Cyberscope

Audit Report
Nutgain

March 2022

Type	BEP20
Network	BSC
Address	0x40a3e5F7dF89cDE44ef7E91dC47a4c5345c32A9b
Audited by	© cyberscope

Table of Contents

Contract Review

Contract Name	NUTGAIN
Compiler Version	v0.8.7+commit.e28d00a7
Optimization	200 runs
Licence	Unlicense
Explorer	https://bscscan.com/token/0x40a3e5F7dF89cDE44ef7E91dC47a4c5345c32A9b
Symbol	NUTGV2
Decimals	9
Total Supply	1,500,000,000
Source	contract.sol
Domain	nutgain.io

Audit Updates

Initial Audit	12th 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

ST - Stop Transactions

Criticality	critical
Location	contract.sol#L618,623,640,492

Description

The contract owner has the authority to stop transactions for all users excluding the owner. The owner may take advantage of it by setting the tradingEnabled to false or the `maxBuyLimit`, `maxWalletLimit` or `_maxTxAmount` to zero.

```
if (!_isExcludedFromFee[from] && !_isExcludedFromFee[to]) {
    require(tradingEnabled, "Trading not active");
}
```

```
require(amount <= maxBuyLimit, "You are exceeding maxBuyLimit");
require(
    balanceOf(to) + amount <= maxWalletLimit,
    "You are exceeding maxWalletLimit"
);
```

The contract owner has the authority to stop the sales for all users excluding the owner. This will cause the contract to operate like a honeypot. The owner may take advantage of it by setting `coolDownTime` or `sellTaxes` to a high value

```
if (coolDownEnabled) {
    uint256 timePassed = block.timestamp - _lastSell[from];
    require(timePassed >= coolDownTime, "Cooldown enabled");
    _lastSell[from] = block.timestamp;
}
```

```
Taxes memory temp;
if (isSell && !useLaunchTax) temp = sellTaxes;
else if (!useLaunchTax) temp = taxes;
else temp = launchtax;
```

Recommendation

The contract could embody a check for not allowing setting the variables less or more 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.

ELFM - Exceed Limit Fees Manipulation

Criticality	critical
Location	contract.sol#L396

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 `setSellTaxes` function with a high percentage value.

```
function setSellTaxes(
    uint256 _rfi,
    uint256 _marketing,
    uint256 _liquidity,
    uint256 _dev,
    uint256 _utility,
    uint256 _burn
) public onlyOwner {
    sellTaxes = Taxes(_rfi, _marketing, _liquidity, _dev, _utility, _burn);
    emit FeesChanged();
}
```

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.

BC - Blacklisted Contracts

Criticality	critical
Location	contract.sol#L616

Description

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

```
require(!_isBlacklisted[from] && !_isBlacklisted[to], "You are a bot");
```

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
●	L01	Public Function could be Declared External
●	L02	State Variables could be Declared Constant
●	L04	Conformance to Solidity Naming Conventions
●	L11	Unnecessary Boolean equality
●	L07	Missing Events Arithmetic
●	L13	Divide before Multiply Operation

L01 - Public Function could be Declared External

Criticality	minor
Location	contract.sol#L55,59,241,245,254,263,267,272,286,291 and 9 more

Description

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

```
rescueAnyBEP20Tokens
setSellTaxes
setTaxes
isExcludedFromFee
includeInFee
excludeFromFee
reflectionFromToken
isExcludedFromReward
transfer
...
```

Recommendation

Use the external attribute for functions never called from the contract

L02 - State Variables could be Declared Constant

Criticality	minor
Location	contract.sol#L142,153

Description

Constant state variables should be declared constant to save gas.

```
deadWallet
_tTotal
```

Recommendation

Add the constant attribute to state variables that never change.

L04 - Conformance to Solidity Naming Conventions

Criticality	minor
Location	contract.sol#L78,185,328,385,386,387,388,389,390,397 and 13 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.

```
_symbol
_name
genesis_block
_decimals
_amount
_to
_tokenAddr
_enabled
_burn
...
```

Recommendation

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

L11 - Unnecessary Boolean equality

Criticality	minor
Location	contract.sol#L326

Description

The comparison to boolean constants is redundant. Boolean constants can be used directly and do not need to be compared to true or false.

```
state == true
```

Recommendation

Remove the equality to the boolean constant.

L07 - Missing Events Arithmetic

Criticality	minor
Location	contract.sol#L326,799,804,832,837

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.

```
maxWalletLimit = amount * 10 ** decimals()
maxBuyLimit = maxBuy * 10 ** decimals()
swapTokensAtAmount = amount * 10 ** _decimals
coolDownTime = time * 1
deadline = _deadline
```

Recommendation

Emit an event for critical parameter changes.

L13 - Divide before Multiply Operation

Criticality	minor
Location	contract.sol#L712

Description

Performing divisions before multiplications may cause lose of prediction.

```
unitBalance = deltaBalance / (denominator - temp.liquidity)
```

Recommendation

The multiplications should be prior to the divisions.

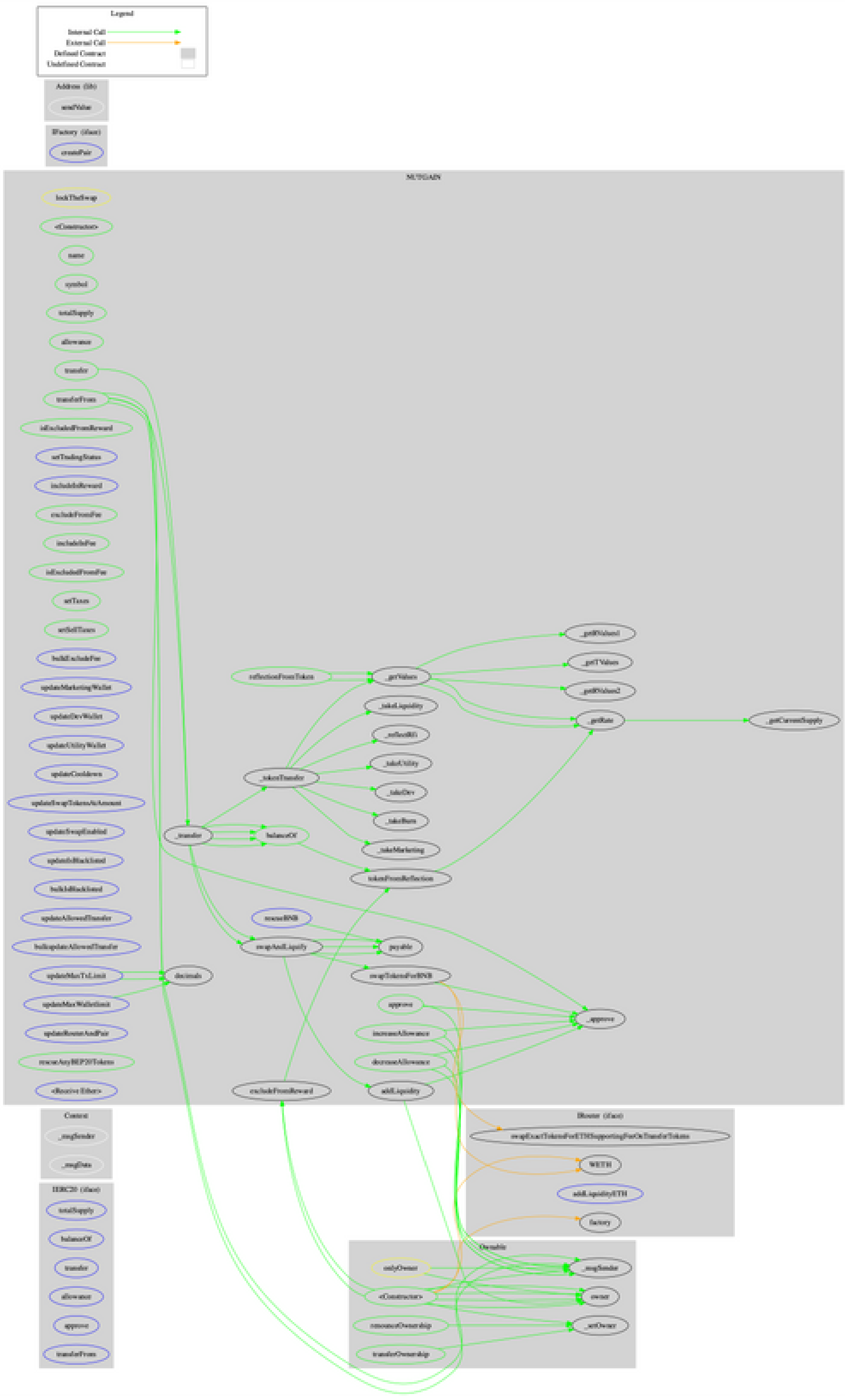
Contract Functions

Contract	Type	Bases		
	Function Name	**Visibility**	**Mutability**	**Modifiers**
IERC20	Interface			
	totalSupply	External		-
	balanceOf	External		-
	transfer	External	✓	-
	allowance	External		-
	approve	External	✓	-
	transferFrom	External	✓	-
Context	Implementation			
	_msgSender	Internal		
	_msgData	Internal		
Ownable	Implementation	Context		
	<Constructor>	Public	✓	-
	owner	Public		-
	renounceOwnership	Public	✓	onlyOwner
	transferOwnership	Public	✓	onlyOwner
	_setOwner	Private	✓	
IFactory	Interface			
	createPair	External	✓	-
IRouter	Interface			
	factory	External		-
	WETH	External		-
	addLiquidityETH	External	Payable	-
	swapExactTokensForETHSupportingFeeOnTransferTokens	External	✓	-

Address	Library			
	sendValue	Internal	✓	
NUTGAIN	Implementation	Context, IERC20, Ownable		
	<Constructor>	Public	✓	-
	name	Public		-
	symbol	Public		-
	decimals	Public		-
	totalSupply	Public		-
	balanceOf	Public		-
	allowance	Public		-
	approve	Public	✓	-
	transferFrom	Public	✓	-
	increaseAllowance	Public	✓	-
	decreaseAllowance	Public	✓	-
	transfer	Public	✓	-
	isExcludedFromReward	Public		-
	reflectionFromToken	Public		-
	setTradingStatus	External	✓	onlyOwner
	tokenFromReflection	Public		-
	excludeFromReward	Public	✓	onlyOwner
	includeInReward	External	✓	onlyOwner
	excludeFromFee	Public	✓	onlyOwner
	includeInFee	Public	✓	onlyOwner
	isExcludedFromFee	Public		-
	setTaxes	Public	✓	onlyOwner
	setSellTaxes	Public	✓	onlyOwner
	_reflectRfi	Private	✓	
	_takeLiquidity	Private	✓	
	_takeMarketing	Private	✓	
	_takeBurn	Private	✓	
	_takeDev	Private	✓	
	_takeUtility	Private	✓	
	_getValues	Private		

	_getTValues	Private		
	_getRValues1	Private		
	_getRValues2	Private		
	_getRate	Private		
	_getCurrentSupply	Private		
	_approve	Private	✓	
	_transfer	Private	✓	
	_tokenTransfer	Private	✓	
	swapAndLiquify	Private	✓	lockTheSwap
	addLiquidity	Private	✓	
	swapTokensForBNB	Private	✓	
	bulkExcludeFee	External	✓	onlyOwner
	updateMarketingWallet	External	✓	onlyOwner
	updateDevWallet	External	✓	onlyOwner
	updateUtilityWallet	External	✓	onlyOwner
	updateCooldown	External	✓	onlyOwner
	updateSwapTokensAtAmount	External	✓	onlyOwner
	updateSwapEnabled	External	✓	onlyOwner
	updateIsBlacklisted	External	✓	onlyOwner
	bulkIsBlacklisted	External	✓	onlyOwner
	updateAllowedTransfer	External	✓	onlyOwner
	bulkupdateAllowedTransfer	External	✓	onlyOwner
	updateMaxTxLimit	External	✓	onlyOwner
	updateMaxWalletlimit	External	✓	onlyOwner
	updateRouterAndPair	External	✓	onlyOwner
	rescueBNB	External	✓	onlyOwner
	rescueAnyBEP20Tokens	Public	✓	onlyOwner
	<Receive Ether>	External	Payable	-

Contract Flow



Domain Info

Domain Name	nutgain.io
Registry Domain ID	fab7836b511f4e12828701bb1b324ae5-DONUTS
Creation Date	2021-08-31T17:15:47Z
Updated Date	2022-01-28T10:29:03Z
Registry Expiry Date	2023-08-31T17:15:47Z
Registrar WHOIS Server	http://whois.cloudflare.com
Registrar URL	http://cloudflare.com
Registrar	Cloudflare, Inc
Registrar IANA ID	1910

The domain has been created 6 months before the creation of the audit. It will expire in over 1 year.

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 manipulating fees, blacklisting wallets and stopping transactions. The contract can be converted into a honeypot and prevent users from selling if the owner abuses the admin functions. 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