Cyberscope

Audit Report

SU

March 2022

Type	BEP20
Network	BSC
Address	0x35b32d4be30e6C9464eD62172eb93bA63F16aE10
Audited by	© cyberscope

Table of Contents

Table of Contents 1
Contract Review 3
Audit Updates 3
Contract Analysis 4
ULTW - Unlimited Liquidity to Team Wallet 5
Description 5
Recommendation 5
BC - Blacklisted Contracts 7
Description 7
Recommendation 7
Contract Diagnostics 8
FSA - Fixed Swap Address 9
Description 9
Recommendation 9
L01 - Public Function could be Declared External 10
Description 10
Recommendation 10
L02 - State Variables could be Declared Constant 11
Description 11
Recommendation 11
L04 - Conformance to Solidity Naming Conventions 12
Description 12
Recommendation 12
L09 - Dead Code Elimination 13
Description 13
Recommendation 13

L07 - Missing Events Arithmetic 14
Description 14
Recommendation 14
Contract Functions 15
Contract Flow 19
Domain Info 20
Summary 21
Disclaimer 22
About Cyberscope 23

Contract Review

Contract Name	SU
Compiler Version	v0.6.12+commit.27d51765
Optimization	200 runs
Licence	MIT
Explorer	https://bscscan.com/token/0x35b32d4be30e6C9464eD62172eb93bA63F16aE10
Symbol	SU
Decimals	18
Total Supply	1,000,000
Source	SU.sol
Domain	constellationstart.com

Audit Updates

Initial Audit	3rd March 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

ULTW - Unlimited Liquidity to Team Wallet

Criticality	minor
Location	contract.sol#L781

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 setting a high calling the `emergencyWithdraw` function.

The contract accumulates 10% fixed funds from every transaction. The sale transactions are transferring the fees to the dead wallet until they reach a threshold. These funds are applicable to be liquified.

```
function emergencyWithdraw(address _token, uint256 amount)
    public
    onlyOwner
{
    uint256 balance;
    if (_token == address(0x0)) {
        balance = address(this).balance;
        if (amount > balance || amount == 0) {
            amount = balance;
        }
        payable(msg.sender).transfer(amount);
        return;
    }

    IBEP20 token = IBEP20(_token);
    balance = token.balanceOf(address(this));
    if (amount > balance || amount == 0) {
        amount = balance;
    }
    token.transfer(msg.sender, amount);
}
```

Recommendation

The contract could embody a check for a maximum withdrawal limit.

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	contract.sol#L657

Description

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

```
require(!isBot[sender] && !isBot[recipient], "BEP20: bot not allowed");
```

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
	FSA	Fixed Swap Address
	L01	Public Function could be Declared External
	L02	State Variables could be Declared Constant
	L04	Conformance to Solidity Naming Conventions
	L09	Dead Code Elimination
	L07	Missing Events Arithmetic

FSA - Fixed Swap Address

Criticality	minor
Location	contract.sol#L534

Description

The swap address is assigned once in the constructor and it can not be changed. The decentralized swaps sometimes create a new swap version or abandon the current. A contract that cannot change the swap address may not be able to catch-up the upgrade.

```
IUniswapV2Router02 _uniswapV2Router = IUniswapV2Router02(
    0x10ED43C718714eb63d5aA57B78B54704E256024E
);
uniswapV2Pair = IUniswapV2Factory(_uniswapV2Router.factory())
    .createPair(address(this), _uniswapV2Router.WETH());
uniswapV2Router = _uniswapV2Router;
```

Recommendation

It could be better to allow the swap address mutation in case of future swap updates.

L01 - Public Function could be Declared External

Criticality	minor
Location	contract.sol#L142,147,622,634,703,708,739,743,752,756 and 1 more

Description

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

```
setBurnLimitPercent
batchSetWhitelists
setWhitelist
batchSetBots
setBot
setNumTokensSellToAddToLiquidity
setSwapAndLiquifyEnabled
decreaseAllowance
increaseAllowance
...
```

Recommendation

Use the external attribute for functions never called from the contract

L02 - State Variables could be Declared Constant

Criticality	minor
Location	contract.sol#L514,516,512

Description

Constant state variables should be declared constant to save gas.

```
marketingAddress
fee
deadAddress
```

Recommendation

Add the constant attribute to state variables that never change.

L04 - Conformance to Solidity Naming Conventions

Criticality	minor
Location	contract.sol#L220,222,252,296,703,739,743,752,756,781 and 3 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.

```
_name
_symbol
_decimals
_token
_isWhitelisted
_isBot
_enabled
WETH
MINIMUM_LIQUIDITY
...
```

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#L48,105,109

Description

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

```
mod
_msgData
```

Recommendation

Remove unused functions.

L07 - Missing Events Arithmetic

Criticality	minor
Location	contract.sol#L708,765

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.

```
burnLimitPercent = val
numTokensSellToAddToLiquidity = val
```

Recommendation

Emit an event for critical parameter changes.

Contract Functions

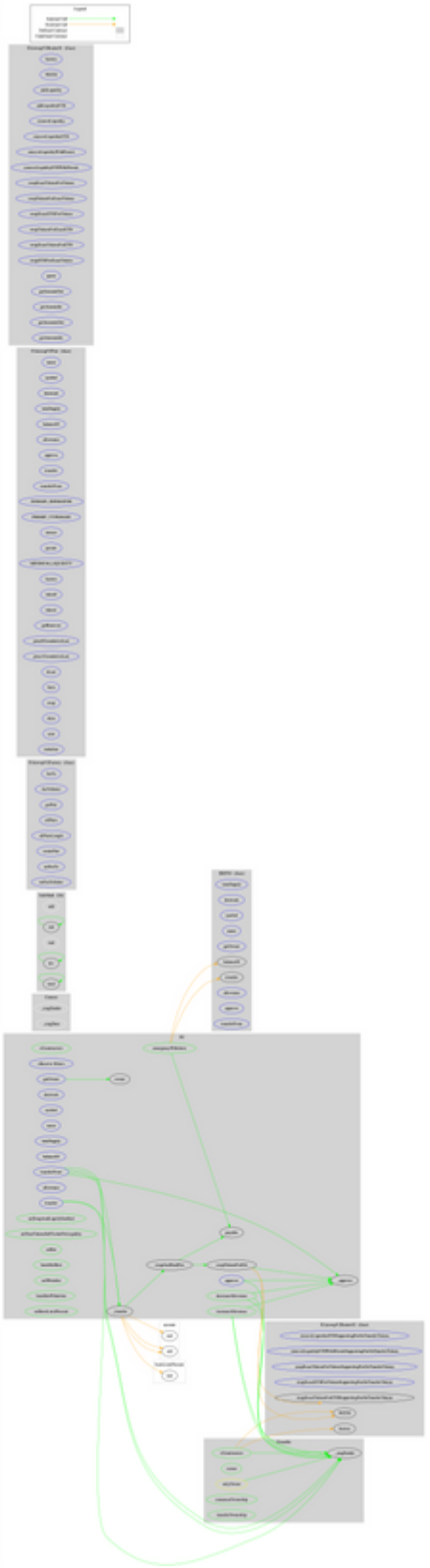
Contract	Type	Bases		
	Function Name	Visibility	Mutability	Modifiers
IBEP20	Interface			
	totalSupply	External		-
	decimals	External		-
	symbol	External		-
	name	External		-
	getOwner	External		-
	balanceOf	External		-
	transfer	External	✓	-
	allowance	External		-
	approve	External	✓	-
	transferFrom	External	✓	-
Context	Implementation			
	_msgSender	Internal		
	_msgData	Internal		
SafeMath	Library			
	add	Internal		
	sub	Internal		
	sub	Internal		
	mul	Internal		
	div	Internal		
	div	Internal		
	mod	Internal		
	mod	Internal		
Ownable	Implementation	Context		
	<Constructor>	Public	✓	-
	owner	Public		-

	renounceOwnership	Public	✓	onlyOwner
	transferOwnership	Public	✓	onlyOwner
IUniswapV2Factory	Interface			
	feeTo	External		-
	feeToSetter	External		-
	getPair	External		-
	allPairs	External		-
	allPairsLength	External		-
	createPair	External	✓	-
	setFeeTo	External	✓	-
	setFeeToSetter	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		-
	burn	External	✓	-
	swap	External	✓	-
	skim	External	✓	-
	sync	External	✓	-
	initialize	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	✓	-
SU	Implementation	Context, IBEP20, Ownable		
	<Constructor>	Public	✓	-
	<Receive Ether>	External	Payable	-
	getOwner	External		-
	decimals	External		-
	symbol	External		-
	name	External		-
	totalSupply	External		-
	balanceOf	External		-
	transfer	External	✓	-
	allowance	External		-
	approve	External	✓	-
	transferFrom	External	✓	-
	increaseAllowance	Public	✓	-
	decreaseAllowance	Public	✓	-
	_transfer	Internal	✓	
	setSwapAndLiquifyEnabled	Public	✓	onlyOwner
	setNumTokensSellToAddToLiquidity	Public	✓	onlyOwner
	swapAndSendFee	Private	✓	
	swapTokensForEth	Private	✓	
	setBot	Public	✓	onlyOwner
	batchSetBots	Public	✓	onlyOwner
	setWhitelist	Public	✓	onlyOwner
	batchSetWhitelists	Public	✓	onlyOwner
	setBurnLimitPercent	Public	✓	onlyOwner
	_approve	Internal	✓	
	emergencyWithdraw	Public	✓	onlyOwner

Contract Flow



Domain Info

Domain Name	constellationstart.com
Registry Domain ID	2676632668_DOMAIN_COM-VRSN
Creation Date	2022-02-21T17:14:10
Updated Date	2022-02-21T17:14:10
Registry Expiry Date	
Registrar WHOIS Server	whois.wix.com
Registrar URL	http://www.wix.com
Registrar	Wix.Com Ltd.
Registrar IANA ID	3817

The domain has been created 10 days before the creation of the audit.

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 massively blacklisting 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.

The fee percentage is fixed to 10%. The contract accumulates the fees in order to liquify and send them to the dev’s wallet. The sale transactions are transferring the fess to the dead wallet until they reach a threshold. This threshold is defined by the contract owner.

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