Cyberscope

Audit Report

Saitama Cat

May 2022

SHA256 97a7b6aa06bdd2ce79e460185f9f168aef7af8428ebb1c18552f8df09a627cc9

Audited by © cyberscope

Table of Contents

Contract Review

Contract Name	SaitamaCat
Testing Deploy	https://testnet.bscscan.com/address/0xADB2DaF8510Dc7a4aeECf7A4944978540265e26a
Symbol	SACA
Decimals	9
Total Supply	20,000,000,000
Domain	saitamacat.com

Audit Updates

Initial Audit	6th May 2022
Corrected	

Source Files

Filename	SHA256
@openzeppelin/contracts/token/ERC20/ERC20.sol	f7831910f2ed6d32acff6431e5998baf50e4a00121303b27e974aab0ec637d79
@openzeppelin/contracts/token/ERC20/extensions/IERC20Metadata.sol	af5c8a77965cc82c33b7ff844deb9826166689e55dc037a7f2f790d057811990
@openzeppelin/contracts/token/ERC20/IERC20.sol	c2b06bb4572bb4f84bfc5477dadc0fcc497cb66c3a1bd53480e68bedc2e154a6
@openzeppelin/contracts/utils/Context.sol	1458c260d010a08e4c20a4a517882259a23a4baa0b5bd9add9fb6d6a1549814a
@openzeppelin/contracts/utils/math/SafeMath.sol	15941f3904992a62ed117e93d9e2d5c4c22bd09a7ff97fdd5f49273cf09703ac
@uniswap/v2-core/contracts/interfaces/IUniswapV2Factory.sol	51d056199e3f5e41cb1a9f11ce581aa3e190cc982db5771ffeef8d8d1f962a0d
@uniswap/v2-periphery/contracts/interfaces/IUniswapV2Router01.sol	0439ffe0fd4a5e1f4e22d71ddbda76d63d61679947d158cba4ee0a1da60cf663
@uniswap/v2-periphery/contracts/interfaces/IUniswapV2Router02.sol	a2900701961cb0b6152fc073856b972564f7c798797a4a044e83d2ab8f0e8d38
contracts/contract.sol	97a7b6aa06bdd2ce79e460185f9f168aef7af8428ebb1c18552f8df09a627cc9

Contract Analysis

Critical Medium Minor Pass

Severity	Code	Description
Medium	ST	Contract Owner is not able to stop or pause transactions
Pass	OCTD	Contract Owner is not able to transfer tokens from specific address
Pass	OTUT	Owner Transfer User's Tokens
Pass	ELFM	Contract Owner is not able to increase fees more than a reasonable percent (25%)
Minor	ULTW	Contract Owner is not able to increase the amount of liquidity taken by dev wallet more than a reasonable percent
Pass	MT	Contract Owner is not able to mint new tokens
Pass	BT	Contract Owner is not able to burn tokens from specific wallet
Pass	BC	Contract Owner is not able to blacklist wallets from selling

ST - Stop Transactions

Criticality	medium
Location	contract.sol#L233

Description

The contract owner has the authority to stop transactions for all users excluding the owner. The owner may take advantage of it by calling the `setMaxTx()` with `maxTxLimit_ = 1` and `limitDenominator_ = totalSupply`. As a result, the transactions will be limited to a very small number that will essentially block the transfers.

```
if (_shouldLimit(from, to)) {
    require(amount <= maxTx.txLimit, "Error: limit exceeded!");
}
```

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.

ULTW - Unlimited Liquidity to Team Wallet

Criticality	minor
Location	contract.sol#L304

Description

The contract owner has the authority to transfer funds without limit to the team wallet. These funds have been accumulated from fees collected from the contract. The owner may take advantage of it by calling the `manualSetup` method.

```
function manualSetup(uint8 percentSwapLimit_, uint8 swapLimitDenominator_)
    external
    authorized
    returns (uint256)
{
    require(
        percentSwapLimit_ >= 0 &&
            percentSwapLimit_ <= swapLimitDenominator_,
        "Error: out of range!"
    );
    _swapLimit = totalSupply().mul(percentSwapLimit_).div(
        swapLimitDenominator_
    );
    _swapTokenToETH(balanceOf(address(this)), wallets.marketingWallet);
    return _swapLimit;
}
```

Recommendation

The contract could embody a check for the maximum amount of funds that can be swapped. Since a huge amount may volatile the token's price.

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
	L07	Missing Events Arithmetic
	L08	Tautology or Contradiction

L01 - Public Function could be Declared External

Criticality	minor
Location	contracts/contract.sol#L100,104,108

Description

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

```
isExcludeFromLimit
isExcludeFromFee
owner
```

Recommendation

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

L07 - Missing Events Arithmetic

Criticality	minor
Location	contracts/contract.sol#L304

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.

```
_swapLimit = totalSupply().mul(percentSwapLimit_).div(swapLimitDenominator_)
```

Recommendation

Emit an event for critical parameter changes.

L08 - Tautology or Contradiction

Criticality	minor
Location	contracts/contract.sol#L304

Description

Detects expressions that are tautologies or contradictions. For instance, an uint variable will always be greater than or equal to zero.

```
require(bool,string)(percentSwapLimit_ >= 0 && percentSwapLimit_ <=
swapLimitDenominator_,Error: out of range!)
```

Recommendation

Fix the incorrect comparison by changing the value type or the comparison.

Contract Functions

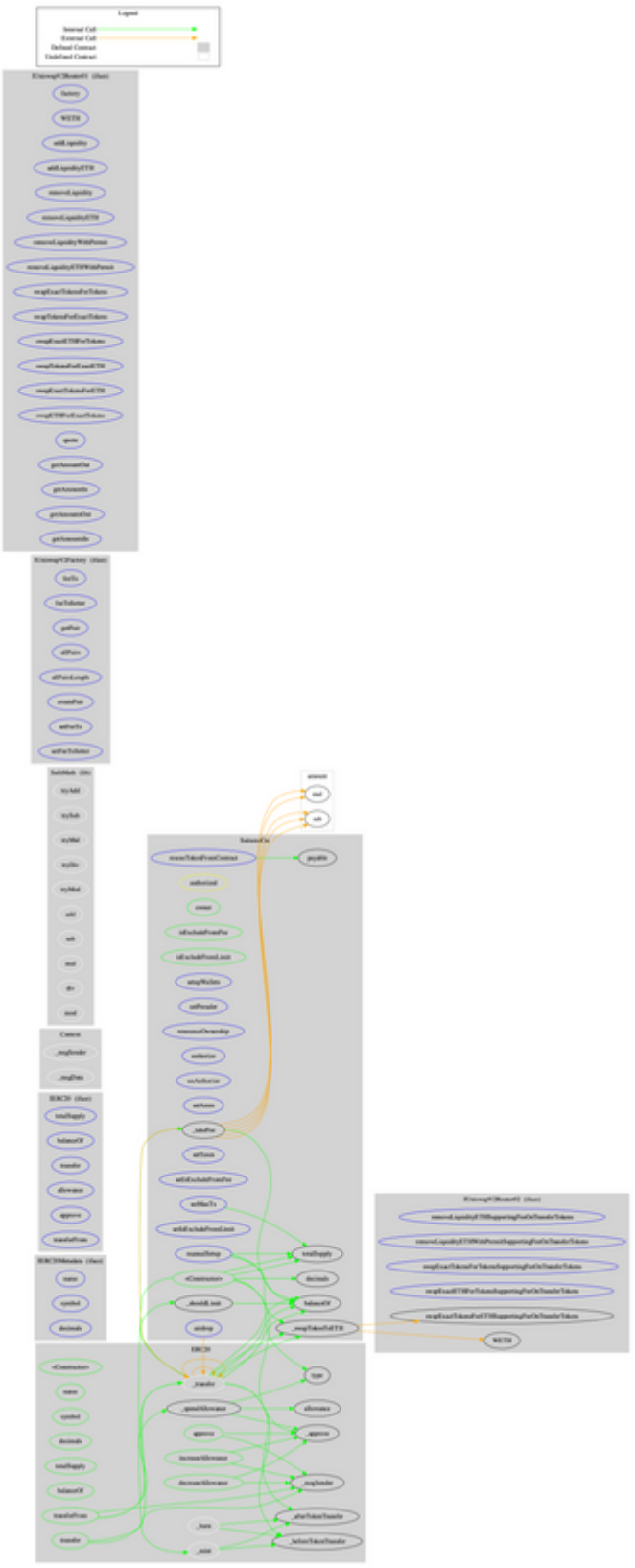
Contract	Type	Bases		
	Function Name	**Visibility**	**Mutability**	**Modifiers**
ERC20	Implementation	Context, IERC20, IERC20Metadata		
	<Constructor>	Public	✓	-
	name	Public		-
	symbol	Public		-
	decimals	Public		-
	totalSupply	Public		-
	balanceOf	Public		-
	transfer	Public	✓	-
	allowance	Public		-
	approve	Public	✓	-
	transferFrom	Public	✓	-
	increaseAllowance	Public	✓	-
	decreaseAllowance	Public	✓	-
	_transfer	Internal	✓	
	_mint	Internal	✓	
	_burn	Internal	✓	
	_approve	Internal	✓	
	_spendAllowance	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		
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		
IUniswapV2Factory	Interface			
	feeTo	External		-
	feeToSetter	External		-
	getPair	External		-
	allPairs	External		-
	allPairsLength	External		-
	createPair	External	✓	-
	setFeeTo	External	✓	-

	setFeeToSetter	External	✓	-
IUniswapV2Router01	Interface			
	factory	External		-
	WETH	External		-
	addLiquidity	External	✓	-
	addLiquidityETH	External	Payable	-
	removeLiquidity	External	✓	-
	removeLiquidityETH	External	✓	-
	removeLiquidityWithPermit	External	✓	-
	removeLiquidityETHWithPermit	External	✓	-
	swapExactTokensForTokens	External	✓	-
	swapTokensForExactTokens	External	✓	-
	swapExactETHForTokens	External	Payable	-
	swapTokensForExactETH	External	✓	-
	swapExactTokensForETH	External	✓	-
	swapETHForExactTokens	External	Payable	-
	quote	External		-
	getAmountOut	External		-
	getAmountIn	External		-
	getAmountsOut	External		-
	getAmountsIn	External		-
IUniswapV2Router02	Interface	IUniswapV2Router01		
	removeLiquidityETHSupportingFeeOnTransferTokens	External	✓	-
	removeLiquidityETHWithPermitSupportingFeeOnTransferTokens	External	✓	-
	swapExactTokensForTokensSupportingFeeOnTransferTokens	External	✓	-
	swapExactETHForTokensSupportingFeeOnTransferTokens	External	Payable	-
	swapExactTokensForETHSupportingFeeOnTransferTokens	External	✓	-
SaitamaCat	Implementation	ERC20		

	<Constructor>	Public	✓	ERC20
	decimals	Public		-
	owner	Public		-
	isExcludeFromFee	Public		-
	isExcludeFromLimit	Public		-
	setupWallets	External	✓	authorized
	setPresaler	External	✓	authorized
	renounceOwnership	External	✓	authorized
	authorize	External	✓	authorized
	unAuthorize	External	✓	authorized
	setAmm	External	✓	authorized
	rescueTokenFromContract	External	✓	authorized
	setTaxes	External	✓	authorized
	setIsExcludeFromFee	External	✓	authorized
	setMaxTx	External	✓	authorized
	setIsExcludeFromLimit	External	✓	authorized
	airdrop	External	✓	-
	_transfer	Internal	✓	
	_takeFee	Internal	✓	
	_shouldLimit	Internal		
	manualSetup	External	✓	authorized
	_swapTokenToETH	Internal	✓	

Contract Flow



Domain Info

Domain Name	
Registry Domain ID	2693994307_DOMAIN_COM-VRSN
Creation Date	2022-05-05T14:37:45.00Z
Updated Date	0001-01-01T00:00:00.00Z
Registry Expiry Date	2023-05-05T14:37:45.00Z
Registrar WHOIS Server	whois.namecheap.com
Registrar URL	http://www.namecheap.com
Registrar	NAMECHEAP INC
Registrar IANA ID	1068

The domain has been created about 19 hours before the creation of the audit. It will expire in 12 months.

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

Summary

There are some functions that can be abused by the owner like stopping transactions and transferring funds to the team’s wallet. 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.

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

The Cyberscope team

https://www.cyberscope.io