Cyberscope

Audit Report

Opsya

March 2022

Type	ERC20
Network	AVAX
Address	0x8DC4D5F5d7caA96B93f7095FA0c7a2Aa8264816d
Audited by	© cyberscope

Table of Contents

Contract Review

Contract Name	ReflectionERC20
Compiler Version	v0.8.4+commit.c7e474f2
Optimization	99999 runs
Licence	None
Explorer	https://snowtrace.io/address/0x8DC4D5F5d7caA96B93f7095FA0c7a2Aa8264816d
Symbol	OPSY
Decimals	8
Total Supply	100,000,000
Source	@openzeppelin/contracts/access/Ownable.sol, @openzeppelin/contracts/token/ERC20/ERC20.sol, @openzeppelin/contracts/token/ERC20/extensions/IERC20Metadata.sol, @openzeppelin/contracts/token/ERC20/IERC20.sol, @openzeppelin/contracts/utils/Context.sol, @openzeppelin/contracts/utils/math/SafeMath.sol, contracts/data/ShareHolder.sol, contracts/data/Tax.sol, contracts/interfaces/IFactory.sol, contracts/interfaces/IHODLRewardDistributor.sol, contracts/interfaces/IReflectionERC20.sol, contracts/interfaces/IRouter.sol, contracts/ReflectionERC20.sol, contracts/SwapHandler.sol
Domain	

Audit Updates

Initial Audit	18th 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	medium
Location	contract.sol#L339

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 `maxTx` to zero.

```
require(whitlisted[from_].maxTx || amount_ <= maxTx, "ReflectionERC20: > maxTX");
```

Recommendation

The contract could embody a check for not allowing setting the maxTx 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	minor
Location	contract.sol#L278

Description

The contract owner has the authority to increase the transfer fees over the allowed limit of 25%. The owner may take advantage of it by calling the `setTransferTax` function with a high percentage value.

```
function setTransferTax(
    uint256 team_,
    uint256 holder_,
    uint256 treasury_,
    uint256 charity_
) external onlyOwner {
    transferTax = Tax(
        team_, holder_, treasury_, charity_
    );
}
```

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

Severity	Code	Description
	FSA	Fixed Swap Address
	CR	Code Repetition
	L01	Public Function could be Declared External
	L04	Conformance to Solidity Naming Conventions
	L07	Missing Events Arithmetic

FSA - Fixed Swap Address

Criticality	minor
Location	contract.sol#L94

Description

The swap address is assigned once in the constructor and it can not be changed. The decentralized swaps sometimes create a new swap version or abandon the current. A contract that cannot change the swap address may not be able to catch-up the upgrade.

```
wavaxPair = IFactory(
    IRouter(swapRouter_).factory()
).createPair(wavax_, address(this));
```

Recommendation

It could be better to allow the swap address mutation in case of future swap updates.

CR - Code Repetition

Criticality	minor
Location	contract.sol#L265

Description

There are code segments that are repetitive in the contract. Those segments increase the code size of the contract unnecessarily.

```
function setBuyerTax(
    uint256 team_,
    uint256 holder_,
    uint256 treasury_,
    uint256 charity_
) external onlyOwner {
    transferTax = Tax(
        team_, holder_, treasury_, charity_
    );
}

function setSellerTax(
    uint256 team_,
    uint256 holder_,
    uint256 treasury_,
    uint256 charity_
) external onlyOwner {
    transferTax = Tax(
        team_, holder_, treasury_, charity_
    );
}

function setTransferTax(
    uint256 team_,
    uint256 holder_,
    uint256 treasury_,
    uint256 charity_
) external onlyOwner {
    transferTax = Tax(
        team_, holder_, treasury_, charity_
    );
}
```

Recommendation

Create an internal function that contains the code segment and remove it from all the sections.

L01 - Public Function could be Declared External

Criticality	minor
Location	@openzeppelin/contracts/access/Ownable.sol#L54,62 @openzeppelin/contracts/token/ERC20/ERC20.sol#L62,70,87,94,113,150,178,197

Description

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

```
decreaseAllowance
increaseAllowance
transferFrom
transfer
totalSupply
decimals
symbol
name
transferOwnership
...
```

Recommendation

Use the external attribute for functions never called from the contract

L04 - Conformance to Solidity Naming Conventions

Criticality	minor
Location	contracts/ReflectionERC20.sol#L72,73,74,75

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.

```
_charityReserved
_treasuryReserved
_hodlReserved
_teamReserved
```

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
Location	contracts/ReflectionERC20.sol#L307

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.

```
maxTx = maxTx_
```

Recommendation

Emit an event for critical parameter changes.

L09 - Dead Code Elimination

Criticality	minor
Location	@openzeppelin/contracts/token/ERC20/ERC20.sol#L351,275

Description

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

```
_burn
_afterTokenTransfer
```

Recommendation

Remove unused functions.

Contract Functions

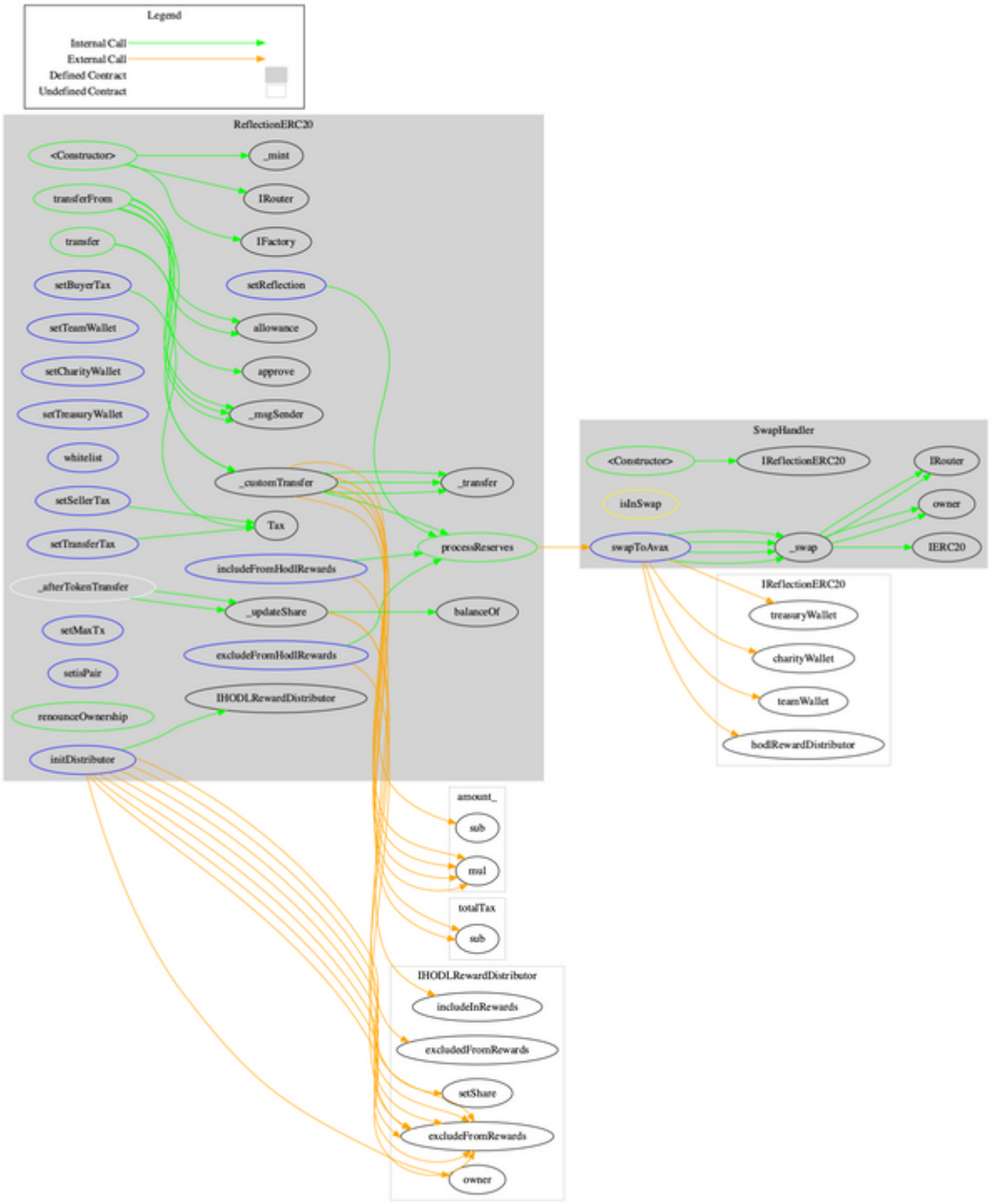
Contract	Type	Bases		
	Function Name	**Visibility**	**Mutability**	**Modifiers**
Ownable	Implementation	Context		
	<Constructor>	Public	✓	-
	owner	Public		-
	renounceOwnership	Public	✓	onlyOwner
	transferOwnership	Public	✓	onlyOwner
	_transferOwnership	Internal	✓	
ERC20	Implementation	Context, IERC20, 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	✓	

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		
IFactory	Interface			
	createPair	External	✓	-

IHODLReward Distributor	Interface			
	excludedFromRewards	External		-
	pending	External		-
	totalPending	External		-
	shareHolderInfo	External		-
	depositWavaxRewards	External	✓	-
	setShare	External	✓	-
	excludeFromRewards	External	✓	-
	includeInRewards	External	✓	-
	claimPending	External	✓	-
	owner	External	✓	-
IReflectionERC20	Interface			
	teamWallet	External	✓	-
	charityWallet	External	✓	-
	treasuryWallet	External	✓	-
	hodlRewardDistributor	External	✓	-
IRouter	Interface			
	factory	External	✓	-
	swapExactTokensForETHSupportingFeeOnTransferTokens	External	✓	-
	swapExactTokensForAVAXSupportingFeeOnTransferTokens	External	✓	-
ReflectionERC20	Implementation	ERC20, Ownable		
	<Constructor>	Public	✓	ERC20
	initDistributor	External	✓	onlyOwner
	transfer	Public	✓	-
	transferFrom	Public	✓	-
	processReserves	Public	✓	-
	setTeamWallet	External	✓	onlyOwner
	setCharityWallet	External	✓	onlyOwner
	setTreasuryWallet	External	✓	onlyOwner

	whitelist	External	✓	onlyOwner
	excludeFromHodlRewards	External	✓	onlyOwner
	includeFromHodlRewards	External	✓	onlyOwner
	setBuyerTax	External	✓	onlyOwner
	setSellerTax	External	✓	onlyOwner
	setTransferTax	External	✓	onlyOwner
	setReflection	External	✓	onlyOwner
	setMaxTx	External	✓	onlyOwner
	setisPair	External	✓	onlyOwner
	renounceOwnership	Public	✓	onlyOwner
	_customTransfer	Internal	✓	
	_afterTokenTransfer	Internal	✓	
	_updateShare	Internal	✓	
SwapHandler	Implementation	Ownable		
	<Constructor>	Public	✓	-
	swapToAvax	External	✓	isInSwap onlyOwner
	_swap	Internal	✓	

Contract Flow



Domain Info

Domain Name	opsya.org
Registry Domain ID	D402200000017863419-LROR
Creation Date	2021-09-19T16:12:16Z
Updated Date	2021-11-19T03:50:15Z
Registry Expiry Date	2022-09-19T16:12:16Z
Registrar WHOIS Server	whois.ovh.com
Registrar URL	http://www.ovh.com
Registrar	OVH
Registrar IANA ID	433

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

There is no public billing information, the creator is protected by the privacy settings.

Summary

The Smart Contract analysis reported a medium severity issue. The contract Owner has the ability to stop the transactions and manipulate the fees only for the transfers. The buy fees are fixed to 3% and the sale fees to 5%. Rather than that, the contract Owner can access some admin functions that can not be used in a malicious way to disturb the users' 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.

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