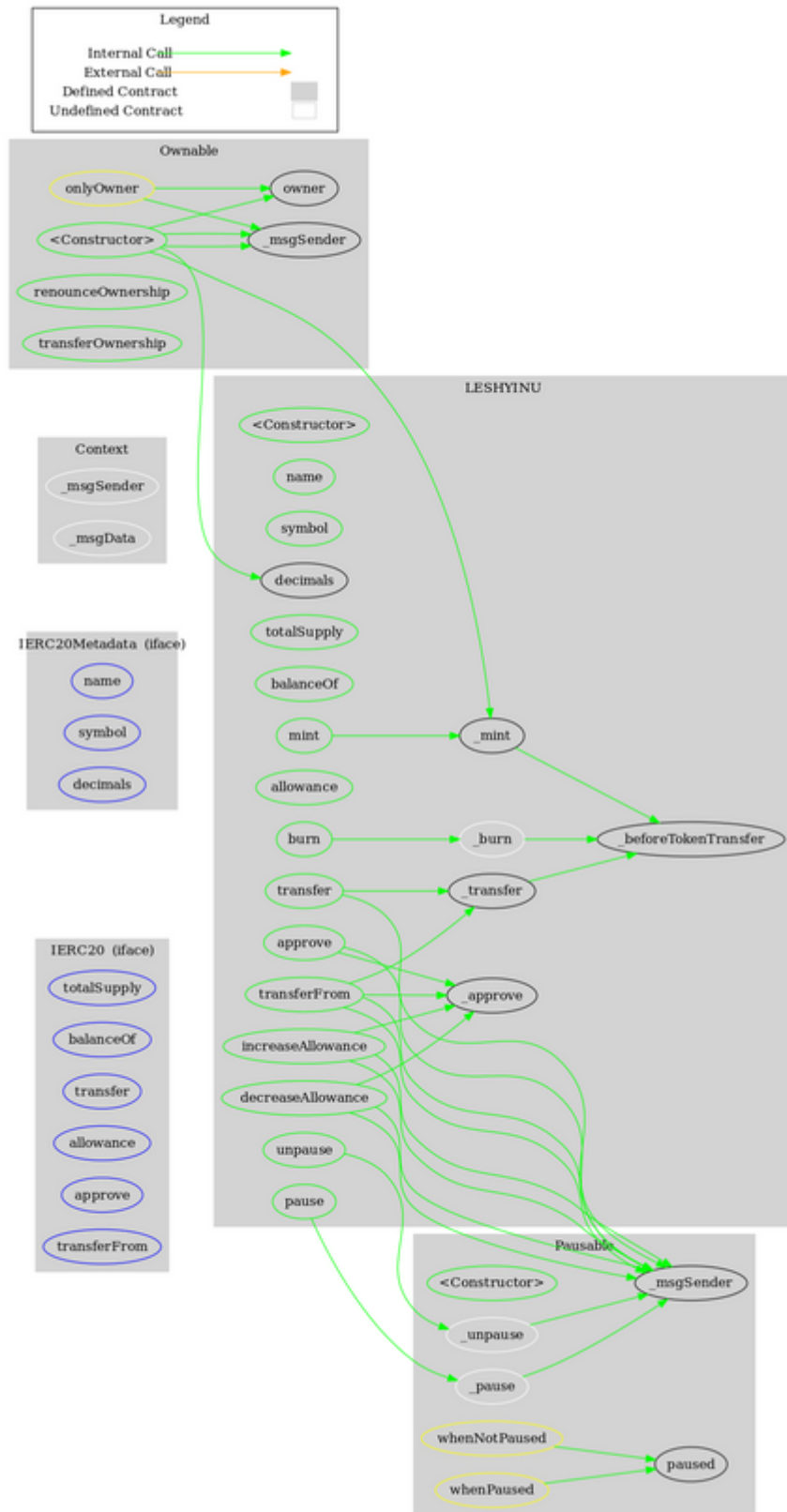
Remove redundant statements if they congest code but offer no value.

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		
Pausable	Implementation	Context		
	<Constructor>	Public	✓	-
	paused	Public		-
	_pause	Internal	✓	whenNotPaused
	_unpause	Internal	✓	whenPaused
Ownable	Implementation	Context		
	<Constructor>	Public	✓	-
	owner	Public		-
	renounceOwnership	Public	✓	onlyOwner

	transferOwnership	Public	✓	onlyOwner
POLYCOIN	Implementation	Context, IERC20, IERC20Met adata, Ownable, Pausable		
	<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	✓	
	mint	Public	✓	onlyOwner
	_burn	Internal	✓	
	burn	Public	✓	onlyOwner
	_approve	Internal	✓	
	pause	Public	✓	onlyOwner
	unpause	Public	✓	onlyOwner
	_beforeTokenTransfer	Internal	✓	

Contract Flow



Domain Info

Domain Name	POLYCOIN.TK
Registry Domain ID	2706661537187_DOMAIN_COM-VRSN
Creation Date	2022-10-10T17:02:43Z
Updated Date	2022-10-10T17:02:43Z
Registry Expiry Date	2022-10-10T17:02:43Z
Registrar WHOIS Server	whois.hostinger.com
Registrar URL	https://www.hostinger.com
Registrar	Hostinger, UAB
Registrar IANA ID	1636456666

The domain has been created 14 days before the creation of the audit. It will expire in 12 months.

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

Summary

The Smart Contract analysis reported one critical severity issue. The contract owner has the authority to mint tokens. The contract tokens will be highly inflated. 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.tk 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.tk 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.tk 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.tk team disclaims any liability for the resulting losses.

About Cyberscope.tk

Coinscope audit and K.Y.C. service has been rebranded to Cyberscope.tk.

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.tk 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.tk team

<https://www.Cyberscope.tk>