Cyberscope

Audit Report

Super Squid Game

July 2022

Type	BEP20
Network	BSC
Address	0xd462aed2d7477ffc70c0cbc136ee410f5bbd09c6
Audited by	© cyberscope

Table of Contents

Contract Review

Contract Name	SuperSquidGame
Compiler Version	v0.8.13+commit.abaa5c0e
Optimization	200 runs
Licence	MIT
Explorer	https://bscscan.com/token/0xd462aed2d7477ffc70c0cbc136ee410f5bbd09c6
Symbol	SSG
Decimals	9
Total Supply	10,000,000
Domain	supersquidgame.io

Source Files

Filename	**SHA256**
contract.sol	2c4d2beadab2d0c42b8a7f27b724344376d1ff282a3acf858bcaeaa28a7605a8

Audit Updates

Initial Audit	8th July 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

ELFM - Exceed Limit Fees Manipulation

Criticality	critical
Location	contract.sol#L2008

Description

The contract owner has the authority to increase over the allowed limit of 25%. The owner may take advantage of it by calling the `setSellFees` function with arguments that sum up to 9800. As a result the fees will be 98%.

```
function setSellFees(
    uint256 liquidityFee,
    uint256 marketingFee,
    uint256 devFee,
    uint256 jackpotFee
) external onlyAuthorized {
    require(
        liquidityFee.add(marketingFee).add(devFee).add(jackpotFee) <=
            TOTAL_FEES_LIMIT,
        "Total fees can not exceed the declared limit"
    );
    sLiquidityFee = liquidityFee;
    sMarketingFee = marketingFee;
    sDevFee = devFee;
    sJackpotFee = jackpotFee;
```

Recommendation

The contract could embody a check for the maximum acceptable value.

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
	L13	Divide before Multiply Operation

L01 - Public Function could be Declared External

Criticality	minor
Location	contract.sol#L158,171,184,197,217,222,243,253,1870,1874,1878,1882,1890,1899,1908,1929,1946,1959,2000,2004,2027,2055,2254,2263,2357,2362,2371,2378,2382,2396,2411,2415,2433,2445,2462,2759

Description

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

```
aboutMe
getPendingTokens
getPendingBalances
getLastBigBang
getLastAwarded
getLastBuy
jackpotBuybackAmount
jackpotBuyerShareAmount
getJackpot
...
```

Recommendation

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

L04 - Conformance to Solidity Naming Conventions

Criticality	minor
Location	contract.sol#L275,519,521,552,2060,2061,2062,2091,2092,2112,1693,1694,1695,1696

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.

```
_tTotal
_decimals
_symbol
_name
_jackpotTimespan
_jackpotHardLimit
_jackpotHardBuyback
_jackpotMinBuy
_jackpotBuyerShare
...
```

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#L1478,1491,1510,1530,1590,1608,1554,1573,1423,1447,1625,854,840,870,1018,934,1106,909,1081,1004,920,1092,899,1071,1034,950,1122

Description

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

```
values
remove
length
contains
at
_values
_length
_at
verifyCallResult
...
```

Recommendation

Remove unused functions.

L13 - Divide before Multiply Operation

Criticality	minor
Location	contract.sol#L2382,2396,2499

Description

Performing divisions before multiplications may cause lose of prediction.

```
tokensOut = _jackpotTokens.mul(jackpotCashout).div(MAX_PCT)
cashedOut = _pendingJackpotBalance.mul(jackpotCashout).div(MAX_PCT)
tokens =
_jackpotTokens.mul(jackpotCashout).div(MAX_PCT).mul(MAX_PCT.sub(jackpotBuyerShar
e)).div(MAX_PCT)
bnb =
_pendingJackpotBalance.mul(jackpotCashout).div(MAX_PCT).mul(MAX_PCT.sub(jackpotB
uyerShare)).div(MAX_PCT)
tokens =
_jackpotTokens.mul(jackpotCashout).div(MAX_PCT).mul(jackpotBuyerShare).div(MAX_P
CT)
bnb =
_pendingJackpotBalance.mul(jackpotCashout).div(MAX_PCT).mul(jackpotBuyerShare).d
iv(MAX_PCT)
```

Recommendation

The multiplications should be prior to the divisions.

Contract Functions

Contract	Type	Bases		
	Function Name	Visibility	Mutability	Modifiers
Context	Implementation			
	_msgSender	Internal		
	_msgData	Internal		
Ownable	Implementation	Context		
	<Constructor>	Public	✓	-
	owner	Public		-
	lockedLiquidity	Public		-
	devWallet	Public		-
	marketingWallet	Public		-
	buybackWallet	Public		-
	setDevWalletAddress	Public	✓	onlyOwner
	setMarketingWalletAddress	Public	✓	onlyOwner
	setBuybackWallet	Public	✓	onlyOwner
	setLockedLiquidityAddress	Public	✓	onlyOwner
	renounceOwnership	Public	✓	onlyOwner
	transferOwnership	Public	✓	onlyOwner
	authorize	Public	✓	onlyOwner
	unauthorize	Public	✓	onlyOwner
	isAuthorized	Public		-
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	✓	-
IUniswapV2Pair	Interface			
	name	External		-
	symbol	External		-
	decimals	External		-
	totalSupply	External		-
	balanceOf	External		-
	allowance	External		-
	approve	External	✓	-
	transfer	External	✓	-
	transferFrom	External	✓	-

	DOMAIN_SEPARATOR	External		-
	PERMIT_TYPEHASH	External		-
	nonces	External		-
	permit	External	✓	-
	MINIMUM_LIQUIDITY	External		-
	factory	External		-
	token0	External		-
	token1	External		-
	getReserves	External		-
	price0CumulativeLast	External		-
	price1CumulativeLast	External		-
	kLast	External		-
	mint	External	✓	-
	burn	External	✓	-
	swap	External	✓	-
	skim	External	✓	-
	sync	External	✓	-
	initialize	External	✓	-
IUniswapV2Factory	Interface			
	feeTo	External		-
	feeToSetter	External		-
	getPair	External		-
	allPairs	External		-
	allPairsLength	External		-
	createPair	External	✓	-
	setFeeTo	External	✓	-
	setFeeToSetter	External	✓	-
IERC20	Interface			
	totalSupply	External		-
	balanceOf	External		-
	transfer	External	✓	-
	allowance	External		-
	approve	External	✓	-

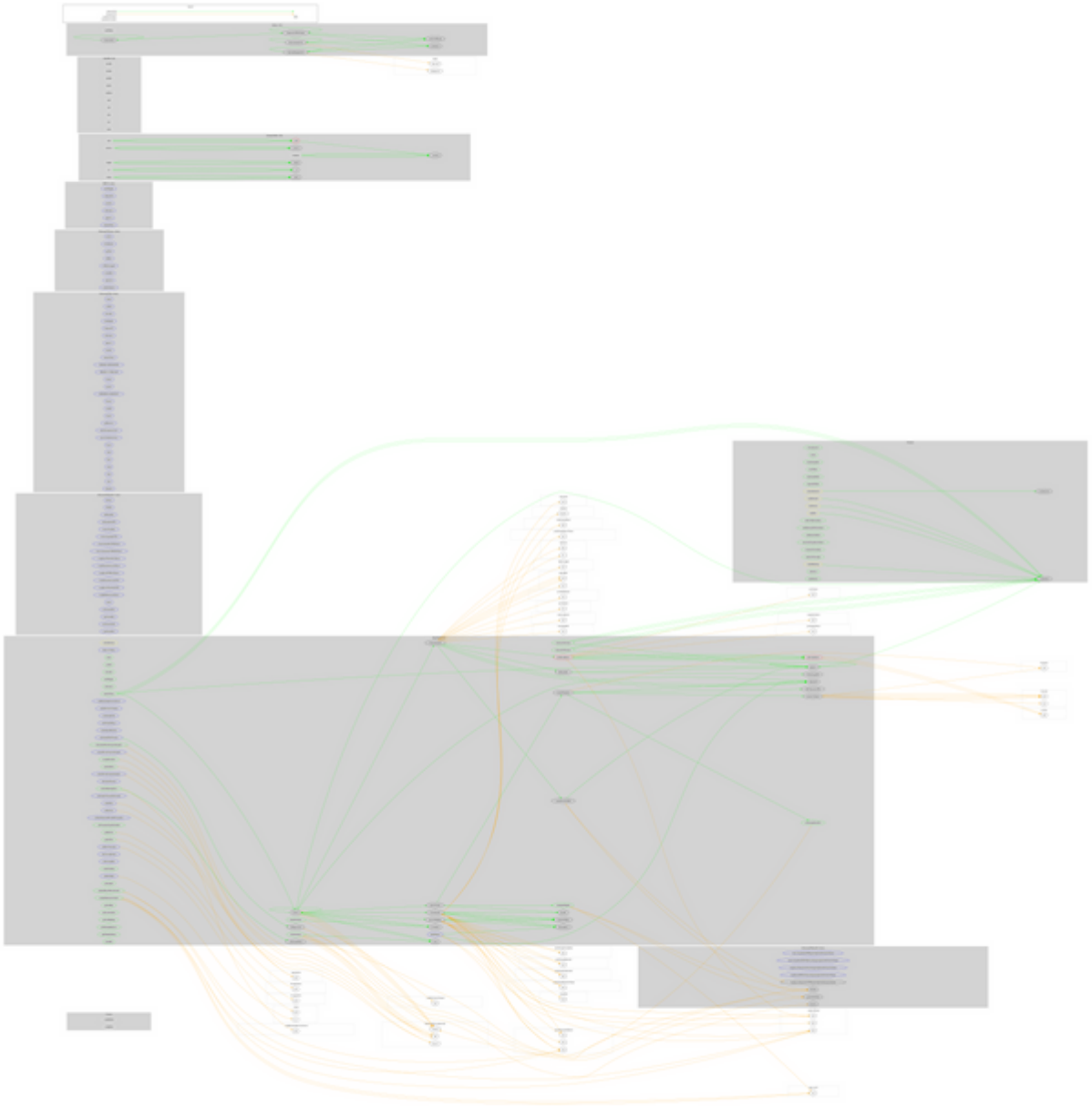
	transferFrom	External	✓	-
EnumerableSet	Library			
	_add	Private	✓	
	_remove	Private	✓	
	_contains	Private		
	_length	Private		
	_at	Private		
	_values	Private		
	add	Internal	✓	
	remove	Internal	✓	
	contains	Internal		
	length	Internal		
	at	Internal		
	values	Internal		
	add	Internal	✓	
	remove	Internal	✓	
	contains	Internal		
	length	Internal		
	at	Internal		
	values	Internal		
	add	Internal	✓	
	remove	Internal	✓	
	contains	Internal		
	length	Internal		
	at	Internal		
	values	Internal		
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		
Address	Library			
	isContract	Internal		
	sendValue	Internal	✓	
	functionCall	Internal	✓	
	functionCall	Internal	✓	
	functionCallWithValue	Internal	✓	
	functionCallWithValue	Internal	✓	
	functionStaticCall	Internal		
	functionStaticCall	Internal		
	functionDelegateCall	Internal	✓	
	functionDelegateCall	Internal	✓	
	verifyCallResult	Internal		
SuperSquidGame	Implementation	Context, IERC20, Ownable		
	<Constructor>	Public	✓	Ownable
	<Receive Ether>	External	Payable	-
	name	Public		-
	symbol	Public		-
	decimals	Public		-
	totalSupply	Public		-
	balanceOf	Public		-
	transfer	Public	✓	-
	allowance	Public		-
	approve	Public	✓	-
	approve	Private	✓	
	transferFrom	Public	✓	-

	increaseAllowance	Public	✓	-
	decreaseAllowance	Public	✓	-
	totalMarketingFeesCollected	External		onlyMarketing
	totalDevFeesCollected	External		onlyDev
	totalJackpotOut	External		-
	totalJackpotBuyer	External		-
	totalJackpotBuyback	External		-
	excludeFromFee	Public	✓	onlyAuthorized
	includeInFee	Public	✓	onlyAuthorized
	setBuyFees	External	✓	onlyAuthorized
	getBuyTax	Public		-
	setSellFees	External	✓	onlyAuthorized
	getSellTax	Public		-
	setJackpotFeatures	External	✓	onlyAuthorized
	setJackpotHardFeatures	External	✓	onlyAuthorized
	setJackpotTimespanInSeconds	External	✓	onlyAuthorized
	setMaxTxAmount	External	✓	onlyAuthorized
	setMaxWallet	External	✓	onlyAuthorized
	setNumTokensSellToAddToLiquidity	External	✓	onlyAuthorized
	fundJackpot	External	Payable	onlyAuthorized
	isJackpotEligible	Public		-
	usdEquivalent	Public		-
	getUsedTokens	Private		
	getTokenShares	Private	✓	
	setSwapAndLiquifyEnabled	Public	✓	onlyOwner
	isExcludedFromFee	Public		-
	isExcludedFromSwapAndLiquify	Public		-
	includeFromSwapAndLiquify	External	✓	onlyOwner
	excludeFromSwapAndLiquify	External	✓	onlyOwner
	setUniswapRouter	External	✓	onlyOwner
	setUniswapPair	External	✓	onlyOwner
	transfer	Private	✓	
	enableTrading	Public	✓	onlyOwner
	collectMarketingFees	Public	✓	onlyMarketing
	collectDevFees	Public	✓	onlyDev

	getJackpot	Public		-
	jackpotBuyerShareAmount	Public		-
	jackpotBuybackAmount	Public		-
	getLastBuy	Public		-
	getLastAwarded	Public		-
	getLastBigBang	Public		-
	getPendingBalances	Public		onlyAuthorized
	getPendingTokens	Public		onlyAuthorized
	processBigBang	Private	✓	lockTheSwap
	awardJackpot	Private	✓	lockTheSwap
	swapAndLiquify	Private	✓	lockTheSwap
	swapTokensForBnb	Private	✓	
	addLiquidity	Private	✓	
	tokenTransfer	Private	✓	
	transferBasic	Private	✓	
	transferStandard	Private	✓	
	processAmount	Private		
	takeTransactionFee	Private	✓	
	aboutMe	Public		-

Contract Flow



Domain Info

Domain Name	supersquidgame.io
Registry Domain ID	024e21aff9694f05887d057a0e3ecd63-DONUTS
Creation Date	2022-06-30T03:39:10Z
Updated Date	2022-07-08T03:06:18Z
Registry Expiry Date	2023-06-30T03:39:10Z
Registrar WHOIS Server	whois.namecheap.com
Registrar URL	https://www.namecheap.com/
Registrar	NameCheap, Inc.
Registrar IANA ID	1068

The domain has been created in 12 months before the creation of the audit.

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

Summary

The Smart Contract analysis reported one critical severity issue. The contract owner has the authority to manipulate the fees. 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 provide all the essential tools to assist users draw their own conclusions.

The Cyberscope team

https://www.cyberscope.io