Audit Report

Kling

February 2022

Type	BEP20
Network	BSC
Address	0xcca166E916088cCe10F4fB0fe0c8BB3577bb6e27
Audited by	© coinscope

Table of Contents

Contract Review

Contract Name	KLingToken
Compiler Version	v0.8.7+commit.e28d00a7
Optimization	200 runs
Licence	None
Explorer	https://bscscan.com/token/0xcca166E916088cCe10F4fB0fe0c8BB3577bb6e27
Symbol	KLing
Decimals	18
Total Supply	1,000,000,000,000
Source	contract.sol
Domain	klingmetaverse.io

Audit Updates

Initial Audit	17th February 2022
Corrected	8th May 2022

Contract Analysis

● Critical ● Medium ● Minor ● Pass

Severity	Code	Description	Resolved
●	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	Renounced
●	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#L934,977
Status	Renounced Ownership

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 to, uint256 amount) public onlyOwner {
    _mint(to, amount);
}
```

The signerAddress that is defined by the contract owner has the authority to mint tokens. The signerAddress may take advantage of it by calling the `claim` function with the appropriate signature. As a result the contract tokens will be highly inflated.

```
function claim(bytes memory params) public {
    require(claimState, "unable to claim now");
    claimInternal(claimDecodeParams(params));
}

function claimInternal(claimParams memory store) private {
    require(store.user == _msgSender(), "Invalid user");

    require(block.timestamp < store.deadline, "Time Expired");
    require(!signStatus[store.signature], "already sign used");
    bytes32 hash_ = keccak256(abi.encodePacked(
        SIGNATURE_PERMIT_TYPEHASH,
        address(this),
        store.user,
        store.amount,
        store.slot,
        store.deadline
    ));

    require(signCheck(ECDSA.toEthSignedMessageHash(hash_),store.signature),
```

```
"Sign Error");
    signStatus[store.signature] = true;
    _mint(store.user,store.amount);

    emit claimEvent(store.user,store.amount,block.timestamp);
}
```

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.

Team Update 8th May 2022

The contract ownership has been renounced. The claimState has been configured to false before the renounce. Hence, the contract cannot be manipulated by the contract owner.

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#L187,195,212,219,226,238,246,257,275,303 and 10 more

Description

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

```
adminEmergency
claim
claimStateUpdate
signerAddressUpdate
mint
unpause
pause
transferOwnership
renounceOwnership
...
```

Recommendation

Use the external attribute for functions never called from the contract

L04 - Conformance to Solidity Naming Conventions

Criticality	minor
Location	contract.sol#L946,924

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.

```
claimEvent
claimParams
```

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#L400,23,657,736,768,819,853

Description

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

```
toTypedDataHash
recover
_throwError
_msgData
_burn
```

Recommendation

Remove unused functions.

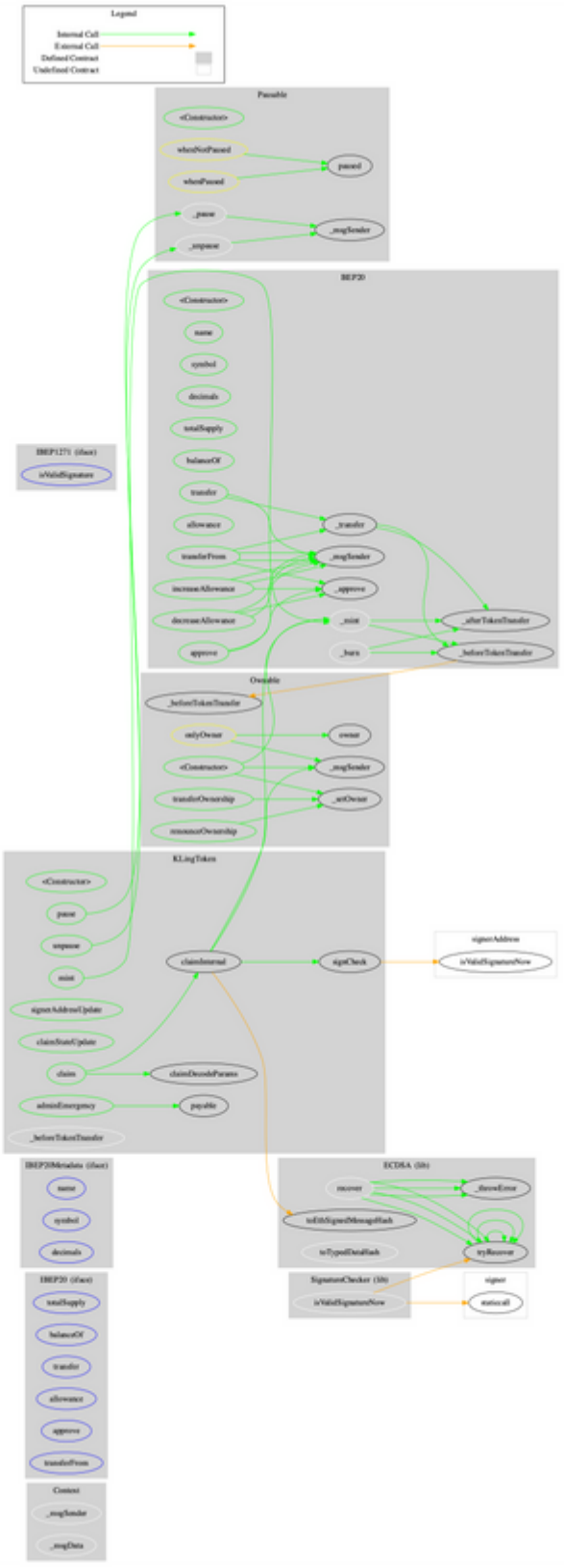
Contract Functions

Contract	Type	Bases		
	Function Name	**Visibility**	**Mutability**	**Modifiers**
Context	Implementation			
	_msgSender	Internal		
	_msgData	Internal		
IBEP20	Interface			
	totalSupply	External		-
	balanceOf	External		-
	transfer	External	✓	-
	allowance	External		-
	approve	External	✓	-
	transferFrom	External	✓	-
IBEP20Metadata	Interface	IBEP20		
	name	External		-
	symbol	External		-
	decimals	External		-
BEP20	Implementation	Context, IBEP20, IBEP20Metadata		
	<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	✓	
Ownable	Implementation	Context		
	<Constructor>	Public	✓	-
	owner	Public		-
	renounceOwnership	Public	✓	onlyOwner
	transferOwnership	Public	✓	onlyOwner
	_setOwner	Private	✓	
Pausable	Implementation	Context		
	<Constructor>	Public	✓	-
	paused	Public		-
	_pause	Internal	✓	whenNotPaused
	_unpause	Internal	✓	whenPaused
ECDSA	Library			
	_throwError	Private		
	tryRecover	Internal		
	recover	Internal		
	tryRecover	Internal		
	recover	Internal		
	tryRecover	Internal		
	recover	Internal		
	toEthSignedMessageHash	Internal		
	toTypedDataHash	Internal		

IBEP1271	Interface			
	isValidSignature	External		-
SignatureChecker	Library			
	isValidSignatureNow	Internal		
KLingToken	Implementation	BEP20, Pausable, Ownable		
	<Constructor>	Public	✓	BEP20
	pause	Public	✓	onlyOwner
	unpause	Public	✓	onlyOwner
	mint	Public	✓	onlyOwner
	signerAddressUpdate	Public	✓	onlyOwner
	claimStateUpdate	Public	✓	onlyOwner
	claimDecodeParams	Public		-
	claim	Public	✓	-
	claimInternal	Private	✓	
	adminEmergency	Public	✓	onlyOwner
	signCheck	Public		-
	_beforeTokenTransfer	Internal	✓	whenNotPaused

Contract Flow



Domain Info

Domain Name	klingmetaverse.io
Registry Domain ID	ab7792f5f514456084221d84cede7fed-DONUTS
Creation Date	2021-11-01T16:12:42Z
Updated Date	2021-12-24T08:29:07Z
Registry Expiry Date	2022-11-01T16:12:42Z
Registrar WHOIS Server	whois.godaddy.com/
Registrar URL	http://www.godaddy.com/domains/search.aspx?ci=8990
Registrar	GoDaddy.com, LLC
Registrar IANA ID	146

The domain has been created 4 months before the creation of the audit. It will expire in 9 months.

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

Summary

The Smart Contract analysis reported one issue. The contract Owner has the authority to mint tokens. The owner also has the ability to permit an address to mint tokens. If this functionality is abused by the contract owner, 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.

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