COINSCOPE

Audit Report

Redlight

January 2022

Github https://github.com/Redlight-Node-District/Token-Contract

Audited by © coinscope

Table of Contents

Contract Review

The contract audit will review the files that are included in the github repository

Github	https://github.com/Redlight-Node-District/Token-Contract
Commit	b4991b8da87369cf4e0d23482019dfc1e09f219f

The audit review is based on the following files

File	**SHA256**
Playmate Final.sol	bb84d9463962768004ae8cc4bde617e606db2cb4bb09120b9c7c0742148f4c4b

Audit Updates

Initial Audit	26th 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	critical
Location	Playmate Final.sol#L551,L621

Description

The contract owner has the authority to stop the sales from all users excluding the owner.

Firstly, the owner may take advantage of it by setting a high value to `snipeBlockAmt`. Then all the users that have bought once, they will not be able to sell except if the owner manually excludes them from the `_isSniper` list.

```
if (block.number - _liqAddBlock < snipeBlockAmt) {
    _isSniper[to] = true;
```

Secondly, the owner may take advantage of it by setting a high value to `vbuy` variables and setting the `MANSION` variable with the contract address.

```
} else if (to == lpPair) {
    currentFee = _taxRates.sellFee + getWhaleFee(from);
}
```

Recommendation

The contract could embody a check for not allowing arbitrary setting the vbuy. The contract could also check for not allowing setting the `snipeBlockAmt` more than a reasonable period.

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	Playmate Final.sol#L596

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 `setvbuy` function with a high percentage value and setting the `MANSION` variable to the contract's address.

```
function setvbuy(uint256 _vbuy1, uint256 _vbuy2, uint256 _vbuy3, uint256 _vbuy4)
external onlyOwner {
    vbuy1 = _vbuy1;
    vbuy2 = _vbuy2;
    vbuy3 = _vbuy3;
    vbuy4 = _vbuy4;
}

function getWhaleFee(address from) public view returns (uint256) {
    if(MANSION.balanceOf(from) >= 1 &&
        MANSION.balanceOf(from) < 20 ){return vbuy1;}
    if(MANSION.balanceOf(from) >= 20 &&
        MANSION.balanceOf(from) < 50 ){return vbuy2;}
    if(MANSION.balanceOf(from) >= 50 &&
        MANSION.balanceOf(from) < 100 ){return vbuy3;}
    if(MANSION.balanceOf(from) >= 100) {return vbuy4;}
    else{
        return 0;
    }

}
```

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	Playmate Final.sol#L537

Description

The contract owner has the authority to stop contracts from transactions. The owner may take advantage of it by calling the `setStartingProtections` function with a high number.

```
if (isSniper(from) || isSniper(to)) {
    revert("Sniper rejected.");
}
```

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	contract.sol#L494,L490,L455 and 7 more

Description

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

```
getMaxWallet
getMaxTX
setNewRouter
...
```

Recommendation

Use the external attribute for functions never called from the contract

L02 - State Variables could be Declared Constant

Criticality	minor
Location	contract.sol#L246,L160,L227 and 4 more

Description

Constant state variables should be declared constant to save gas.

```
whaleFee
startingSupply
rewardsPool
...
```

Recommendation

Add the constant attribute to state variables that never change.

L05 - Unused State Variable

Criticality	minor
Location	contract.sol#L246,L237

Description

There are segments that contains unused state variable.

```
whaleFee
init
```

Recommendation

Remove unused state variables.

L04 - Conformance to Solidity Naming Conventions

Criticality	minor
Location	contract.sol#L248,L240,L224 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.

```
MANSION
_hasLiqBeenAdded
ZERO
...
```

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#L7,L11

Description

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

```
_msgSender
_msgData
```

Recommendation

Remove unused functions.

L11 - Unnecessary Boolean equality

Criticality	minor
Location	contract.sol#L468

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.

```
enabled == false
```

Recommendation

Remove the equality to the boolean constant.

L07 - Missing Events Arithmetic

Criticality	minor
Location	contract.sol#L596,L485,L480 and 2 more

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.

```
vbuy1 = _vbuy1
_maxWalletSize = (_tTotal * percent) / divisor
_maxTxAmount = (_tTotal * percent) / divisor
...
```

Recommendation

Emit an event for critical parameter changes.

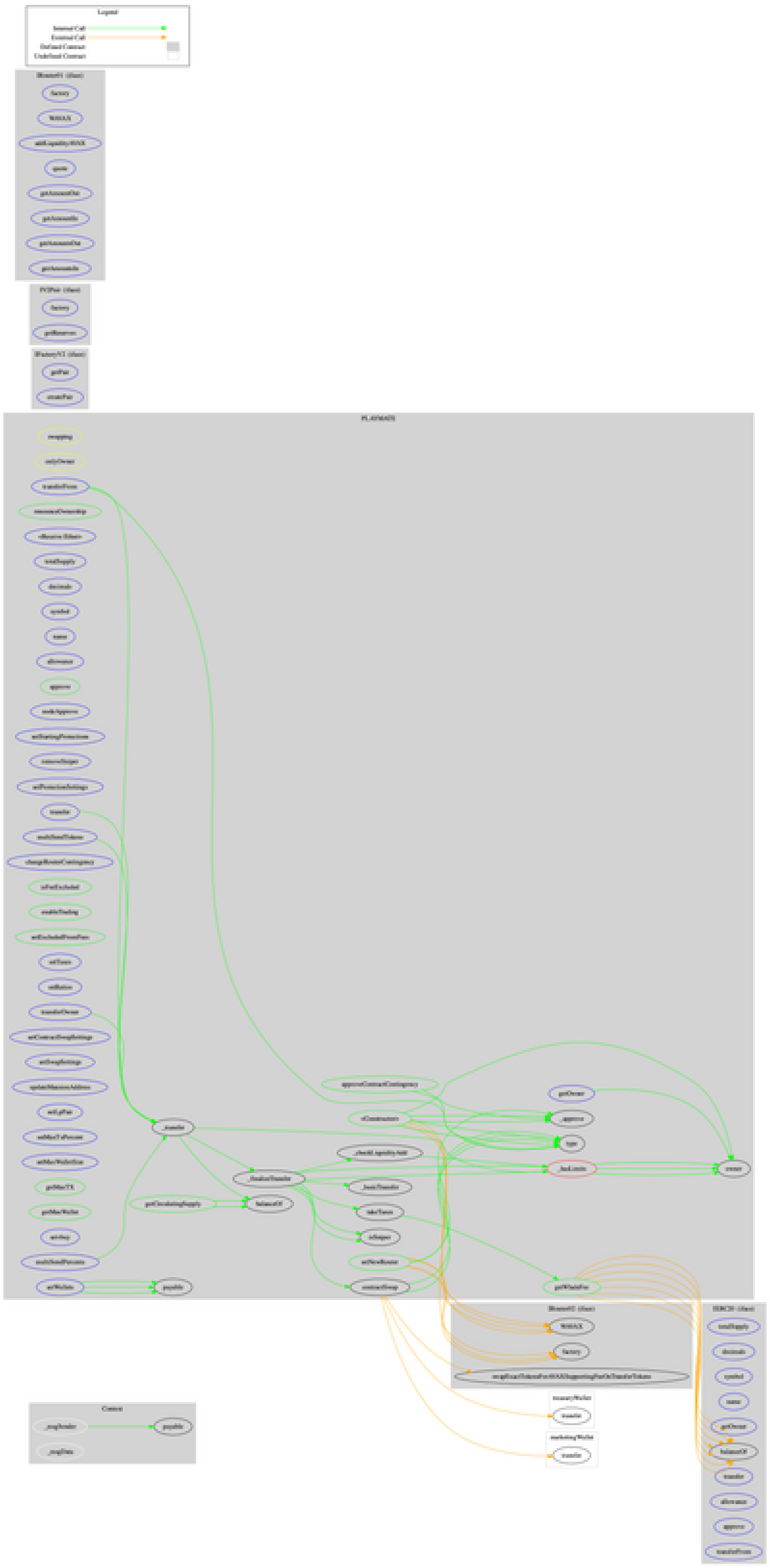
Contract Functions

Contract	Type	Bases		
	Function Name	**Visibility**	**Mutability**	**Modifiers**
Context	Implementation			
	_msgSender	Internal		
	_msgData	Internal		
IERC20	Interface			
	totalSupply	External		-
	decimals	External		-
	symbol	External		-
	name	External		-
	getOwner	External		-
	balanceOf	External		-
	transfer	External	✓	-
	allowance	External		-
	approve	External	✓	-
	transferFrom	External	✓	-
IFactoryV2	Interface			
	getPair	External		-
	createPair	External	✓	-
IV2Pair	Interface			
	factory	External		-
	getReserves	External		-
IRouter01	Interface			
	factory	External		-
	WAVAX	External		-
	addLiquidityAVAX	External	Payable	-
	quote	External		-

	getAmountOut	External		-
	getAmountIn	External		-
	getAmountsOut	External		-
	getAmountsIn	External		-
IRouter02	Interface	IRouter01		
	swapExactTokensForAVAXSupportingFeeOnTransferTokens	External	✓	-
PLAYMATE	Implementation	IERC20		
	<Constructor>	Public	✓	-
	owner	Public		-
	transferOwner	External	✓	onlyOwner
	renounceOwnership	Public	✓	onlyOwner
	<Receive Ether>	External	Payable	-
	totalSupply	External		-
	decimals	External		-
	symbol	External		-
	name	External		-
	getOwner	External		-
	balanceOf	Public		-
	allowance	External		-
	approve	Public	✓	-
	nodeApprove	External	✓	-
	_approve	Private	✓	
	approveContractContingency	Public	✓	onlyOwner
	setStartingProtections	External	✓	onlyOwner
	isSniper	Public		-
	removeSniper	External	✓	onlyOwner
	setProtectionSettings	External	✓	onlyOwner
	transfer	External	✓	-
	transferFrom	External	✓	-
	changeRouterContingency	External	✓	onlyOwner
	isFeeExcluded	Public		-
	enableTrading	Public	✓	onlyOwner
	setExcludedFromFees	Public	✓	onlyOwner

	setTaxes	External	✓	onlyOwner
	setRatios	External	✓	onlyOwner
	setWallets	External	✓	onlyOwner
	setContractSwapSettings	External	✓	onlyOwner
	setSwapSettings	External	✓	onlyOwner
	getCirculatingSupply	Public		-
	updateMansionAddress	External	✓	onlyOwner
	setNewRouter	Public	✓	onlyOwner
	setLpPair	External	✓	onlyOwner
	setMaxTxPercent	External	✓	onlyOwner
	setMaxWalletSize	External	✓	onlyOwner
	getMaxTX	Public		-
	getMaxWallet	Public		-
	_hasLimits	Private		
	_transfer	Internal	✓	
	_finalizeTransfer	Internal	✓	
	_basicTransfer	Internal	✓	
	setvbuy	External	✓	onlyOwner
	getWhaleFee	Public		-
	takeTaxes	Internal	✓	
	contractSwap	Internal	✓	swapping
	_checkLiquidityAdd	Private	✓	
	multiSendTokens	External	✓	-
	multiSendPercents	External	✓	-

Contract Flow



Domain Info

Domain Name	redlight.finance
Registry Domain ID	2ea0de243d0b4adf822de9e023ba24f3-DONUTS
Creation Date	2022-01-06T15:50:10Z
Updated Date	2022-01-11T15:50:45Z
Registry Expiry Date	2023-01-06T15:50:10Z
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 20 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 manipulating fees, blacklisting addresses and stopping transactions. The contract can potentially operate as a honeypot if the contract owner misuse some variables. 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