Cyberscope

Audit Report

Kazama Senshi

September 2022

Type	BEP20
Network	BSC TESTNET
Address	0x9f21B9909048724Ef07E72969B31ABa0Ed026Fd0
Audited by	© cyberscope

Table of Contents

Contract Review

Contract Name	KazamaSenshi
Compiler Version	v0.8.17+commit.8df45f5f
Licence	MIT
Testing Deploy	https://testnet.bscscan.com/token/0x9f21B9909048724Ef07E72969B31ABa0Ed026Fd0
Symbol	KAZAMA
Decimals	18
Total Supply	775,000,000
Domain	

Source Files

Filename	**SHA256**
contract.sol	7e193fe0415beff7d19f47c941bc48c58f5ca533f20d708781b36dab16a23911

Audit Updates

Initial Audit	17th September 2022 https://github.com/cyberscope-io/audits/blob/main/v1/1-kazama/audit.pdf
Corrected	19th September 2022

Contract Analysis

● Critical ● Medium ● Minor / Informative ● Pass

Severity	Code	Description	Status
●	ST	Stops Transactions	Passed
●	OCTD	Transfers Contract's Tokens	Passed
●	OTUT	Transfers User's Tokens	Passed
●	ELFM	Exceeds Fees Limit	Passed
●	ULTW	Transfers Liquidity to Team Wallet	Passed
●	MT	Mints Tokens	Unresolved
●	BT	Burns Tokens	Passed
●	BC	Blacklists Addresses	Passed

MT - Mints Tokens

Criticality	critical
Location	contract.sol#L1609
Status	Unresolved

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.

```
/// @notice Creates `_amount` token to `_to`. Must only be called by an contract with the SenshiMaster role (i.e SenshiMaster & Bridge contract).
function mint(address _to, uint256 _amount) public OnlySenshiMaster {
    _mint(_to, _amount);
    _moveDelegates(address(0), _delegates[_to], _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 / Informative

Severity	Code	Description	Status
	L01	Public Function could be Declared External	Unresolved
	L02	State Variables could be Declared Constant	Unresolved
	L04	Conformance to Solidity Naming Conventions	Unresolved
	L07	Missing Events Arithmetic	Unresolved
	L09	Dead Code Elimination	Unresolved
	L11	Unnecessary Boolean equality	Unresolved

L01 - Public Function could be Declared External

Criticality	minor / informative
Location	contract.sol#L904,911,918,947,977,1106,1125,1609,1614
Status	Unresolved

Description

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

```
totalSupply
decimals
symbol
allowance
transfer
increaseAllowance
decreaseAllowance
mint
burn
```

Recommendation

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

L02 - State Variables could be Declared Constant

Criticality	minor / informative
Location	contract.sol#L836,605
Status	Unresolved

Description

Constant state variables should be declared constant to save gas.

```
FeeDenominator
WBNB
```

Recommendation

Add the constant attribute to state variables that never change.

L04 - Conformance to Solidity Naming Conventions

Criticality	minor / informative
Location	contract.sol#L539,641,596,604,605,606,619,1446,1456,1501,1543,1554,1558,1562,1575,1580,785,789,790,791,792,796,801,802,804,808,809,810,811,812,814,815,817,818,819,820,823,824,825,826,827,829,830,831,834,835,836,839,851,1609,1625
Status	Unresolved

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.

```
WETH
_minPeriod
_minDistribution
_token
BUSD
WBNB
Router
dividendsPerShareAccuracyFactor
_tokenAddress
...
```

Recommendation

Follow the Solidity naming convention.
https://docs.soliditylang.org/en/v0.4.25/style-guide.html#naming-conventions.

L07 - Missing Events Arithmetic

Criticality	minor / informative
Location	contract.sol#L641
Status	Unresolved

Description

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

```
minPeriod = _minPeriod
```

Recommendation

Emit an event for critical parameter changes.

L09 - Dead Code Elimination

Criticality	minor / informative
Location	contract.sol#L230,237
Status	Unresolved

Description

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

```
max
min
```

Recommendation

Remove unused functions.

L11 - Unnecessary Boolean equality

Criticality	minor / informative
Location	contract.sol#L1038,1149,955
Status	Unresolved

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.

```
shouldBurnSender(sender) == false
require(bool,string)(BuyBacker[_msgSender()] == true,)
```

Recommendation

Remove the equality to the boolean constant.

Contract Functions

Contract	Type	Bases		
	Function Name	Visibility	Mutability	Modifiers
Context	Implementation			
	_msgSender	Internal		
	_msgData	Internal		
SafeMath	Library			
	tryAdd	Internal		
	trySub	Internal		
	tryMul	Internal		
	tryDiv	Internal		
	tryMod	Internal		
	add	Internal		
	sub	Internal		
	mul	Internal		
	div	Internal		
	mod	Internal		
	sub	Internal		
	div	Internal		
	mod	Internal		
	max	Internal		
	min	Internal		
	ceil	Internal		
TheZaibatsu	Implementation	Context		
	<Constructor>	Public	✓	-
	owner	Public		-
	isSenshiMaster	Public		-
	isJin	Public		-
	isZaibatsu	Public		-

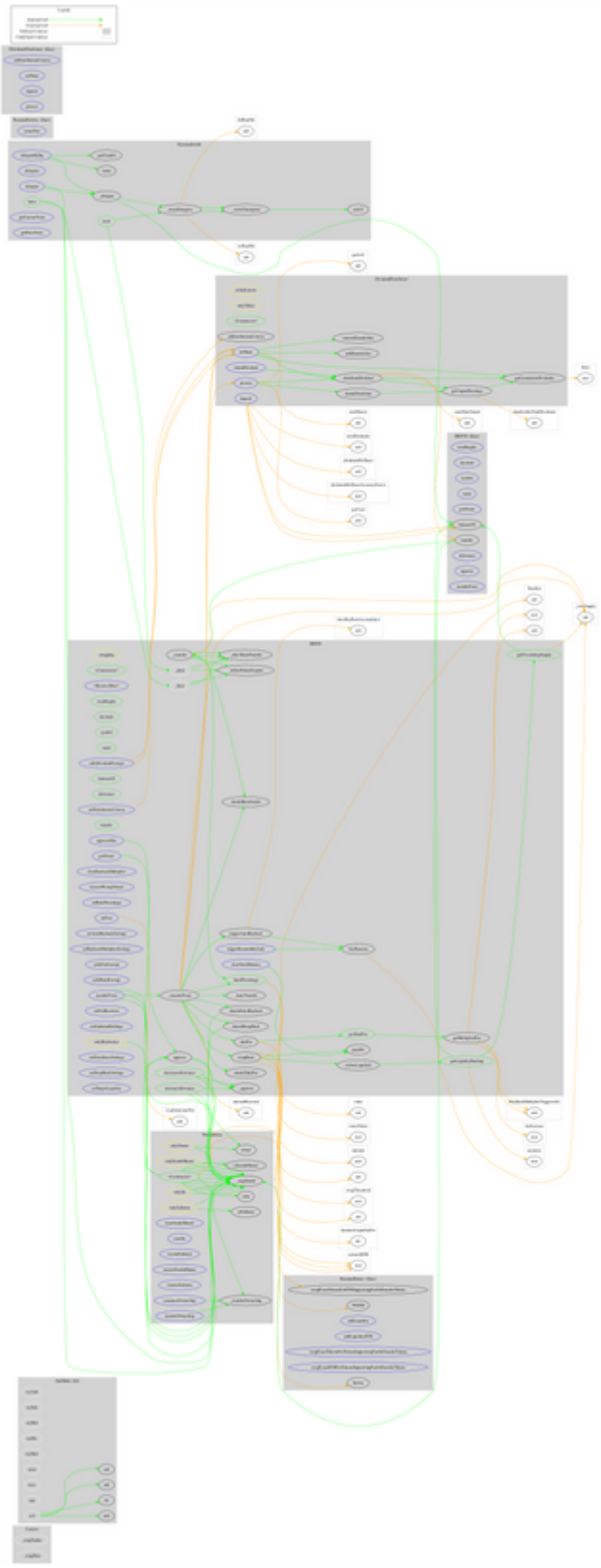
	raiseSenshiMaster	External	✓	onlyJin
	raiseJin	External	✓	onlyJin
	recruitZaibatsu	External	✓	onlyJin
	removeSenshiMaster	External	✓	onlyJin
	removeZaibatsu	External	✓	onlyJin
	renounceOwnership	External	✓	onlyJin
	transferOwnership	External	✓	onlyJin
	_transferOwnership	Internal	✓	
IBEP20	Interface			
	totalSupply	External		-
	decimals	External		-
	symbol	External		-
	name	External		-
	getOwner	External		-
	balanceOf	External		-
	transfer	External	✓	-
	allowance	External		-
	approve	External	✓	-
	transferFrom	External	✓	-
KazamaFactory	Interface			
	createPair	External	✓	-
KazamaRouter	Interface			
	factory	External		-
	WETH	External		-
	addLiquidity	External	✓	-
	addLiquidityETH	External	Payable	-
	swapExactTokensForTokensSupportingFeeOnTransferTokens	External	✓	-
	swapExactETHForTokensSupportingFeeOnTransferTokens	External	Payable	-
	swapExactTokensForETHSupporting	External	✓	-

	FeeOnTransferTokens			
IDividendDistributor	Interface			
	setDistributionCriteria	External	✓	-
	setShare	External	✓	-
	deposit	External	Payable	-
	process	External	✓	-
DividendDistributor	Implementation	IDividendDistributor		
	<Constructor>	Public	✓	-
	setDistributionCriteria	External	✓	onlyToken
	setShare	External	✓	onlyToken
	deposit	External	Payable	onlyToken
	process	External	✓	onlyToken
	shouldDistribute	Internal		
	distributeDividend	Internal	✓	
	claimDividend	External	✓	-
	getUnpaidEarnings	Public		-
	getCumulativeDividends	Internal		
	addShareholder	Internal	✓	
	removeShareholder	Internal	✓	
BEP20	Implementation	IBEP20, TheZaibatsu		
	<Constructor>	Public	Payable	-
	<Receive Ether>	External	Payable	-
	totalSupply	Public		-
	decimals	Public		-
	symbol	Public		-
	name	Public		-
	getOwner	External		-
	balanceOf	Public		-
	allowance	Public		-
	burnPercentage	Public		-

	transfer	Public	✓	-
	approve	Public	✓	-
	approveMax	External	✓	-
	transferFrom	External	✓	-
	_transferFrom	Internal	✓	
	_basicTransfer	Internal	✓	
	increaseAllowance	Public	✓	-
	decreaseAllowance	Public	✓	-
	_transfer	Internal	✓	
	_mint	Internal	✓	
	_burn	Internal	✓	
	_approve	Internal	✓	
	_beforeTokenTransfer	Internal	✓	
	_afterTokenTransfer	Internal	✓	
	shouldTakeFee	Internal		
	shouldBurnSender	Internal		
	getTotalFee	Public		-
	getMultipliedFee	Public		-
	takeFee	Internal	✓	
	shouldSwapBack	Internal		
	swapBack	Internal	✓	swapping
	shouldAutoBuyback	Internal		
	triggerKazamaBuyback	External	✓	onlyZaibatsu
	clearBuybackMultiplier	External	✓	onlyZaibatsu
	clearStuckBalance	External	✓	onlyZaibatsu
	recoverWrongTokens	External	✓	onlyJin
	setBurnPercentage	External	✓	onlyZaibatsu
	setIsDividendExempt	External	✓	onlyJin
	triggerAutoBuyback	Internal	✓	
	buyKazama	Internal	✓	swapping
	setAutoBuybackSettings	External	✓	onlyZaibatsu
	setBuybackMultiplierSettings	External	✓	onlyZaibatsu
	setIsFeeExempt	External	✓	onlyZaibatsu
	setIsBurnExempt	External	✓	onlyZaibatsu

	setFees	External	✓	onlyJin
	setFeeReceivers	External	✓	onlyJin
	setZaibatsuHoldings	External	✓	onlyJin
	setDistributionCriteria	External	✓	onlyZaibatsu
	setDistributorSettings	External	✓	onlyZaibatsu
	setSwapBackSettings	External	✓	onlyZaibatsu
	setTargetLiquidity	External	✓	onlyJin
	getCirculatingSupply	Public		-
	getLiquidityBacking	Public		-
	isOverLiquified	Public		-
KazamaSenshi	Implementation	BEP20		
	mint	Public	✓	onlySenshiMaster
	burn	Public	✓	-
	delegates	External		-
	delegate	External	✓	-
	delegateBySig	External	✓	-
	getCurrentVotes	External		-
	getPriorVotes	External		-
	_delegate	Internal	✓	
	_moveDelegates	Internal	✓	
	_writeCheckpoint	Internal	✓	
	safe32	Internal		
	getChainId	Internal		

Contract Flow



Domain Info

Domain Name	kazamaswap.finance
Registry Domain ID	8d4510f5c86046b7964acf67bec09b38-DONUTS
Creation Date	2022-03-10T12:30:39Z
Updated Date	2022-03-15T12:31:09Z
Registry Expiry Date	2023-03-10T12:30:39Z
Registrar WHOIS Server	whois.namecheap.com
Registrar URL	https://www.namecheap.com/
Registrar	NameCheap, Inc.
Registrar IANA ID	1068

The domain was 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

If the contract owner abuses the mint functionality, then the contract will be highly inflated. A multi-wallet signing pattern will provide security against potential hacks. Temporarily locking the contract or renouncing ownership will eliminate the threat. There is also a limit of max 13% fees.

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 provide all the essential tools to assist users draw their own conclusions.

The Cyberscope team

https://www.cyberscope.io