Audit Report

Mole Hunting

January 2022

Type	BEP20
Network	TESTNET.BSC
Address	0xa9fa4a4089e35da561f20867fd134af870517a84
Audited by	© coinscope

Table of Contents

Contract Review

Contract Name	MOH
Compiler Version	v0.8.7+commit.e28d00a7
Optimization	No with 200 runs
Licence	None
Explorer	https://testnet.bscscan.com/token/0xa9fa4a4089e35da561f20867fd134af870517a84
Symbol	MOH

Audit Updates

Initial Audit	30th December 2021
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	high
Location	https://testnet.bscscan.com/address/0xa9fa4a4089e35da561f20867fd134af870517a84#L1858

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, however there is a check to not surpass the max supply.

```
    function mint(address to, uint256 amount) public virtual override
onlyMinter {
        require(totalSupply() + amount <= MAX_SUPPLY, "MOH: Max supply
exceeded");
        _mint(to, amount);
    }
```

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.

BC - Blacklisted Contracts

Criticality	medium
Location	https://testnet.bscscan.com/address/0xa9fa4a4089e35da561f20867fd134af870517a84#L1863

Description

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

```
    function setBotPrevent(address _BP) external onlyAdmin {
        require(address(_BP) != address(0), "address BP is address zero");
        BP = IBotPrevent(_BP);
    }
```

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
	L04	Conformance to Solidity Naming Conventions
	L09	Dead Code Elimination

L01 - Public Function could be Declared External

Criticality	minor
Location	contract.sol#L1918,L1913,L1908 and 23 more

Description

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

```
withdrawERC721
withdrawTokenAll
withdrawNativeAll
...
```

Recommendation

Use the external attribute for functions never called from the contract

L04 - Conformance to Solidity Naming Conventions

Criticality	minor
Location	contract.sol#L1832,L1918,L1913 and 6 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.

```
BP
_tokenIds
_token
...
```

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#L586,L611,L354 and 16 more

Description

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

```
toString
toHexString
values
...
```

Recommendation

Remove unused functions.

Contract Functions

Contract	Type	Bases		
	Function Name	**Visibility**	**Mutability**	**Modifiers**
IBotPrevent	Interface			
	protect	External		-
EnumerableSet	Library			
	_add	Private	✓	
	_remove	Private	✓	
	_contains	Private		
	_length	Private		
	_at	Private		
	_values	Private		
	add	Internal	✓	
	remove	Internal	✓	
	contains	Internal		
	length	Internal		
	at	Internal		
	values	Internal		
	add	Internal	✓	
	remove	Internal	✓	
	contains	Internal		
	length	Internal		
	at	Internal		
	values	Internal		
	add	Internal	✓	
	remove	Internal	✓	
	contains	Internal		
	length	Internal		

	at	Internal		
	values	Internal		
IERC165	Interface			
	supportsInterface	External		-
IERC721	Interface	IERC165		
	balanceOf	External		-
	ownerOf	External		-
	safeTransferFrom	External	✓	-
	transferFrom	External	✓	-
	approve	External	✓	-
	getApproved	External		-
	setApprovalForAll	External	✓	-
	isApprovedForAll	External		-
	safeTransferFrom	External	✓	-
ERC165	Implementation	IERC165		
	supportsInterface	Public		-
Strings	Library			
	toString	Internal		
	toHexString	Internal		
	toHexString	Internal		
IAccessControl	Interface			
	hasRole	External		-
	getRoleAdmin	External		-
	grantRole	External	✓	-
	revokeRole	External	✓	-
	renounceRole	External	✓	-
IAccessControlEnumerable	Interface	IAccessControl		
	getRoleMember	External		-

	getRoleMemberCount	External		-
Context	Implementation			
	_msgSender	Internal		
	_msgData	Internal		
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	✓	
AccessControlEnumerable	Implementation	IAccessControlEnumerable, AccessControl		
	supportsInterface	Public		-
	getRoleMember	Public		-
	getRoleMemberCount	Public		-
	_grantRole	Internal	✓	
	_revokeRole	Internal	✓	
Pausable	Implementation	Context		
	<Constructor>	Public	✓	-
	paused	Public		-
	_pause	Internal	✓	whenNotPaused

	_unpause	Internal	✓	whenPaused
IERC20	Interface			
	totalSupply	External		-
	balanceOf	External		-
	transfer	External	✓	-
	allowance	External		-
	approve	External	✓	-
	transferFrom	External	✓	-
IERC20Metadata	Interface	IERC20		
	name	External		-
	symbol	External		-
	decimals	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	✓	
ERC20Pausable	Implementation	ERC20, Pausable		
	_beforeTokenTransfer	Internal	✓	
ERC20Burnable	Implementation	Context, ERC20		
	burn	Public	✓	-
	burnFrom	Public	✓	-
ERC20PresetMinterPauser	Implementation	Context, AccessControlEnumerable, ERC20Burnable, ERC20Pausable		
	<Constructor>	Public	✓	ERC20
	mint	Public	✓	-
	pause	Public	✓	-
	unpause	Public	✓	-
	_beforeTokenTransfer	Internal	✓	
MOH	Implementation	ERC20PresetMinterPauser		
	<Constructor>	Public	✓	ERC20PresetMinterPauser
	mint	Public	✓	onlyMinter
	setBotPrevent	External	✓	onlyAdmin
	enabledBP	External	✓	onlyAdmin
	disableBP	External	✓	onlyAdmin
	_transfer	Internal	✓	
	getBalanceNavite	Public		-
	getBalanceToken	Public		-
	withdrawNative	Public	✓	onlyAdmin

	withdrawToken	Public	✓	onlyAdmin
	withdrawNativeAll	Public	✓	onlyAdmin
	withdrawTokenAll	Public	✓	onlyAdmin
	withdrawERC721	Public	✓	onlyAdmin
	<Receive Ether>	External	Payable	-

Contract Flow

Domain Info

Domain Name	molehunting.io
Registry Domain ID	cfbeb68439e74763ab51db693ac67d16-DONUTS
Creation Date	2021-12-06T07:53:47Z
Updated Date	2021-12-11T07:53:59Z
Registry Expiry Date	2022-12-06T07:53:47Z
Registrar WHOIS Server	whois.namecheap.com
Registrar URL	https://www.namecheap.com/
Registrar	NameCheap, Inc.
Registrar IANA ID	1068

The domain has been created 27 days 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

Mole Hunting is a game where people can have an experience of hunting the mole. The project has a friendly and growing community. There are some functions that can be abused by the owner, like minting new tokens but up to the limit of max supply, and blacklisting users. 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