Audit Report

Cryptorado

January 2022

Type	BEP20
Network	BSC
Address	0x66AFEaF11652216dA917e29BC6791c3fFBAe194B
Audited by	© coinscope

Table of Contents

Contract Review

Contract Name	Cryptorado
Compiler Version	v0.5.17+commit.d19bba13
Optimization	200 runs
Licence	None
Explorer	https://bscscan.com/token/0x66AFEaF11652216dA917e29BC6791c3fFBAe194B
Symbol	CRDO
Decimals	18
Total Supply	200,000,000
Source	contract.sol
Domain	cryptorado.online

Audit Updates

Initial Audit	20th January 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#L1,L892

Description

Addresses that have the minter role have the authority to mint tokens. They 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 _value) public onlyMinter returns (bool
_success) {
  return _mint(_to, _value);
}
```

Recommendation

If this functionality is required by the business logic, then there should be some limits to the maximum amount of tokens that can be minted from every address.

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
	L01	Public Function could be Declared External
	L04	Conformance to Solidity Naming Conventions
	L09	Dead Code Elimination

L01 - Public Function could be Declared External

Criticality	minor
Location	contract.sol#L301,L288,L261 and 5 more

Description

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

```
mint
isMinter
removeMinters
...
```

Recommendation

Use the external attribute for functions never called from the contract

L04 - Conformance to Solidity Naming Conventions

Criticality	minor
Location	contract.sol#L301,L288,L261 and 22 more

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.

```
_value
_to
_addr
...
```

Recommendation

Follow the Solidity naming convention.
https://docs.soliditylang.org/en/v0.4.25/style-guide.html#naming-conventions

L09 - Dead Code Elimination

Criticality	minor
Location	contract.sol#L18,L34,L27 and 1 more

Description

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

```
mul
mod
div
...
```

Recommendation

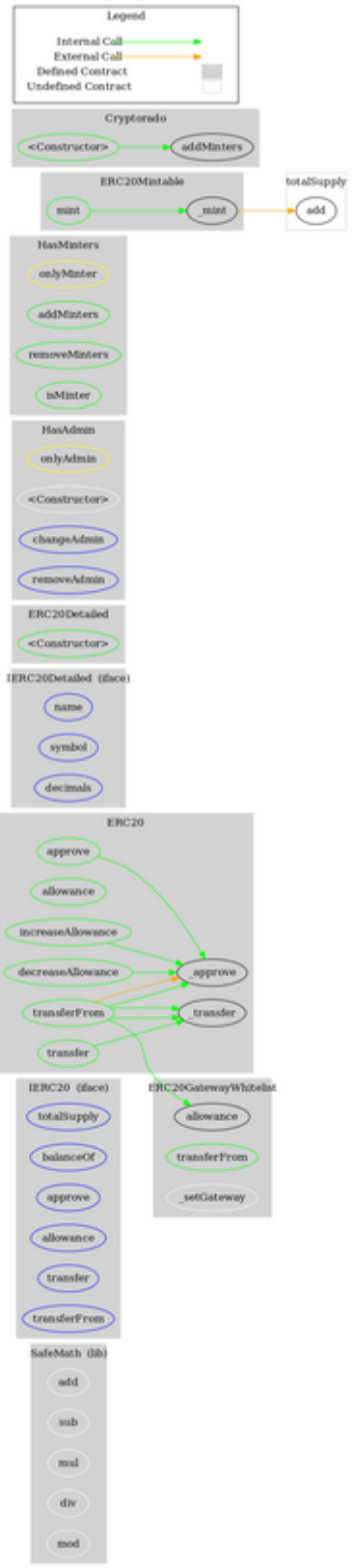
Remove unused functions.

Contract Functions

Contract	Type	Bases		
	Function Name	**Visibility**	**Mutability**	**Modifiers**
SafeMath	Library			
	add	Internal		
	sub	Internal		
	mul	Internal		
	div	Internal		
	mod	Internal		
IERC20	Interface			
	totalSupply	External		-
	balanceOf	External		-
	approve	External	✓	-
	allowance	External		-
	transfer	External	✓	-
	transferFrom	External	✓	-
ERC20	Implementation	IERC20		
	approve	Public	✓	-
	allowance	Public		-
	increaseAllowance	Public	✓	-
	decreaseAllowance	Public	✓	-
	transfer	Public	✓	-
	transferFrom	Public	✓	-
	_approve	Internal	✓	
	_transfer	Internal	✓	
IERC20Detailed	Interface			
	name	External		-
	symbol	External		-

	decimals	External		-
ERC20Detailed	Implementation	ERC20, IERC20Detailed		
	<Constructor>	Public	✓	-
ERC20GatewayWhitelist	Implementation	ERC20		
	allowance	Public		-
	transferFrom	Public	✓	-
	_setGateway	Internal	✓	
HasAdmin	Implementation			
	<Constructor>	Internal	✓	
	changeAdmin	External	✓	onlyAdmin
	removeAdmin	External	✓	onlyAdmin
HasMinters	Implementation	HasAdmin		
	addMinters	Public	✓	onlyAdmin
	removeMinters	Public	✓	onlyAdmin
	isMinter	Public		-
ERC20Mintable	Implementation	HasMinters, ERC20		
	mint	Public	✓	onlyMinter
	_mint	Internal	✓	
Cryptorado	Implementation	ERC20Detailed, ERC20Mintable, ERC20GatewayWhitelist		
	<Constructor>	Public	✓	ERC20Detailed

Contract Flow



Domain Info

Domain Name	cryptorado.online
Registry Domain ID	D270870962-CNIC
Creation Date	2022-01-20T09:23:13+00:00
Updated Date	2022-01-20T09:23:14+00:00
Registry Expiry Date	2023-01-20T23:59:59+00:00
Registrar WHOIS Server	whois.hostinger.com
Registrar URL	https://www.hostinger.com/
Registrar	Hostinger, UAB
Registrar IANA ID	1636

The domain has been created about 11 hours before the creation of the audit. It will expire in about 1 year.

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

Summary

The contract analysis did not report any compiler errors and only 1 major issue. The contract owner may arbitrarily give mint access to wallets. These wallets can mint tokens to any recipient. This functionality could highly inflate the token's value. 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.

Coinscope 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 Coinscope 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 Coinscope 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 Coinscope team disclaims any liability for the resulting losses.

About Coinscope

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.

Coinscope is aiming to make crypto discoverable and efficient globally. It provides all the essential tools to assist users draw their own conclusions.

The Coinscope.co team

https://www.coinscope.co