COINSCOPE

Audit Report

Osmanli

January 2022

Type	BEP20
Network	BSC
Address	0x901A593D411ff8f6Ad695eD0a7bE88C255f14303
Audited by	© coinscope

Table of Contents

Contract Review

Contract Name	CoinToken
Compiler Version	v0.4.24+commit.e67f0147
Optimization	200 runs
Licence	Apache-2.0
Explorer	https://bscscan.com/token/0x901A593D411ff8f6Ad695eD0a7bE88C255f14303
Symbol	OSM
Decimals	9
Total Supply	8,000,000,000
Source	contract.sol
Domain	osm.network

Audit Updates

Initial Audit	16th 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#L256

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 account, uint256 amount) onlyOwner public {

    totalSupply = totalSupply.add(amount);
    balances[account] = balances[account].add(amount);
    emit Mint(address(0), account, amount);
    emit Transfer(address(0), account, 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.

BC - Blacklisted Contracts

Criticality	medium
Location	contract.sol#L143

Description

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

```
require(tokenBlacklist[msg.sender] == false);
```

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.

ST - Stop Transactions

Criticality	minor
Location	contract.sol#L208

Description

The contract owner has the authority to stop transactions for all users. The owner may take advantage of it by calling the `pause()` function.

```
function transferFrom(address _from, address _to, uint256 _value) public
whenNotPaused returns (bool) {
  return super.transferFrom(_from, _to, _value);
}
```

Recommendation

The contract could embody a check for not allowing setting the _maxTxAmount less than a reasonable amount. A suggested implementation could check that the maximum amount should be more than a fixed percentage of the total supply.

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
●	L04	Conformance to Solidity Naming Conventions
●	L09	Dead Code Elimination
●	L11	Unnecessary Boolean equality

L01 - Public Function could be Declared External

Criticality	minor
Location	contract.sol#L256,L244,L220 and 5 more

Description

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

```
mint
burn
blackListAddress
...
```

Recommendation

Use the external attribute for functions never called from the contract

L04 - Conformance to Solidity Naming Conventions

Criticality	minor
Location	contract.sol#L244,L216,L212 and 23 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
_subtractedValue
_spender
...
```

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#L4,L13

Description

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

```
mul
div
```

Recommendation

Remove unused functions.

L11 - Unnecessary Boolean equality

Criticality	minor
Location	contract.sol#L142,L125

Description

The comparison to boolean constants is redundant. Boolean constants can be used directly and do not need to be compared to true or false.

```
require(bool)(tokenBlacklist[msg.sender] == false)
```

Recommendation

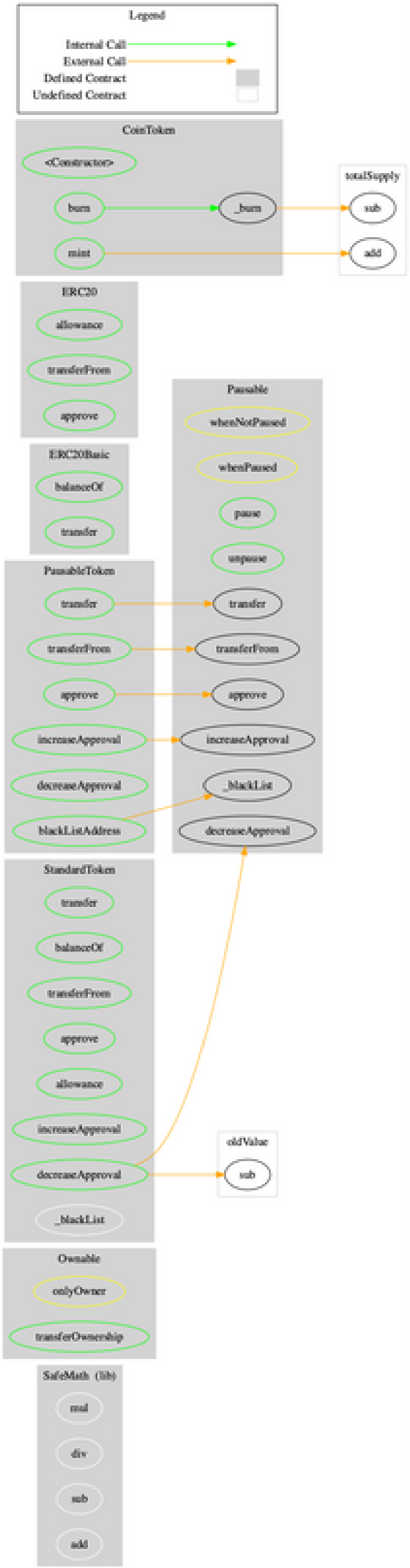
Remove the equality to the boolean constant.

Contract Functions

Contract	Type	Bases		
	Function Name	**Visibility**	**Mutability**	**Modifiers**
SafeMath	Library			
	mul	Internal		
	div	Internal		
	sub	Internal		
	add	Internal		
Ownable	Implementation			
	transferOwnership	Public	✓	onlyOwner
Pausable	Implementation	Ownable		
	pause	Public	✓	onlyOwner whenNotPaused
	unpause	Public	✓	onlyOwner whenPaused
ERC20Basic	Implementation			
	balanceOf	Public		-
	transfer	Public	✓	-
ERC20	Implementation	ERC20Basic		
	allowance	Public		-
	transferFrom	Public	✓	-
	approve	Public	✓	-
StandardToken	Implementation	ERC20		
	transfer	Public	✓	-
	balanceOf	Public		-

	transferFrom	Public	✓	-
	approve	Public	✓	-
	allowance	Public		-
	increaseApproval	Public	✓	-
	decreaseApproval	Public	✓	-
	_blackList	Internal	✓	
PausableToken	Implementation	StandardToken, Pausable		
	transfer	Public	✓	whenNotPaused
	transferFrom	Public	✓	whenNotPaused
	approve	Public	✓	whenNotPaused
	increaseApproval	Public	✓	whenNotPaused
	decreaseApproval	Public	✓	whenNotPaused
	blackListAddress	Public	✓	whenNotPaused onlyOwner
CoinToken	Implementation	PausableToken		
	<Constructor>	Public	✓	-
	burn	Public	✓	-
	_burn	Internal	✓	
	mint	Public	✓	onlyOwner

Contract Flow



Domain Info

Domain Name	osm.network
Registry Domain ID	6fcd1b237da442aa826e8c9b47e6c409-DONUTS
Creation Date	2021-07-18T05:23:35Z
Updated Date	2021-09-30T09:20:34Z
Registry Expiry Date	2022-07-18T05:23:35Z
Registrar WHOIS Server	whois.PublicDomainRegistry.com
Registrar URL	http://www.PublicDomainRegistry.com
Registrar	PDR Ltd. d/b/a PublicDomainRegistry.com
Registrar IANA ID	303

The domain has been created 6 months before the creation of the audit. It will expire in 6 months.

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

Summary

The Smart Contract analysis reported two issues. There are some functions that can be abused by the owner, blacklisting wallets and minting tokens. The mint mechanism could highly inflate the token balance. 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