



Cyberscope

Audit Report

WooZoo Music

April 2022

Github <https://github.com/woozoomusic01/wzm-token>

Commit [dd25247226c3333e7d84765f690ff4a65cbe95dc](#)

Audited by © cyberscope

Table of Contents

Table of Contents	1
Contract Review	3
Source Files	3
Audit Updates	3
Contract Analysis	4
MT - Mint Tokens	5
Description	5
Recommendation	5
BC - Blacklisted Contracts	6
Description	6
Recommendation	6
Contract Diagnostics	7
L01 - Public Function could be Declared External	8
Description	8
Recommendation	8
L02 - State Variables could be Declared Constant	9
Description	9
Recommendation	9
L04 - Conformance to Solidity Naming Conventions	10
Description	10
Recommendation	10
L06 - Missing Events Access Control	11
Description	11
Recommendation	11
L09 - Dead Code Elimination	12
Description	12

Recommendation	12
Contract Functions	13
Contract Flow	15
Domain Info	16
Summary	17
Disclaimer	18
About Cyberscope	19

Contract Review

Contract Name	WooZooMusic
Github	https://github.com/woozoomusic01/wzm-token/blob/main/wzm.sol
Commit	dd25247226c3333e7d84765f690ff4a65cbe95dc
Domain	woozoomusic.com

Source Files

Filename	SHA256
contract.sol	a75d5e1cbeeb9710fdb4b4383939ccfbd171a6052f2589c33421d6491533951a6

Audit Updates

Initial Audit	20th April 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#L221

Description

The contract owner has the authority to mint tokens. The owner may take advantage of it by calling the `mintToken` function. As a result the contract tokens will be highly inflated

```
function mintToken(address target, uint256 mintedAmount) onlyOwner public {  
    require (mintedAmount > 0);  
    totalSupply = totalSupply.add(mintedAmount);  
    balanceOf[target] = balanceOf[target].add(mintedAmount);  
    emit Transfer(0, this, mintedAmount);  
    emit Transfer(this, target, mintedAmount);  
}
```

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.

BC - Blacklisted Contracts

Criticality	medium
Location	contract.sol#L214

Description

The contract owner has the authority to stop contracts from transactions. The owner may take advantage of it by calling the `freezeAccount` function.

```
require(!frozenAccount[_from]);  
require(!frozenAccount[_to]);
```

Recommendation

The team should carefully manage the private keys of the owner's account. We strongly recommend a powerful security mechanism that will prevent a single user from accessing the contract admin functions. That risk can be prevented by temporarily locking the contract or renouncing ownership.

Contract Diagnostics

● Critical ● Medium ● Minor

Severity	Code	Description
●	L01	Public Function could be Declared External
●	L02	State Variables could be Declared Constant
●	L04	Conformance to Solidity Naming Conventions
●	L06	Missing Events Access Control
●	L09	Dead Code Elimination

L01 - Public Function could be Declared External

Criticality	minor
Location	contract.sol#L67,105,133,142,161,176,189,221,229

Description

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

```
freezeAccount  
mintToken  
burnFrom  
burn  
approveAndCall  
transferFrom  
transfer  
release  
transferOwnership
```

Recommendation

Use the external attribute for functions never called from the contract

L02 - State Variables could be Declared Constant

Criticality

minor

Location

contract.sol#L82

Description

Constant state variables should be declared constant to save gas.

```
decimals
```

Recommendation

Add the constant attribute to state variables that never change.

L04 - Conformance to Solidity Naming Conventions

Criticality

minor

Location

contract.sol#L55,75,133,142,150,161,176,189

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  
_from  
_extraData  
_spender  
_to  
tokenRecipient  
owned  
...
```

Recommendation

Follow the Solidity naming convention.

<https://docs.soliditylang.org/en/v0.4.25/style-guide.html#naming-conventions>

L06 - Missing Events Access Control

Criticality

minor

Location

contract.sol#L67

Description

Detected missing events for critical access control parameters. There are functions that have no event emitted, so it is difficult to track off-chain changes.

```
owner = newOwner
```

Recommendation

Emit an event for critical parameter changes.

L09 - Dead Code Elimination

Criticality

minor

Location

contract.sol#L120

Description

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

```
_transfer
```

Recommendation

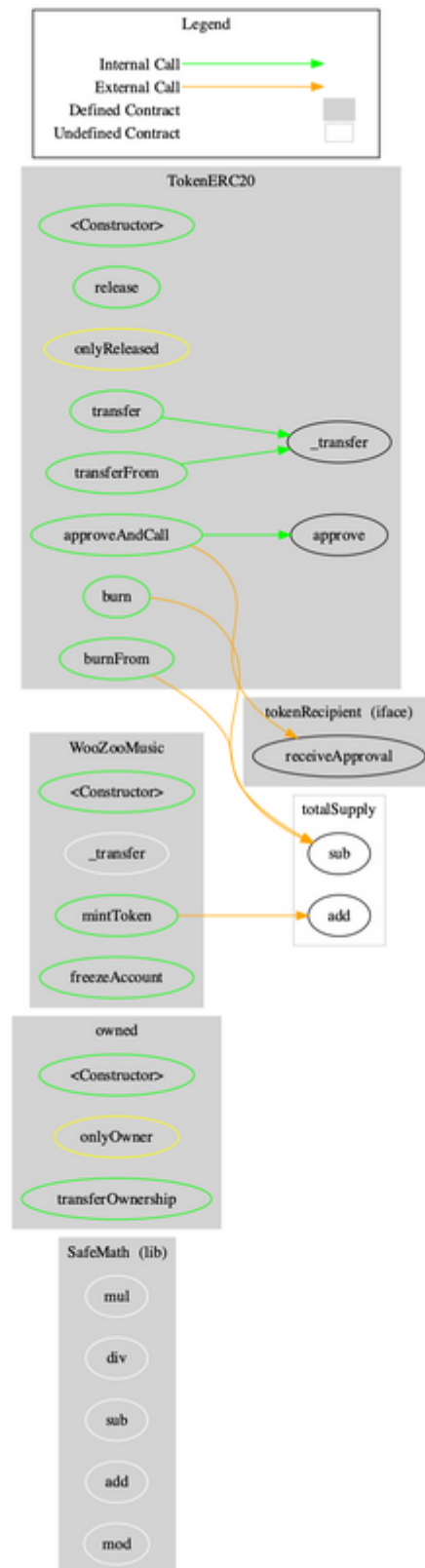
Remove unused functions.

Contract Functions

Contract	Type	Bases		
	Function Name	Visibility	Mutability	Modifiers
SafeMath	Library			
	mul	Internal		
	div	Internal		
	sub	Internal		
	add	Internal		
	mod	Internal		
owned	Implementation			
	<Constructor>	Public	✓	-
	transferOwnership	Public	✓	onlyOwner
tokenRecipient	Interface			
	receiveApproval	External	✓	-
TokenERC20	Implementation	owned		
	<Constructor>	Public	✓	-
	release	Public	✓	onlyOwner
	_transfer	Internal	✓	onlyReleased
	transfer	Public	✓	onlyReleased
	transferFrom	Public	✓	onlyReleased
	approve	Public	✓	onlyReleased
	approveAndCall	Public	✓	onlyReleased
	burn	Public	✓	onlyReleased
	burnFrom	Public	✓	onlyReleased
WooZooMusic	Implementation	owned, TokenERC20		
	<Constructor>	Public	✓	TokenERC20

	_transfer	Internal	✓	onlyReleased
	mintToken	Public	✓	onlyOwner
	freezeAccount	Public	✓	onlyOwner

Contract Flow



Domain Info

Domain Name	woozoomusic.com
Registry Domain ID	
Creation Date	2021-05-05T15:00:00Z
Updated Date	2021-09-28T08:41:45Z
Registry Expiry Date	2023-05-05T15:00:00Z
Registrar WHOIS Server	whois.gabia.com
Registrar URL	https://www.gabia.com
Registrar	gabia
Registrar IANA ID	244

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

Summary

WooZoo Music is an interesting project that has a friendly and growing community. There are some functions that can be abused by the owner, like minting tokens and blacklisting addresses. If the mint method is abused by the contract owner then 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 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>