



Cyberscope

Audit Report

3D Coin

July 2022

SHA256 855edc1439280f4ded8a3695fa7d20cfb8daf7959f03d422358cf14b340dd865

Audited by © cyberscope

Table of Contents

Table of Contents	1
Contract Review	3
Audit Updates	3
Source Files	3
Contract Analysis	4
MT - Mint Tokens	5
Description	5
Recommendation	5
Contract Diagnostics	6
L01 - Public Function could be Declared External	7
Description	7
Recommendation	7
L04 - Conformance to Solidity Naming Conventions	8
Description	8
Recommendation	8
L09 - Dead Code Elimination	9
Description	9
Recommendation	9
Contract Functions	10
Contract Flow	12
Domain Info	13
Summary	14
Disclaimer	15
About Cyberscope	16

Contract Review

Contract Name	ERC20
Test Deploy	https://testnet.bscscan.com/address/0xFb6AaF4Abe26512caC497DEfb9d8B736E4E0a151#code
Domain	https://www.3dhoudini.com

Audit Updates

Initial Audit	15th July 2022
Corrected	

Source Files

Filename	SHA256
ERC20.sol	855edc1439280f4ded8a3695fa7d20cfb8daf7959f03d422358cf14b340dd865
ERC20/Context.sol	50cb25764d82c4b12f4d7e88fa32e1eccd6c2f84745406a382ff641345b2684f
ERC20/IERC20.sol	71fbff972272b30e8803940937dd09eb49434da67a8c9d8c5ae23a7474bbfeef
ERC20/IERC20Metadata.sol	9c6c7705b5af119a56b517d69ce64a5729e4b5dd0170680ef5040e1081e38997

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#L111

Description

Everyone has access to mint tokens. As a result the contract tokens will be highly inflated.

```
function _mint(address account, uint256 amount) public {  
    require(account != address(0), "ERC20: mint to the zero address");  
  
    _beforeTokenTransfer(address(0), account, amount);  
  
    _totalSupply += amount;  
    _balances[account] += amount;  
    emit Transfer(address(0), account, amount);  
  
    _afterTokenTransfer(address(0), account, amount);  
}
```

Recommendation

The owner should rewrite this code segments to make the contract secure from the public. We advised considering an extra-strong security mechanism that the actions may be quarantined by many users instead of one.

Contract Diagnostics

● Critical ● Medium ● Minor

Severity	Code	Description
●	CO	Code Optimization
●	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

contracts/ERC20.sol#L111,78,37,72,29,33,25,61,55,41,45

Description

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

```
transfer
balanceOf
approve
transferFrom
name
decimals
symbol
increaseAllowance
totalSupply
...
```

Recommendation

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

L04 - Conformance to Solidity Naming Conventions

Criticality

minor

Location

contracts/ERC20.sol#L111

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.

`_mint`

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

contracts/ERC20.sol#L123

Description

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

```
_burn
```

Recommendation

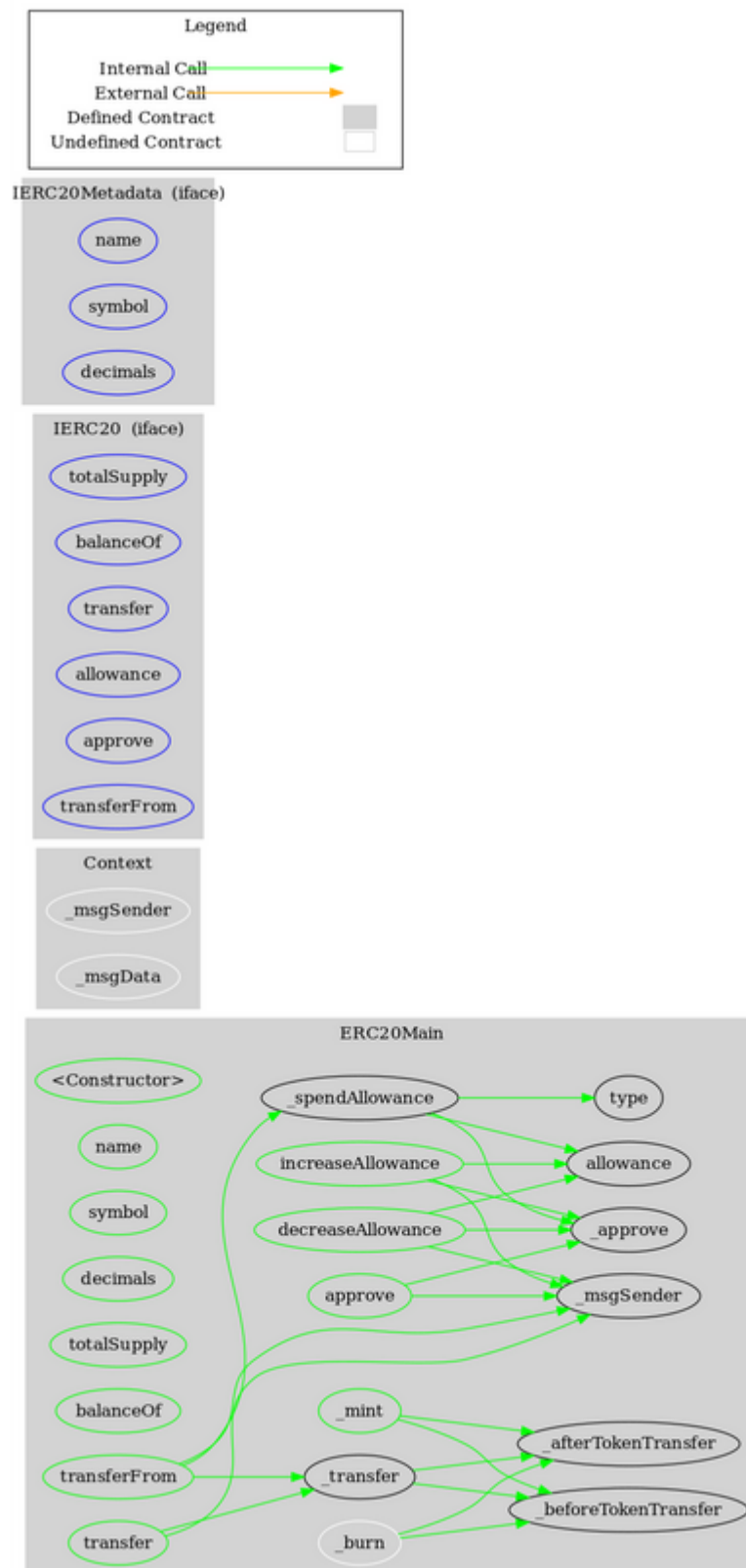
Remove unused functions.

Contract Functions

Contract	Type	Bases		
	Function Name	Visibility	Mutability	Modifiers
ERC20Main	Implementation	Context, IERC20, IERC20Met adata		
	<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	Public	✓	-
	_burn	Internal	✓	
	_approve	Internal	✓	
	_spendAllowance	Internal	✓	
	_beforeTokenTransfer	Internal	✓	
	_afterTokenTransfer	Internal	✓	
Context	Implementation			
	_msgSender	Internal		
	_msgData	Internal		
IERC20				
	Interface			

	totalSupply	External		-
	balanceOf	External		-
	transfer	External	✓	-
	allowance	External		-
	approve	External	✓	-
	transferFrom	External	✓	-
IERC20Metadata	Interface	IERC20		
	name	External		-
	symbol	External		-
	decimals	External		-

Contract Flow



Domain Info

Domain Name	3dhoudini.com
Registry Domain ID	2410837419_DOMAIN_COM-VRSN
Creation Date	2019-07-09T05:11:00.00Z
Updated Date	2022-06-07T07:52:34.00Z
Registry Expiry Date	2023-07-09T05:11:36.00Z
Registrar WHOIS Server	WHOIS.DREAMHOST.COM
Registrar URL	WWW.DREAMHOST.COM
Registrar	DREAMHOST
Registrar IANA ID	431

The domain has been created in 12 months before the creation of the audit.

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

Summary

The Smart Contract analysis reported one critical severity issue. Everyone has the authority to mint tokens. If this functionality is abused, then the contract will be highly inflated. A multi-wallet signing pattern will provide security against potential hacks.

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>