Cyberscope

Audit Report

BlueChip Protocol

March 2022

Type	ERC20
Network	ETH
Address	0xf64896032ECa8077A283916f9FE7693383B8a6EB
Audited by	© cyberscope

Table of Contents

Contract Review

Contract Name	BCPToken
Compiler Version	v0.6.6+commit.6c089d02
Optimization	runs
Licence	MIT
Explorer	https://etherscan.io/token/0xf64896032ECa8077A283916f9FE7693383B8a6EB
Symbol	BCP
Decimals	18
Total Supply	1,000,000,000
Domain	blueswap.net

Source Files

Filename	**SHA256**
contract.sol	7c85539fea208179b14efc524fb6c19be20f2bb24311025bb57e4ac82bbfc216

Audit Updates

Initial Audit	30th March 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#L1458

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 to, uint256 amount) public virtual {
        require(hasRole(MINTER_ROLE, _msgSender()), "ERC20PresetMinterPauser:
must have minter role to mint");
        _mint(to, 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

The contract uses basic ERC20 implementations and has no custom code.

Contract Functions

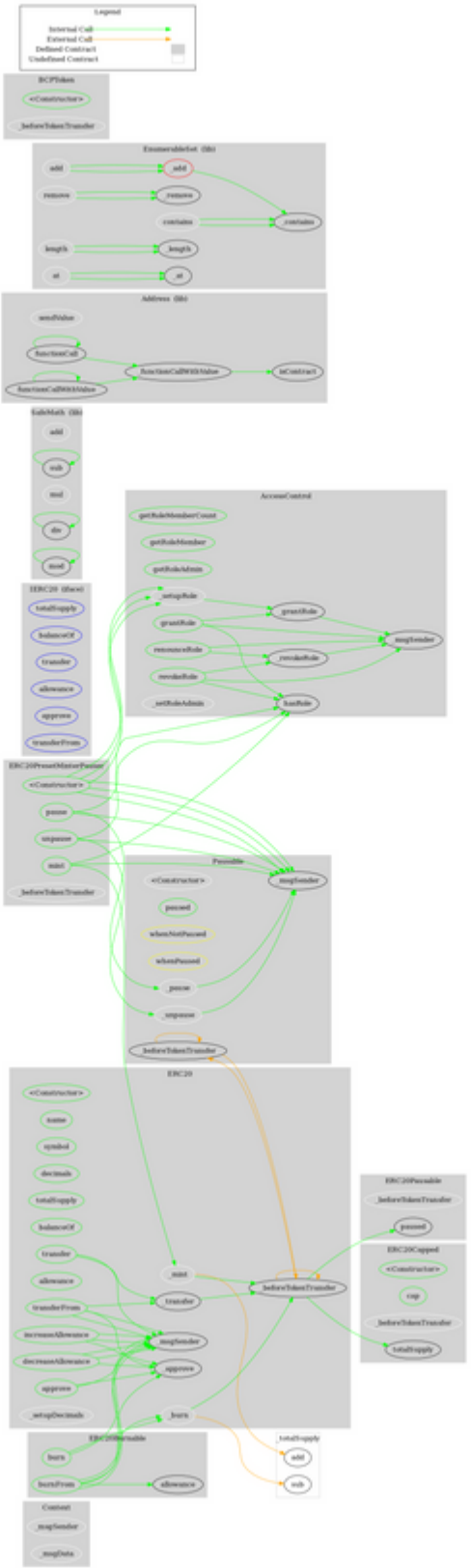
Contract	Type	Bases		
	Function Name	**Visibility**	**Mutability**	**Modifiers**
Context	Implementation			
	_msgSender	Internal		
	_msgData	Internal		
Pausable	Implementation	Context		
	<Constructor>	Internal	✓	
	paused	Public		-
	_pause	Internal	✓	whenNotPaused
	_unpause	Internal	✓	whenPaused
IERC20	Interface			
	totalSupply	External		-
	balanceOf	External		-
	transfer	External	✓	-
	allowance	External		-
	approve	External	✓	-
	transferFrom	External	✓	-
ERC20	Implementation	Context, 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	✓	
	_setupDecimals	Internal	✓	
	_beforeTokenTransfer	Internal	✓	
ERC20Capped	Implementation	ERC20		
	<Constructor>	Public	✓	-
	cap	Public		-
	_beforeTokenTransfer	Internal	✓	
ERC20Pausable	Implementation	ERC20, Pausable		
	_beforeTokenTransfer	Internal	✓	
ERC20Burnable	Implementation	Context, ERC20		
	burn	Public	✓	-
	burnFrom	Public	✓	-
SafeMath	Library			
	add	Internal		
	sub	Internal		
	sub	Internal		
	mul	Internal		
	div	Internal		
	div	Internal		
	mod	Internal		
	mod	Internal		
Address	Library			

	isContract	Internal		
	sendValue	Internal	✓	
	functionCall	Internal	✓	
	functionCall	Internal	✓	
	functionCallWithValue	Internal	✓	
	functionCallWithValue	Internal	✓	
	_functionCallWithValue	Private	✓	
EnumerableSet	Library			
	_add	Private	✓	
	_remove	Private	✓	
	_contains	Private		
	_length	Private		
	_at	Private		
	add	Internal	✓	
	remove	Internal	✓	
	contains	Internal		
	length	Internal		
	at	Internal		
	add	Internal	✓	
	remove	Internal	✓	
	contains	Internal		
	length	Internal		
	at	Internal		
AccessControl	Implementation	Context		
	hasRole	Public		-
	getRoleMemberCount	Public		-
	getRoleMember	Public		-
	getRoleAdmin	Public		-
	grantRole	Public	✓	-
	revokeRole	Public	✓	-
	renounceRole	Public	✓	-
	_setupRole	Internal	✓	
	_setRoleAdmin	Internal	✓	

	_grantRole	Private	✓	
	_revokeRole	Private	✓	
ERC20Preset MinterPauser	Implementation	Context, AccessControl, ERC20Burnable, ERC20Pausable		
	<Constructor>	Public	✓	ERC20
	mint	Public	✓	-
	pause	Public	✓	-
	unpause	Public	✓	-
	_beforeTokenTransfer	Internal	✓	
BCPToken	Implementation	ERC20PresetMinterPauser, ERC20Capped		
	<Constructor>	Public	✓	ERC20Preset MinterPauser ERC20Capped
	_beforeTokenTransfer	Internal	✓	

Contract Flow



Domain Info

Domain Name	blueswap.net
Registry Domain ID	2684233734_DOMAIN_NET-VRSN
Creation Date	2022-03-25T14:43:03.00Z
Updated Date	-
Registry Expiry Date	2023-03-25T14:43:03.00Z
Registrar WHOIS Server	whois.namecheap.com
Registrar URL	http://www.namecheap.com
Registrar	NAMECHEAP INC
Registrar IANA ID	1068

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

Summary

BlueChip Protocol is an interesting project that has a friendly and growing community. The Smart Contract analysis reported no compiler error and only one critical issue. The contract Owner can mint new tokens after initial deployment and inflate the total supply. 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