Cyberscope

Audit Report

GreenTech

August 2022

Type	BEP20
Network	BSC
Address	0xaAA75ab5ECd2Ba6966458D7Bd93A32b0Afe60f33
Audited by	© cyberscope

Table of Contents

Table of Contents 1
Contract Review 3
Audit Updates 3
Source Files 4
Contract Analysis 6
OCTD - Transfers Contract's Tokens 7
Description 7
Recommendation 7
ELFM - Exceeds Fees Limit 8
Description 8
Recommendation 10
Contract Diagnostics 11
BLC - Business Logic Concern 12
Description 12
Recommendation 13
L01 - Public Function could be Declared External 14
Description 14
Recommendation 14
L04 - Conformance to Solidity Naming Conventions 15
Description 15
Recommendation 15
L07 - Missing Events Arithmetic 16
Description 16
Recommendation 16
L13 - Divide before Multiply Operation 17
Description 17

Recommendation 17
Contract Functions 18
Contract Flow 22
Summary 23
Disclaimer 24
About Cyberscope 25

Contract Review

Contract Name	GreenTech
Compiler Version	v0.8.16+commit.07a7930e
Optimization	200 runs
Explorer	https://bscscan.com/token/0xaAA75ab5ECd2Ba6966458D7Bd93A32b0Afe60f33
Symbol	GTECH
Decimals	18
Total Supply	10,000,000,000

Audit Updates

Initial Audit	1st September 2022
Corrected	

Source Files

Filename	SHA256
@openzeppelin/contracts/access/Ownable.sol	0195650aabf5270babe540969c56f8f244342aebce89266787a3b015e41d608f
@openzeppelin/contracts/interfaces/IERC20.sol	81d367c8c643a25ad0733d22ae9ee9cf2b5aead302e2416c7233bc1dd0c56c7c
@openzeppelin/contracts/token/ERC20/ERC20.sol	80e33e340442acecc4bd995b4ead9b51adc4231c8213357fca18996b945f850b
@openzeppelin/contracts/token/ERC20/extensions/ERC20Burnable.sol	600052c7df2ee2e969592df597ae5f78aad5822c8bee181e58b2713321efb888
@openzeppelin/contracts/token/ERC20/extensions/IERC20Metadata.sol	4e2ce556a0419415ec3b01a0fa0322c20d6d53de5a05728c068e90d5684486c1
@openzeppelin/contracts/token/ERC20/IERC20.sol	b2565dec975f684ef0edfa505e212d0d0b602e1311afab782ea06ea8d3f49bb6
@openzeppelin/contracts/utils/Context.sol	5828bf38f9376b659a8edbbe2df0d06b29a09e37ecd470465dda2bbcb612c85d
@openzeppelin/contracts/utils/math/SafeMath.sol	a6357cd855b7f26b18812e89084475213054c3c76ce12ff2b82f4f9b3b5ae76b
contracts/Green	09189b89f5f034c053fda76cd358097f4dbae06523653353

Tech.sol	89b482153098f0dd
contracts/interface/IUniswapFactory.sol	355315153855a505f660047d2eec8e164cbbbfc7ee497f1aec2114cb63a0f4d9
contracts/interface/IUniswapV2Router.sol	7d97e4f187732c5bfd111400adaebab5cb37409bb602641fba5feee73a95c0c6

Contract Analysis

● Critical ● Medium ● Minor / Informative ● Pass

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

OCTD - Transfers Contract's Tokens

Criticality	minor / informative
Location	contract.sol#L810
Status	Unresolved

Description

The contract owner has the authority to claim all the balance of the contract. The owner may take advantage of it by calling the sendDustBNB function.

```
function sendDustBNB(address payable _recipient) public onlyOwner {
        _recipient.transfer(address(this).balance);
}
```

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.

ELFM - Exceeds Fees Limit

Criticality	critical
Location	contract.sol#L243,262,281,300,319,339,358
Status	Unresolved

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 setBurnFee, setLiquidityFee, setProjectFee, setMarketingFee, setDevelopmentFee, setEcoFee, setPartnerFee methods with the maximum acceptable value. The maximum acceptable value is 10%. As a result the total fees will be 70%

```
function setBurnFee(
    uint256 buy,
    uint256 sell,
    uint256 p2p
) external onlyOwner {
    require(
        buy <= maxIndividualFee &&
            sell <= maxIndividualFee &&
            p2p <= maxIndividualFee,
        "You must respect the maximum allowed fee"
    );


function setLiquidityFee(
    uint256 buy,
    uint256 sell,
    uint256 p2p
) external onlyOwner {
    require(
        buy <= maxIndividualFee &&
            sell <= maxIndividualFee &&
            p2p <= maxIndividualFee,
        "You must respect the maximum allowed fee"
    );
```

```
function setProjectFee(
        uint256 buy,
        uint256 sell,
        uint256 p2p
    ) external onlyOwner {
        require(
            buy <= maxIndividualFee &&
                sell <= maxIndividualFee &&
                p2p <= maxIndividualFee,
            "You must respect the maximum allowed fee"
        );


 function setMarketingFee(
        uint256 buy,
        uint256 sell,
        uint256 p2p
    ) external onlyOwner {
        require(
            buy <= maxIndividualFee &&
                sell <= maxIndividualFee &&
                p2p <= maxIndividualFee,
            "You must respect the maximum allowed fee"
        );


    function setDevelopmentFee(
        uint256 buy,
        uint256 sell,
        uint256 p2p
    ) external onlyOwner {
        require(
            buy <= maxIndividualFee &&
                sell <= maxIndividualFee &&
                p2p <= maxIndividualFee,
            "You must respect the maximum allowed fee"
        );


    function setEcoFee(
        uint256 buy,
        uint256 sell,
        uint256 p2p
    ) external onlyOwner {
        require(
            buy <= maxIndividualFee &&
                sell <= maxIndividualFee &&
                p2p <= maxIndividualFee,
            "You must respect the maximum allowed fee"
        );
```

```
function setPartnerFee(
        uint256 buy,
        uint256 sell,
        uint256 p2p
    ) external onlyOwner {
        require(
            buy <= maxIndividualFee &&
                sell <= maxIndividualFee &&
                p2p <= maxIndividualFee,
            "You must respect the maximum allowed fee"
        );
```

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 / Informative

Severity	Code	Description	Status
●	BLC	Business Logic Concern	Unresolved
●	L01	Public Function could be Declared External	Unresolved
●	L04	Conformance to Solidity Naming Conventions	Unresolved
●	L07	Missing Events Arithmetic	Unresolved
●	L13	Divide before Multiply Operation	Unresolved

BLC - Business Logic Concern

Criticality	medium
Location	contracts#L48
Status	Unresolved

Description

The variables `marketingPart, developmentPart, projectPart, ecoPart, partnerPart, liquidityPart` are transferred to the corresponding wallet but they are not subtracting from the corresponding variables `marketingFeeTotal, developmentFeeTotal ,projectFeeTotal, ecoFeeTotal, partnerFeeTotal, liquidityFeeTotal`. On the contrary new values are calculated that might produce conflict. For instance, the `swapTokensAtAmount.mul(tokenToMarketing).div(tokenToSwapPlusLiq)` will be divorced from `marketingPart`.

```
uint256 marketingPart = newBalance.mul(tokenToMarketing).div(tokenToSwap);
uint256 developmentPart = newBalance.mul(tokenToDevelopment).div(tokenToSwap);
uint256 projectPart = newBalance.mul(tokenToProject).div(tokenToSwap);
uint256 ecoPart = newBalance.mul(tokenToEco).div(tokenToSwap);
uint256 partnerPart = newBalance.mul(tokenToPartner).div(tokenToSwap);
uint256 liquidityPart = newBalance.sub(marketingPart).sub(developmentPart).sub(HalfSum);

if (marketingPart > 0) {
    payable(marketingWalletAddress).transfer(marketingPart);
    marketingFeeTotal =
marketingFeeTotal.sub(swapTokensAtAmount.mul(tokenToMarketing).div(tokenToSwapPlusLiq));
}

if (developmentPart > 0) {
    payable(developmentWalletAddress).transfer(developmentPart);
    developmentFeeTotal =
developmentFeeTotal.sub(swapTokensAtAmount.mul(tokenToDevelopment).div(tokenToSwapPlu
sLiq));
}

if (projectPart > 0) {
    payable(projectWalletAddress).transfer(projectPart);
    projectFeeTotal =
projectFeeTotal.sub(swapTokensAtAmount.mul(tokenToProject).div(tokenToSwapPlusLiq));
}
```

```
if (ecoPart > 0) {
    payable(ecoWalletAddress).transfer(ecoPart);
    ecoFeeTotal =
ecoFeeTotal.sub(swapTokensAtAmount.mul(tokenToEco).div(tokenToSwapPlusLiq));
}

if (partnerPart > 0) {
    payable(partnerWalletAddress).transfer(partnerPart);
    partnerFeeTotal =
partnerFeeTotal.sub(swapTokensAtAmount.mul(tokenToPartner).div(tokenToSwapPlusLiq));
}

// Add liquidity to pancakeswap
if (liquidityPart > 0) {
    addLiquidity(halfTokenToLiquidity, liquidityPart, _lpDestination);
    liquidityFeeTotal =
liquidityFeeTotal.sub(swapTokensAtAmount.mul(tokenToLiquidity).div(tokenToSwapPlusLiq));
}
```

Recommendation

The team is advised to carefully check if the implementation follows the expected business logic.

L01 - Public Function could be Declared External

Criticality	minor / informative
Location	contracts/GreenTech.sol#L810,425,134,403,418,377,188,174,469,410
Status	Unresolved

Description

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

```
sendDustBNB
setSwapAndLiquifyEnabled
updateUniswapV2Router
isExcludedFromFees
TotalSellFee
setAutomatedMarketMakerPair
excludeMultipleAccountsFromFees
excludeFromLimitAmount
setSwapTokensAmount
...
```

Recommendation

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

L04 - Conformance to Solidity Naming Conventions

Criticality	minor / informative
Location	contracts/GreenTech.sol#L410,810,418
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.

```
TotalBuyFee
_recipient
TotalSellFee
```

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	contracts/GreenTech.sol#L432,469,457,445
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.

```
maxTxAmount = amount
swapTokensAtAmount = amount
maxBuyAmount = amount
maxSaleAmount = amount
```

Recommendation

Emit an event for critical parameter changes.

L13 - Divide before Multiply Operation

Criticality	minor / informative
Location	contracts/GreenTech.sol#L480
Status	Unresolved

Description

Performing divisions before multiplications may cause lose of prediction.

```
rateLiqFee = halfTokenToLiquidity.mul(10000).div(tokenToSwapPlusLiq)
```

Recommendation

The multiplications should be prior to the divisions.

Contract Functions

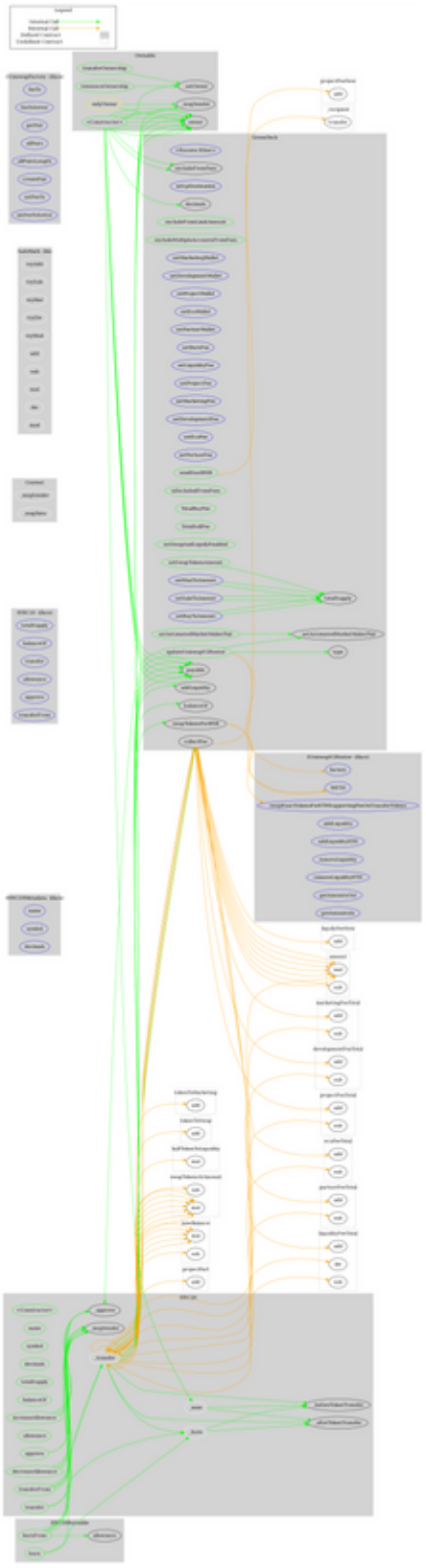
Contract	Type	Bases		
	Function Name	Visibility	Mutability	Modifiers
Ownable	Implementation	Context		
	<Constructor>	Public	✓	-
	owner	Public		-
	renounceOwnership	Public	✓	onlyOwner
	transferOwnership	Public	✓	onlyOwner
	_setOwner	Private	✓	
ERC20	Implementation	Context, IERC20, IERC20Metadata		
	<Constructor>	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	✓	
	_beforeTokenTransfer	Internal	✓	
	_afterTokenTransfer	Internal	✓	

ERC20Burnable	Implementation	Context, ERC20		
	burn	Public	✓	-
	burnFrom	Public	✓	-
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		
GreenTech	Implementation	Ownable, ERC20Burnable		
	<Constructor>	Public	✓	ERC20
	<Receive Ether>	External	Payable	-
	updateUniswapV2Router	Public	✓	onlyOwner
	setLpDestination	External	✓	onlyOwner
	excludeFromFees	Public	✓	onlyOwner
	excludeFromLimitAmount	Public	✓	onlyOwner
	excludeMultipleAccountsFromFees	Public	✓	onlyOwner
	setMarketingWallet	External	✓	onlyOwner
	setDevelopmentWallet	External	✓	onlyOwner
	setProjectWallet	External	✓	onlyOwner
	setEcoWallet	External	✓	onlyOwner
	setPartnerWallet	External	✓	onlyOwner
	setBurnFee	External	✓	onlyOwner
	setLiquidityFee	External	✓	onlyOwner
	setProjectFee	External	✓	onlyOwner
	setMarketingFee	External	✓	onlyOwner
	setDevelopmentFee	External	✓	onlyOwner
	setEcoFee	External	✓	onlyOwner
	setPartnerFee	External	✓	onlyOwner
	setAutomatedMarketMakerPair	Public	✓	onlyOwner
	_setAutomatedMarketMakerPair	Private	✓	
	isExcludedFromFees	Public		-
	TotalBuyFee	Public		-
	TotalSellFee	Public		-
	setSwapAndLiquifyEnabled	Public	✓	onlyOwner
	setMaxTxAmount	External	✓	onlyOwner
	setSaleTxAmount	External	✓	onlyOwner
	setBuyTxAmount	External	✓	onlyOwner
	setSwapTokensAmount	Public	✓	onlyOwner

	_transfer	Internal	✓	
	collectFee	Private	✓	
	swapTokensForBNB	Private	✓	
	addLiquidity	Internal	✓	
	sendDustBNB	Public	✓	onlyOwner
IUniswapFactory	Interface			
	feeTo	External		-
	feeToSetter	External		-
	getPair	External		-
	allPairs	External		-
	allPairsLength	External		-
	createPair	External	✓	-
	setFeeTo	External	✓	-
	setFeeToSetter	External	✓	-
IUniswapV2Router	Interface			
	factory	External		-
	WETH	External		-
	addLiquidity	External	✓	-
	addLiquidityETH	External	Payable	-
	removeLiquidity	External	✓	-
	removeLiquidityETH	External	✓	-
	getAmountsOut	External		-
	getAmountsIn	External		-
	swapExactTokensForETHSupportingFeeOnTransferTokens	External	✓	-

Contract Flow



Summary

There are some functions that can be abused by the owner like transferring tokens to the team’s wallet and manipulating 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