

Audit Report

SPACE

January 2022

Type	BEP20
Network	BSC
Address	0x32b86D0Fd22426955C3bD4A9FbB14142fcb60355
Audited by	© coinscope

Table of Contents

Table of Contents 1
Contract Review 3
Audit Updates 3
Contract Analysis 4
MT - Mint Tokens 5
Description 5
Recommendation 5
BT - Burn Tokens 6
Description 6
Recommendation 6
Contract Diagnostics 7
L01 - Public Function could be Declared External 8
Description 8
Recommendation 8
L04 - Conformance to Solidity Naming Conventions 9
Description 9
Recommendation 9
L09 - Dead Code Elimination 10
Description 10
Recommendation 10
Contract Functions 11
Contract Flow 14
Domain Info 15
Summary 16
Disclaimer 17
About Coinscope 18

Contract Review

Contract Name	MSSpaceToken
Compiler Version	v0.8.7+commit.e28d00a7
Optimization	200 runs
Licence	MIT
Explorer	https://bscscan.com/token/0x32b86D0Fd22426955C3bD4A9FbB14142fcb60355
Symbol	SPACE
Decimals	18
Total Supply	-
Source	@openzeppelin/contracts/access/AccessControl.sol, @openzeppelin/contracts/access/IAccessControl.sol, @openzeppelin/contracts/token/ERC20/ERC20.sol, @openzeppelin/contracts/token/ERC20/IERC20.sol, @openzeppelin/contracts/token/ERC20/extensions/IERC20Metadata.sol, @openzeppelin/contracts/utils/Context.sol, @openzeppelin/contracts/utils/Strings.sol, @openzeppelin/contracts/utils/introspection/ERC165.sol, @openzeppelin/contracts/utils/introspection/IERC165.sol, contracts/IMSSpaceToken.sol, contracts/MSSpaceToken.sol
Domain	boomspace.fi

Audit Updates

Initial Audit	25th 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

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

```
    function msMint(address recipient, uint256 amount) override  external
returns (bool)
    {
        require(hasRole(OPERATOR_ROLE, _msgSender()), "Caller is not a
operator");
        _mint(recipient, amount);
        return true;
    }
```

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.

BT - Burn Tokens

Criticality	critical
Location	contract.sol#L1

Description

The contract owner has the authority to burn tokens from a specific address. The owner may take advantage of it by calling the `msBurn` function. As a result the targeted contract address will lose the corresponding tokens.

```
    function msBurn(address _who,uint256 _amount) override external {
        require(hasRole(OPERATOR_ROLE, _msgSender()), "Caller is not a
operator");
        _burn(_who, _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

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	@openzeppelin/contracts/access/AccessControl.sol#L197,L178,L132 and 7 more

Description

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

```
decreaseAllowance
increaseAllowance
approve
...
```

Recommendation

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

L04 - Conformance to Solidity Naming Conventions

Criticality	minor
Location	contracts/MSSpaceToken.sol#L30

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.

```
_amount
_who
```

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	@openzeppelin/contracts/access/AccessControl.sol#L15,L40,L21 and 1 more

Description

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

```
toString
toHexString
_msgData
...
```

Recommendation

Remove unused functions.

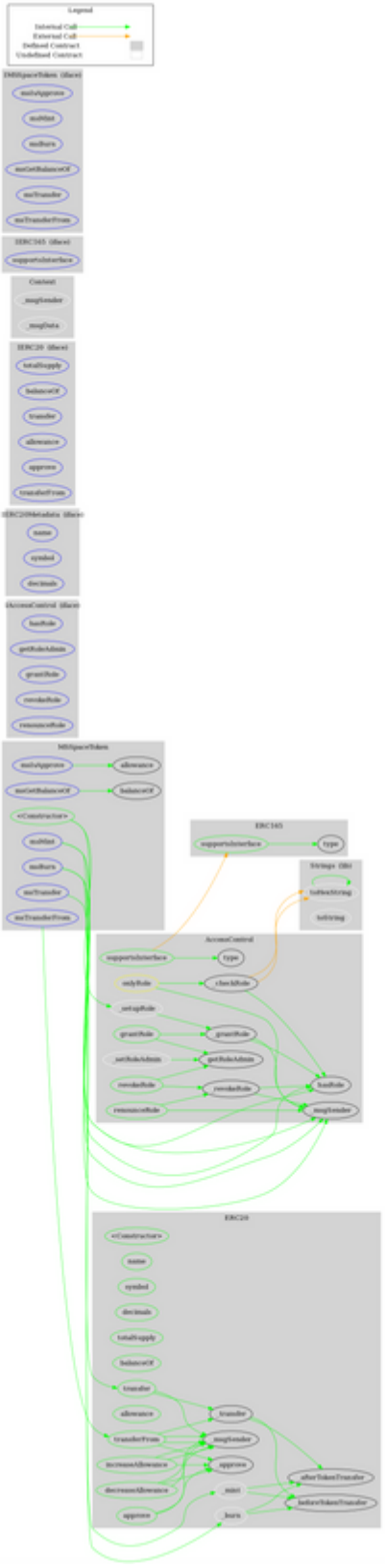
Contract Functions

Contract	Type	Bases		
	Function Name	**Visibility**	**Mutability**	**Modifiers**
AccessControl	Implementation	Context, IAccessControl, ERC165		
	supportsInterface	Public		-
	hasRole	Public		-
	_checkRole	Internal		
	getRoleAdmin	Public		-
	grantRole	Public	✓	onlyRole
	revokeRole	Public	✓	onlyRole
	renounceRole	Public	✓	-
	_setupRole	Internal	✓	
	_setRoleAdmin	Internal	✓	
	_grantRole	Internal	✓	
	_revokeRole	Internal	✓	
IAccessControl	Interface			
	hasRole	External		-
	getRoleAdmin	External		-
	grantRole	External	✓	-
	revokeRole	External	✓	-
	renounceRole	External	✓	-
ERC20	Implementation	Context, IERC20, IERC20Metadata		
	<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	✓	
	_beforeTokenTransfer	Internal	✓	
	_afterTokenTransfer	Internal	✓	
IERC20Metadata	Interface	IERC20		
	name	External		-
	symbol	External		-
	decimals	External		-
IERC20	Interface			
	totalSupply	External		-
	balanceOf	External		-
	transfer	External	✓	-
	allowance	External		-
	approve	External	✓	-
	transferFrom	External	✓	-
Context	Implementation			
	_msgSender	Internal		
	_msgData	Internal		
ERC165	Implementation	IERC165		
	supportsInterface	Public		-

IERC165	Interface			
	supportsInterface	External		-
Strings	Library			
	toString	Internal		
	toHexString	Internal		
	toHexString	Internal		
IMSSpaceToken	Interface			
	msIsApprove	External		-
	msMint	External	✓	-
	msBurn	External	✓	-
	msGetBalanceOf	External		-
	msTransfer	External	✓	-
	msTransferFrom	External	✓	-
MSSpaceToken	Implementation	IMSSpaceToken, ERC20, AccessControl		
	<Constructor>	Public	✓	ERC20
	msIsApprove	External		-
	msMint	External	✓	-
	msBurn	External	✓	-
	msGetBalanceOf	External		-
	msTransfer	External	✓	-
	msTransferFrom	External	✓	-

Contract Flow



Domain Info

Domain Name	boomspace.fi
Registry Domain ID	
Creation Date	2021-12-14T10:13:21+00:00
Updated Date	
Registry Expiry Date	2022-12-14T10:13:21+00:00
Registrar WHOIS Server	
Registrar URL	
Registrar	Instra Corporation Pty Ltd
Registrar IANA ID	

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

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

Summary

Space is a theme project focused on the Metaverse and NFTs. The Project has a friendly and growing community. The Smart Contract analysis reported no compiler error and 2 critical issues. There are some functions that can be abused by the owner, like minting new tokens and burning tokens of specific users. There is a role system to grant mint/burn access to more members. 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