Cyberscope

Audit Report

GREENSPACE

October 2022

Type	BEP20
Network	BSC
Address	0xa013aD999Aa00F40b8cd80FbaCAe1357DBbAaDfD
Audited by	© cyberscope

Table of Contents

Contract Review

Contract Name	GREENSPACE
Compiler Version	v0.7.6+commit.7338295f
Optimization	200 runs
Licence	None
Explorer	https://bscscan.com/token/0xa013aD999Aa00F40b8cd80FbaCAe1357DBbAaDfD
Symbol	GREENSPACE
Decimals	5
Total Supply	250,000
Domain	https://www.greenspacetoken.com

Source Files

Filename	SHA256
contract.sol	9e00599db2713309c33fa04b7adf3dd57bacfdec747f513f0ce3668cf0d0b774

Audit Updates

Initial Audit	3rd October 2022
Corrected	24th October 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	**Resolved**
●	MT	Mints Tokens	Passed
●	BT	Burns Tokens	Passed
●	BC	Blacklists Addresses	**Resolved**

ULTW - Transfers Liquidity to Team Wallet

Criticality	minor / informative
Location	contract.sol#L919
Status	Resolved

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 `withdrawAllToTreasury` methods.

```
function withdrawAllToTreasury() external swapping onlyOwner {

    uint256 amountToSwap = _gonBalances[address(this)].div(_gonsPerFragment);
    require( amountToSwap > 0,"There is no GREENSPACE token deposited in token contract");
    address[] memory path = new address[](2);
    path[0] = address(this);
    path[1] = router.WETH();
    router.swapExactTokensForETHSupportingFeeOnTransferTokens(
        amountToSwap,
        0,
        path,
        treasuryReceiver,
        block.timestamp
    );
}
```

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.

Updated 24 October 2022

The team has renounced ownership and resolved the issues.

BC - Blacklists Addresses

Criticality	minor
Location	contract.sol#L1103
Status	Resolved

Description

The contract owner has the authority to stop only contracts from transactions. The owner may take advantage of it by calling the `setBotBlacklist` function.

```
function setBotBlacklist(address _botAddress, bool _flag) external onlyOwner {
        require(isContract(_botAddress), "only contract address, not allowed externally owned account");
        blacklist[_botAddress] = _flag;
    }
```

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.

Updated 24 October 2022

The team has renounced ownership and resolved the issues.

Contract Diagnostics

Critical Medium Minor / Informative

Severity	Code	Description	Status
Medium	BLC	Business Logic Concern	Unresolved
Minor	MTS	Manipulate Total Supply	Resolved
Minor	L01	Public Function could be Declared External	Unresolved
Minor	L02	State Variables could be Declared Constant	Unresolved
Minor	L04	Conformance to Solidity Naming Conventions	Unresolved
Minor	L05	Unused State Variable	Unresolved
Minor	L07	Missing Events Arithmetic	Unresolved
Minor	L09	Dead Code Elimination	Unresolved
Minor	L13	Divide before Multiply Operation	Unresolved
Minor	L14	Uninitialized Variables in Local Scope	Unresolved

BLC - Business Logic Concern

Criticality	medium
Location	contract.sol#L703,1079
Status	Unresolved

Description

An unsigned integer can either be greater or less than a number (385 days). As a result, the rest conditions will never executed.

```
if (deltaTimeFromInit < (385 days)) {
    rebaseRate = 450;
} else if (deltaTimeFromInit >= (385 days)) {
    rebaseRate = 120;
} else if (deltaTimeFromInit >= ((15 * 365 days) / 10)) {
    rebaseRate = 12;
} else if (deltaTimeFromInit >= (7 * 365 days)) {
    rebaseRate = 6;
}
```

The autofirePit usually refers to a burn mechanism. The contract owner has the authority to change the address of the autofirePit. As a result, the autofirePit fee will not be transferred to the dead address.

```
function setFeeReceivers(
        address _autoLiquidityReceiver,
        address _treasuryReceiver,
        address _autofirePit
    ) external onlyOwner {
        autoLiquidityReceiver = _autoLiquidityReceiver;
        treasuryReceiver = _treasuryReceiver;
        autofirePit = _autofirePit;
    }
```

Recommendation

The contract should remove the branch logic that will never be executed.

The autofirePit address should not be able to change.

MTS - Manipulate Total Supply

Criticality	minor / informative
Location	contract.sol#L694
Status	Resolved

Description

Owner is able to manipulate total supply. This change will have a direct impact on the token price and Market Cap.

```
function rebase() internal {
      / /..

       for (uint256 i = 0; i < times; i++) {
          _totalSupply = _totalSupply
              .mul((10**RATE_DECIMALS).add(rebaseRate))
              .div(10**RATE_DECIMALS);
       }

       _gonsPerFragment = TOTAL_GONS.div(_totalSupply);
       _lastRebasedTime = _lastRebasedTime.add(times.mul(15 minutes));

       pairContract.sync();

       emit LogRebase(epoch, _totalSupply);
   }
```

Recommendation

The contract owner should carefully manage the adjustment of the circulating supply (increases or decreases), according to the token's price fluctuations.

Updated 24 October 2022

The team has renounced ownership and resolved the issues.

L01 - Public Function could be Declared External

Criticality	minor / informative
Location	contract.sol#L571,567,563,532,519,537,1085
Status	Unresolved

Description

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

```
decimals
symbol
name
renounceOwnership
owner
transferOwnership
getLiquidityBacking
```

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#L610,600,620,601,602,369,598,599,609,607
Status	Unresolved

Description

Constant state variables should be declared constant to save gas.

```
ZERO
GSDividendFee
swapEnabled
sellFee
autofirePitFee
dividendsPerShareAccuracyFactor
liquidityFee
treasuryFee
DEAD
...
```

Recommendation

Add the constant attribute to state variables that never change.

L04 - Conformance to Solidity Naming Conventions

Criticality	minor / informative
Location	contract.sol#L637,609,1099,641,152,600,973,964,353,636,1051,189,1104,640,616,1077,1076,391,151,1078,169,1036,345,1095,639,610,584,638
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.

```
_autoAddLiquidity
DEAD
_flag
_totalSupply
PERMIT_TYPEHASH
GSDividendFee
BUSD
_autoRebase
_minDistribution
...
```

Recommendation

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

L05 - Unused State Variable

Criticality	minor / informative
Location	contract.sol#L18
Status	Unresolved

Description

There are segments that contain unused state variables.

```
MAX_INT256
```

Recommendation

Remove unused state variables.

L07 - Missing Events Arithmetic

Criticality	minor / informative
Location	contract.sol#L391
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#L46
Status	Unresolved

Description

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

```
abs
```

Recommendation

Remove unused functions.

L13 - Divide before Multiply Operation

Criticality	minor / informative
Location	contract.sol#L690,804,1085
Status	Unresolved

Description

Performing divisions before multiplications may cause lose of prediction.

```
times = deltaTime.div(900)
_gonBalances[autofirePit] =
_gonBalances[autofirePit].add(gonAmount.div(feeDenominator).mul(autofirePitFee))
feeAmount = gonAmount.div(feeDenominator).mul(_totalFee)
_gonBalances[autoLiquidityReceiver] =
_gonBalances[autoLiquidityReceiver].add(gonAmount.div(feeDenominator).mul(liquidityFee))
liquidityBalance = _gonBalances[pair].div(_gonsPerFragment)
_gonBalances[address(this)] =
_gonBalances[address(this)].add(gonAmount.div(feeDenominator).mul(_treasuryFee.add(GSDividendFee)))
```

Recommendation

The multiplications should be prior to the divisions.

L14 - Uninitialized Variables in Local Scope

Criticality	minor / informative
Location	contract.sol#L693
Status	Unresolved

Description

The are variables that are defined in the local scope and are not initialized.

```
rebaseRate
```

Recommendation

All the local scoped variables should be initialized.

Contract Functions

Contract	Type	Bases		
	Function Name	Visibility	Mutability	Modifiers
SafeMathInt	Library			
	mul	Internal		
	div	Internal		
	sub	Internal		
	add	Internal		
	abs	Internal		
SafeMath	Library			
	add	Internal		
	sub	Internal		
	sub	Internal		
	mul	Internal		
	div	Internal		
	div	Internal		
	mod	Internal		
IERC20	Interface			
	totalSupply	External		-
	balanceOf	External		-
	allowance	External		-
	transfer	External	✓	-
	approve	External	✓	-
	transferFrom	External	✓	-
IPancakeSwapPair	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	✓	-
IPancakeSwap Router	Interface			
	factory	External		-
	WETH	External		-
	addLiquidity	External	✓	-
	addLiquidityETH	External	Payable	-
	removeLiquidity	External	✓	-
	removeLiquidityETH	External	✓	-
	removeLiquidityWithPermit	External	✓	-
	removeLiquidityETHWithPermit	External	✓	-

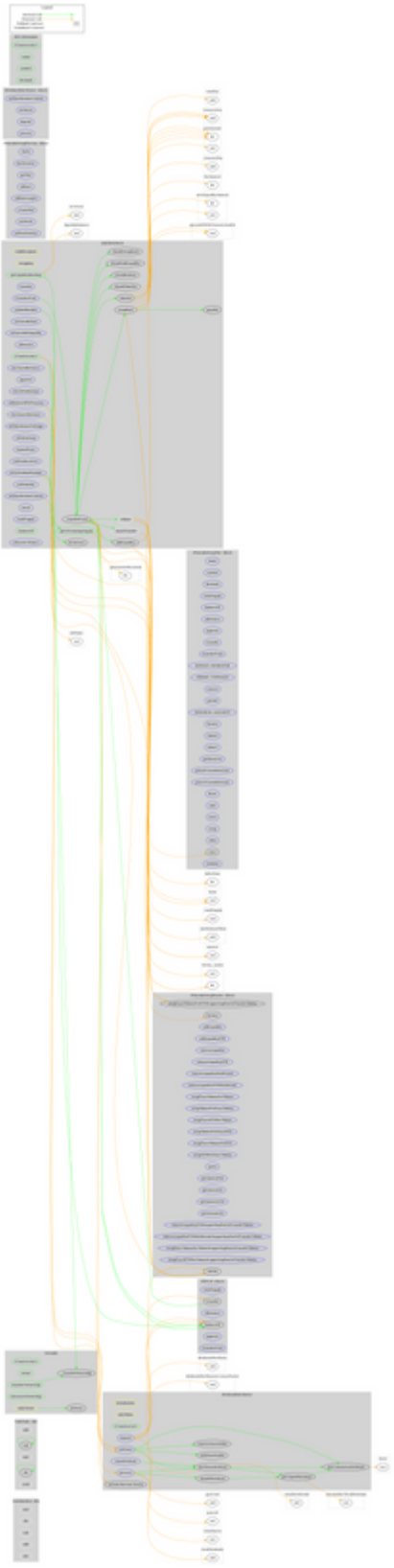
	swapExactTokensForTokens	External	✓	-
	swapTokensForExactTokens	External	✓	-
	swapExactETHForTokens	External	Payable	-
	swapTokensForExactETH	External	✓	-
	swapExactTokensForETH	External	✓	-
	swapETHForExactTokens	External	Payable	-
	quote	External		-
	getAmountOut	External		-
	getAmountIn	External		-
	getAmountsOut	External		-
	getAmountsIn	External		-
	removeLiquidityETHSupportingFeeOnTransferTokens	External	✓	-
	removeLiquidityETHWithPermitSupportingFeeOnTransferTokens	External	✓	-
	swapExactTokensForTokensSupportingFeeOnTransferTokens	External	✓	-
	swapExactETHForTokensSupportingFeeOnTransferTokens	External	Payable	-
	swapExactTokensForETHSupportingFeeOnTransferTokens	External	✓	-
IPancakeSwapFactory	Interface			
	feeTo	External		-
	feeToSetter	External		-
	getPair	External		-
	allPairs	External		-
	allPairsLength	External		-
	createPair	External	✓	-
	setFeeTo	External	✓	-
	setFeeToSetter	External	✓	-
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	✓	
Ownable	Implementation			
	<Constructor>	Public	✓	-
	owner	Public		-
	isOwner	Public		-
	renounceOwnership	Public	✓	onlyOwner
	transferOwnership	Public	✓	onlyOwner
	_transferOwnership	Internal	✓	
ERC20Detailed	Implementation	IERC20		
	<Constructor>	Public	✓	-
	name	Public		-
	symbol	Public		-
	decimals	Public		-
GREENSPACE	Implementation	ERC20Detailed, Ownable		

	<Constructor>	Public	✓	ERC20Detailed Ownable
	rebase	Internal	✓	
	transfer	External	✓	validRecipient
	transferFrom	External	✓	validRecipient
	_basicTransfer	Internal	✓	
	_transferFrom	Internal	✓	
	takeFee	Internal	✓	
	addLiquidity	Internal	✓	swapping
	swapBack	Internal	✓	swapping
	withdrawAllToTreasury	External	✓	swapping onlyOwner
	shouldTakeFee	Internal		
	shouldRebase	Internal		
	shouldAddLiquidity	Internal		
	shouldSwapBack	Internal		
	setAutoRebase	External	✓	onlyOwner
	setAutoAddLiquidity	External	✓	onlyOwner
	allowance	External		-
	decreaseAllowance	External	✓	-
	increaseAllowance	External	✓	-
	approve	External	✓	-
	checkFeeExempt	External		-
	setIsDividendExempt	External	✓	onlyOwner
	setDistributionCriteria	External	✓	onlyOwner
	setDistributorSettings	External	✓	onlyOwner
	getCirculatingSupply	Public		-
	isNotInSwap	External		-
	manualSync	External	✓	-
	setFeeReceivers	External	✓	onlyOwner
	getLiquidityBacking	Public		-
	setWhitelist	External	✓	onlyOwner
	setBotBlacklist	External	✓	onlyOwner
	setLP	External	✓	onlyOwner
	totalSupply	External		-

	balanceOf	Public		-
	isContract	Internal		
	<Receive Ether>	External	Payable	-

Contract Flow



Domain Info

Domain Name	greenspacetoken.com
Registry Domain ID	2723705293_DOMAIN_COM-VRSN
Creation Date	2022-09-07T05:09:55Z
Updated Date	2022-09-07T05:09:55Z
Registry Expiry Date	2023-09-07T05:09:55Z
Registrar WHOIS Server	whois.godaddy.com
Registrar URL	https://www.godaddy.com
Registrar	GoDaddy.com, LLC
Registrar IANA ID	146

The domain was created 26 days before the creation of the audit. It will expire in 11 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 transferring funds to the team’s wallet and blacklisting addresses. A multi-wallet signing pattern will provide security against potential hacks. Temporarily locking the contract or renouncing ownership will eliminate all the contract threats. There is also a fixed fee of 16%.

Updated 24 October 2022

The team has renounced ownership and resolved the owner’s permissions related issues.

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