Audit Report

Metagalaxy

January 2022

Type	BEP20
Network	BSC
Address	0xD2477CA77c14C4D2335b2b2bA9d9dd0558Cc7ee2
Audited by	© coinscope

Table of Contents

Contract Review

Contract Name	MGXY
Compiler Version	v0.8.6+commit.11564f7e
Optimization	200 runs
Licence	MIT
Explorer	https://bscscan.com/token/0xD2477CA77c14C4D2335b2b2bA9d9dd0558Cc7ee2
Symbol	MGXY
Decimals	9
Total Supply	10,000,000,000
Source	contract.sol
Domain	mgxy.io

Audit Updates

Initial Audit	5th January 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	medium
Location	contract.sol#L364

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 `maxSellAmountPerCycle` to zero.

```
if(!_isExcludedFromFees[from] && !_isExcludedFromFees[to] && !swapping &&
!automatedMarketMakerPairs[from]){
    bool newCycle = block.timestamp - userLastSell[from].firstSellTime >=
antiDumpCycle;
    if(!newCycle){
        require(userLastSell[from].amountSoldInCycle + amount <=
maxSellAmountPerCycle, "You are exceeding maxSellAmountPerCycle");
        userLastSell[from].amountSoldInCycle += amount;
    }
    else{
        require(amount <= maxSellAmountPerCycle, "You are exceeding
maxSellAmountPerCycle");
        userLastSell[from].amountSoldInCycle = amount;
        userLastSell[from].firstSellTime = block.timestamp;
    }
}
```

Recommendation

The contract could embody a check for not allowing setting the `maxSellAmountPerCycle` less 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	https://bscscan.com/address/0x8983a6f5b70315f9373d39e14de5afeabf835588#code#L209,L213

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 `setBuyTaxes` function with a high percentage value.

```
function setBuyTaxes(uint256 _rewards, uint256 _marketing, uint256 _liquidity,
uint256 _dev) external onlyOwner{
    buyTaxes = Taxes(_rewards, _marketing, _liquidity, _dev);
}
```

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#L234,L239

Description

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

```
function setBulkBot(address[] memory bots, bool value) external onlyOwner{
    for(uint256 i; i<bots.length; i++){
        _isBot[bots[i]] = value;
    }
}
```

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
	L05	Unused State Variable
	L04	Conformance to Solidity Naming Conventions
	L09	Dead Code Elimination
	L11	Unnecessary Boolean equality
	L07	Missing Events Arithmetic

L01 - Public Function could be Declared External

Criticality	minor
Location	DividendPayingToken.sol#L52,L43,L688 and 23 more

Description

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

```
transferOwnership
renounceOwnership
process
...
```

Recommendation

Use the external attribute for functions never called from the contract

L02 - State Variables could be Declared Constant

Criticality	minor
Location	MetaGalaxy.sol#L75

Description

Constant state variables should be declared constant to save gas.

```
antiBotBlocks
```

Recommendation

Add the constant attribute to state variables that never change.

L05 - Unused State Variable

Criticality	minor
Location	SafeMath.sol#L154

Description

There are segments that contains unused state variable.

```
MAX_INT256
```

Recommendation

Remove unused state variables.

L04 - Conformance to Solidity Naming Conventions

Criticality	minor
Location	DividendPayingToken.sol#L597,L74,L35 and 17 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.

```
_account
_isBot
BUSD
...
```

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	Context.sol#L159,L171,L200 and 6 more

Description

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

```
mul
div
abs
...
```

Recommendation

Remove unused functions.

L11 - Unnecessary Boolean equality

Criticality	minor
Location	MetaGalaxy.sol#L567

Description

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

```
value == true
```

Recommendation

Remove the equality to the boolean constant.

L07 - Missing Events Arithmetic

Criticality	minor
Location	MetaGalaxy.sol#L338,L205

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.

```
antiDumpCycle = timeInMinutes * 60
swapTokensAtAmount = amount * 10 ** 9
```

Recommendation

Emit an event for critical parameter changes.

Contract Functions

Contract	Type	Bases		
	Function Name	**Visibility**	**Mutability**	**Modifiers**
Context	Implementation			
	_msgSender	Internal		
	_msgData	Internal		
DividendPayingToken	Implementation	ERC20, DividendPayingTokenInterface, Ownable		
	<Constructor>	Public	✓	ERC20
	distributeBUSDDividends	Public	✓	onlyOwner
	withdrawDividend	Public	✓	-
	_withdrawDividendOfUser	Internal	✓	
	dividendOf	Public		-
	withdrawableDividendOf	Public		-
	withdrawnDividendOf	Public		-
	accumulativeDividendOf	Public		-
	_transfer	Internal	✓	
	_mint	Internal	✓	
	_burn	Internal	✓	
	_setBalance	Internal	✓	
DividendPayingTokenInterface	Interface			
	dividendOf	External		-
	withdrawDividend	External	✓	-
	withdrawableDividendOf	External		-
	withdrawnDividendOf	External		-
	accumulativeDividendOf	External		-

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	✓	
IPair	Interface			
	sync	External	✓	-
IFactory	Interface			
	createPair	External	✓	-
	getPair	External		-
IRouter	Interface			
	factory	External		-
	WETH	External		-
	addLiquidityETH	External	Payable	-
	swapExactTokensForTokensSupportingFeeOnTransferTokens	External	✓	-
	swapExactETHForTokens	External	Payable	-

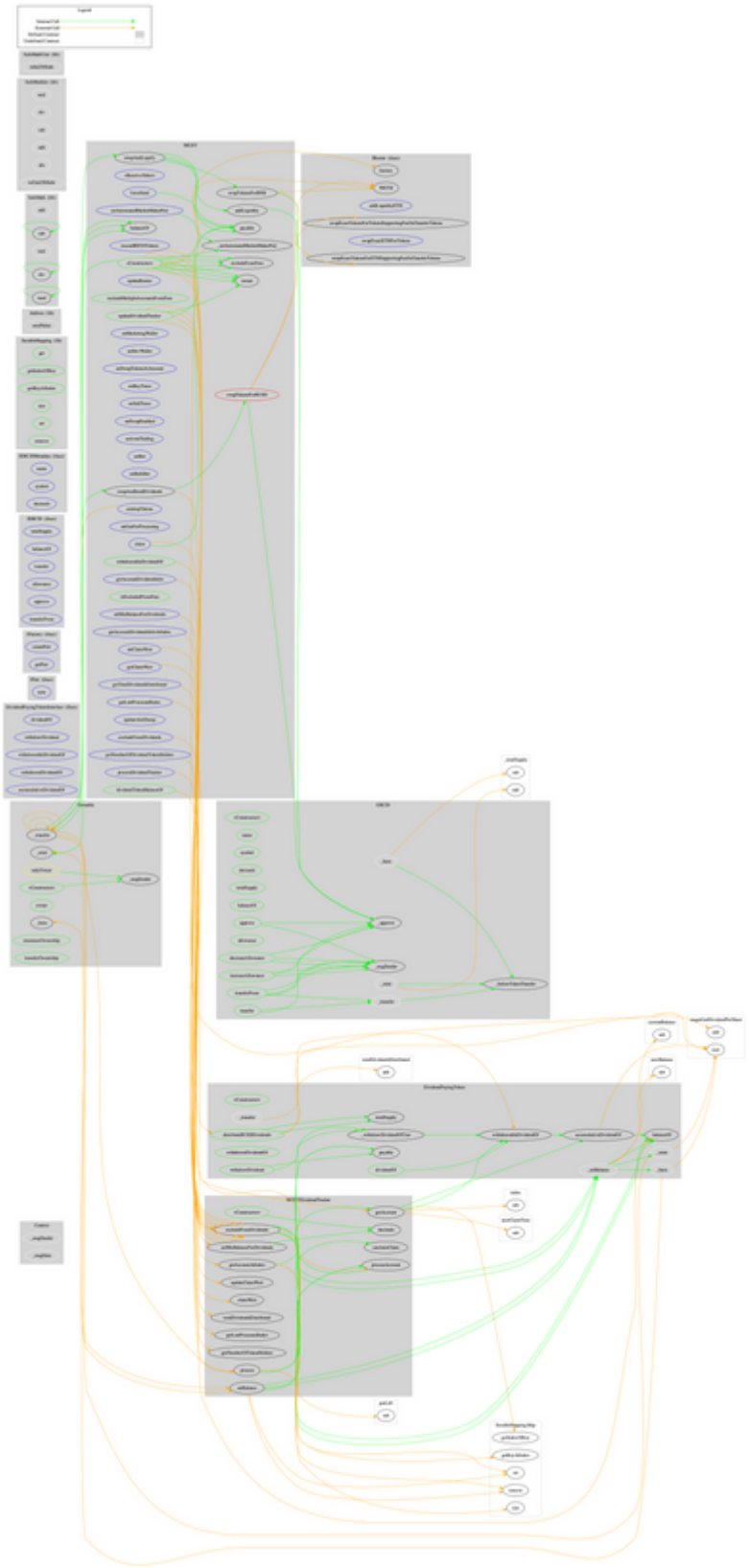
	swapExactTokensForETHSupportingFeeOnTransferTokens	External	✓	-
IERC20	Interface			
	totalSupply	External		-
	balanceOf	External		-
	transfer	External	✓	-
	allowance	External		-
	approve	External	✓	-
	transferFrom	External	✓	-
IERC20Metadata	Interface	IERC20		
	name	External		-
	symbol	External		-
	decimals	External		-
IterableMapping	Library			
	get	Public		-
	getIndexOfKey	Public		-
	getKeyAtIndex	Public		-
	size	Public		-
	set	Public	✓	-
	remove	Public	✓	-
Address	Library			
	sendValue	Internal	✓	
MGXY	Implementation	ERC20, Ownable		
	<Constructor>	Public	✓	ERC20
	<Receive Ether>	External	Payable	-
	updateDividendTracker	Public	✓	onlyOwner
	processDividendTracker	External	✓	-
	claim	External	✓	-
	rescueBEP20Tokens	External	✓	onlyOwner

	forceSend	External	✓	-
	updateRouter	External	✓	onlyOwner
	excludeFromFees	Public	✓	onlyOwner
	excludeMultipleAccountsFromFees	Public	✓	onlyOwner
	excludeFromDividends	External	✓	onlyOwner
	setMarketingWallet	External	✓	onlyOwner
	setDevWallet	External	✓	onlyOwner
	setSwapTokensAtAmount	External	✓	onlyOwner
	setBuyTaxes	External	✓	onlyOwner
	setSellTaxes	External	✓	onlyOwner
	setSwapEnabled	External	✓	onlyOwner
	activateTrading	External	✓	onlyOwner
	setBot	External	✓	onlyOwner
	setBulkBot	External	✓	onlyOwner
	setAutomatedMarketMakerPair	External	✓	onlyOwner
	setMinBalanceForDividends	External	✓	onlyOwner
	_setAutomatedMarketMakerPair	Private	✓	
	setGasForProcessing	External	✓	onlyOwner
	setClaimWait	External	✓	onlyOwner
	getClaimWait	External		-
	getTotalDividendsDistributed	External		-
	isExcludedFromFees	Public		-
	withdrawableDividendOf	Public		-
	dividendTokenBalanceOf	Public		-
	getAccountDividendsInfo	External		-
	getAccountDividendsInfoAtIndex	External		-
	getLastProcessedIndex	External		-
	getNumberOfDividendTokenHolders	External		-
	updateAntiDump	External	✓	onlyOwner
	airdropTokens	External	✓	onlyOwner
	_transfer	Internal	✓	
	swapAndLiquify	Private	✓	
	swapTokensForBUSD	Private	✓	
	swapAndSendDividends	Private	✓	
	swapTokensForBNB	Private	✓	

	addLiquidity	Private	✓	
MGXYDividend Tracker	Implementation	Ownable, DividendPayingToken		
	<Constructor>	Public	✓	DividendPayingToken
	_transfer	Internal		
	setMinBalanceForDividends	External	✓	onlyOwner
	excludeFromDividends	External	✓	onlyOwner
	updateClaimWait	External	✓	onlyOwner
	getLastProcessedIndex	External		-
	getNumberOfTokenHolders	External		-
	getAccount	Public		-
	getAccountAtIndex	Public		-
	canAutoClaim	Private		
	setBalance	Public	✓	onlyOwner
	process	Public	✓	-
	processAccount	Public	✓	onlyOwner
Ownable	Implementation	Context		
	<Constructor>	Public	✓	-
	owner	Public		-
	renounceOwnership	Public	✓	onlyOwner
	transferOwnership	Public	✓	onlyOwner
SafeMath	Library			
	add	Internal		
	sub	Internal		
	sub	Internal		
	mul	Internal		
	div	Internal		
	div	Internal		
	mod	Internal		
	mod	Internal		

SafeMathInt	Library			
	mul	Internal		
	div	Internal		
	sub	Internal		
	add	Internal		
	abs	Internal		
	toUint256Safe	Internal		
SafeMathUint	Library			
	toInt256Safe	Internal		

Contract Flow



Domain Info

Domain Name	mgxy.io
Registry Domain ID	ee49702e67d447899f12f416287513bc-DONUTS
Creation Date	2021-12-06T23:46:14Z
Updated Date	2021-12-11T23:46:51Z
Registry Expiry Date	2022-12-06T23:46:14Z
Registrar WHOIS Server	whois.godaddy.com/
Registrar URL	http://www.godaddy.com/domains/search.aspx?ci=8990
Registrar	GoDaddy.com, LLC
Registrar IANA ID	146

The domain has been created 29 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

Metagalaxy is aiming to create an open world metaverse. The token has a friendly and growing community. The contract analysis reported two critical and one medium threat issues. There are some functions that can be abused by the owner, like manipulating fees, blacklisting contracts and indirectly stopping the transactions. 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.

Coinscope 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 Coinscope 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 Coinscope 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 Coinscope team disclaims any liability for the resulting losses.

About Coinscope

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.

Coinscope is aiming to make crypto discoverable and efficient globally. It provides all the essential tools to assist users draw their own conclusions.

The Coinscope.co team

https://www.coinscope.co