Cyberscope

Audit Report

Max ROI

October 2022

SHA256 5286a34f00c51fd43fb2087e2fff5607ea7662d5680839727f1a01c7d2563a5a

Audited by © cyberscope

Table of Contents

Contract Review

Contract Name	MaxROI
Compiler Version	v0.8.17+commit.8df45f5f
Testing Deploy	https://testnet.bscscan.com/token/0x02D4BF176a0DF8d8A338a1550E73d991E8755CA5
Symbol	mxR
Decimals	18
Total Supply	100,000,000,000
Domain	https://safeinvantage.com/safemaxroi

Audit Updates

Initial Audit	15th October 2022
Corrected	

Source Files

Filename	SHA256
@openzeppelin/contracts/access/Ownable.sol	9353af89436556f7ba8abb3f37a6677249aa4df6024fbfaa94f79ab2f44f3231
@openzeppelin/contracts/token/ERC20/ERC20.sol	5031430cc2613c32736d598037d3075985a2a09e61592a013dbd09a5bc2041b8
@openzeppelin/contracts/token/ERC20/extensions/IERC20Metadata.sol	af5c8a77965cc82c33b7ff844deb9826166689e55dc037a7f2f790d057811990
@openzeppelin/contracts/token/ERC20/IERC20.sol	94f23e4af51a18c2269b355b8c7cf4db8003d075c9c541019eb8dcf4122864d5
@openzeppelin/contracts/utils/Context.sol	1458c260d010a08e4c20a4a517882259a23a4baa0b5bd9add9fb6d6a1549814a
contracts/MaxROI.sol	5286a34f00c51fd43fb2087e2fff5607ea7662d5680839727f1a01c7d2563a5a

Contract Analysis

● Critical ● Medium ● Minor / Informative ● Pass

Severity	Code	Description	Status
●	ST	Stops Transactions	Unresolved
●	OCTD	Transfers Contract's Tokens	Passed
●	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

ST - Stops Transactions

Criticality	critical
Location	contract.sol#L202
Status	Unresolved

Description

The contract owner has the authority to stop the sales for all users excluding the owner. The owner may take advantage of it by setting the tradeVolumeRanges cap to zero. As a result, the contract may operate as a honeypot.

```
require((currTradeVolume + amount) <= (balanceOf(from) * cap) / BASIS_POINTS,
"Daily cap exceeded");
```

Recommendation

The ‘tradeVolumeRanges’ property should be configured before transfers start. The cap should not allowed to be zero. Even if the contract applies periodical trading limitations, the ‘tradeVolumeRanges’ should allow the users to transfer a reasonable amount of tokens on every trade.

ELFM - Exceeds Fees Limit

Criticality	critical
Location	contract.sol#L85
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 `reinvestPerc` function with a high percentage value.

```
function updateParams(
  uint16 _instantRelease,
  uint16 _reinvestPerc
) public onlyOwner {
  require(_reinvestPerc <= maxTax, "MAX_TAX");
  require(_instantRelease + _reinvestPerc == BASIS_POINTS, "NOT_BASIS_POINTS");

  emit InstantReleaseUpdated(instantRelease, _instantRelease);
  emit ReinvestPercUpdated(reinvestPerc, _reinvestPerc);

  instantRelease = _instantRelease;
  reinvestPerc = _reinvestPerc;
}
```

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
●	ZD	Zero Division	Unresolved
●	NCAP	Numbers Calculations Precision	Unresolved
●	NCOP	Numbers Comparison Precision	Unresolved
●	L04	Conformance to Solidity Naming Conventions	Unresolved

ZD - Zero Division

Criticality	minor / informative
Location	contract.sol#L191,195
Status	Unresolved

Description

The contract is using variables that may be set to zero as denominators. As a result, the transactions will revert.

```
uint256 currEpoch = block.timestamp / epochLength;
```

Recommendation

The contract should prevent those variables to be set to zero or should not allow to execute the corresponding statements.

NCAP - Numbers Calculations Precision

Criticality	medium
Location	contract.sol#L186
Status	Unresolved

Description

The transferred amount is divided into 2 shares. Since Solidity has not floating types, then the result of a deviation may miss the decimals precision. As a result, the splited shares will not have the exact precision and some funds may not be transferred as expected. This may cause a diversion between the total supply and the sum of the balances.

```
uint256 recipientAmount = (amount * instantRelease) / BASIS_POINTS;
if(recipientAmount > 0) {
  super._transfer(from, to, recipientAmount);
}

// transfer % to the reinvest wallet
uint256 reinvestAmount = (amount * reinvestPerc) / BASIS_POINTS;
if(reinvestAmount > 0) {
  super._transfer(from, reinvestWallet, reinvestAmount);
}
```

Recommendation

The contract could transfer the subtraction of the distributed funds in the last calculation in order to avoid the deviation rounding issue. For instance, the contract could calculate the last amount using a formula similar to:
`uint256 reinvestAmount = amount - recipientAmount`

NCOP - Numbers Comparison Precision

Criticality	medium
Location	contract.sol#L195
Status	Unresolved

Description

The ‘sellCap.lastSwapTs’ type is `uint32`, the ‘currEpoch’ type is `uint256`. The comparison between a uint32 and uint256 may produce unexpected results. For instance the expression `uint32(2^34) > uint256(2^32)` will yield a false result.

```
uint256 currTradeVolume = currEpoch > sellCap.lastSwapTs / epochLength
  ? 0
  : sellCap.tradeVolume;
...
sellCap.lastSwapTs = uint32(block.timestamp);
```

Recommendation

The contract should compare numbers of the same type. If the business logic defines that the numbers will never more than `uint32` then the variables should be normalized before the comparison.

L04 - Conformance to Solidity Naming Conventions

Criticality	minor / informative
Location	contracts/MaxROI.sol#L106,86,87,99
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.

```
_reinvestWallet
_instantRelease
_reinvestPerc
_epochLength
```

Recommendation

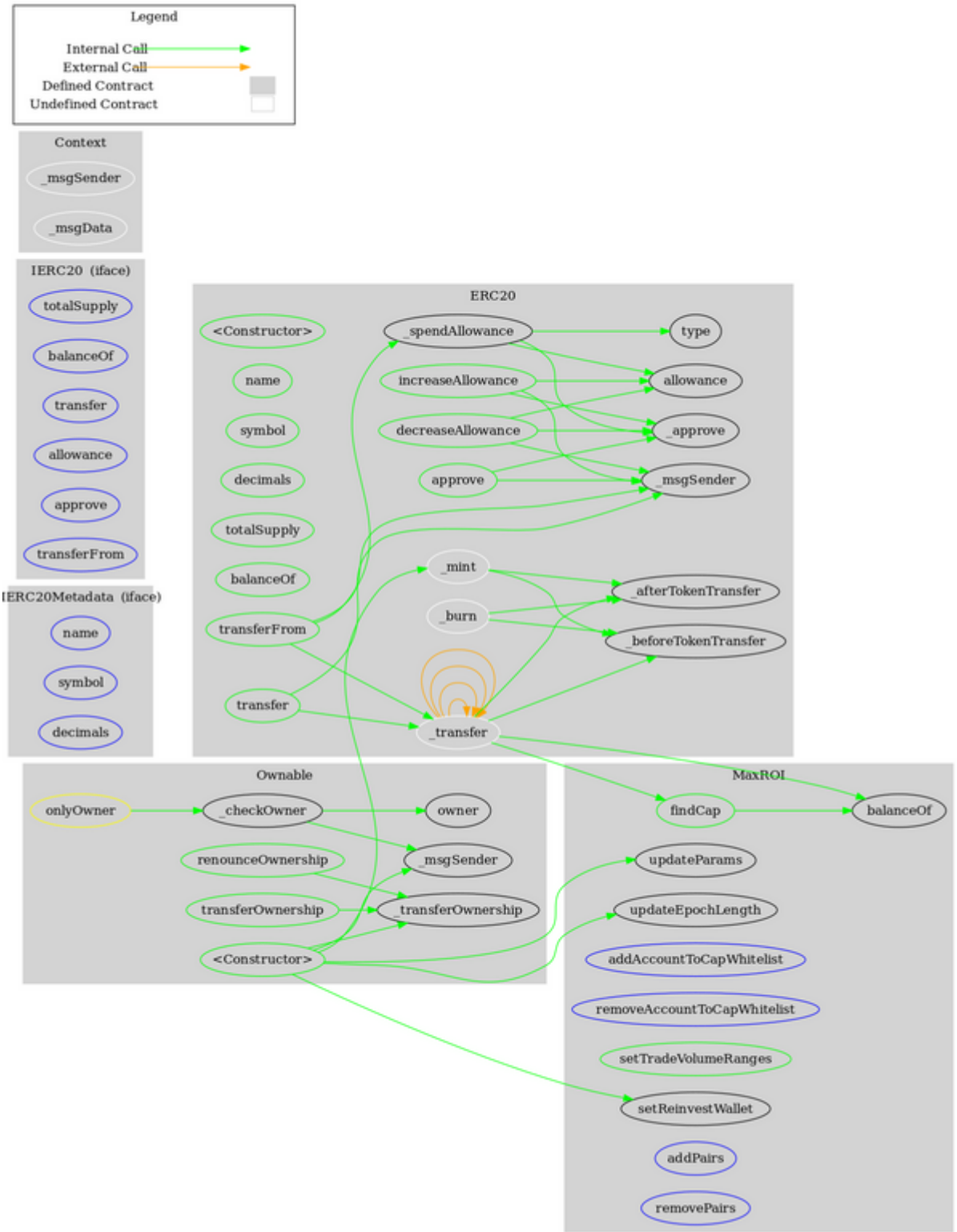
Follow the Solidity naming convention.
https://docs.soliditylang.org/en/v0.4.25/style-guide.html#naming-conventions.

Contract Functions

Contract	Type	Bases		
	Function Name	Visibility	Mutability	Modifiers
Ownable	Implementation	Context		
	<Constructor>	Public	✓	-
	owner	Public		-
	_checkOwner	Internal		
	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	✓	
	_spendAllowance	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		
MaxROI	Implementation	Ownable, ERC20		
	<Constructor>	Public	✓	ERC20
	updateParams	Public	✓	onlyOwner
	updateEpochLength	Public	✓	onlyOwner
	setReinvestWallet	Public	✓	onlyOwner
	addAccountToCapWhitelist	External	✓	onlyOwner
	removeAccountToCapWhitelist	External	✓	onlyOwner
	setTradeVolumeRanges	Public	✓	onlyOwner
	findCap	Public		-
	addPairs	External	✓	onlyOwner
	removePairs	External	✓	onlyOwner
	_transfer	Internal	✓	

Contract Flow



Domain Info

Domain Name	safeinvantage.com
Registry Domain ID	2675690812_DOMAIN_COM-VRSN
Creation Date	2022-02-16T21:01:41Z
Updated Date	2022-08-02T19:01:38Z
Registry Expiry Date	2023-02-16T21:01:41Z
Registrar WHOIS Server	whois.launchpad.com
Registrar URL	LaunchPad.com
Registrar	Launchpad, Inc. (HostGator)
Registrar IANA ID	955

The domain was created 8 months before the creation of the audit. It will expire in 4 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 stopping transactions and manipulating fees. The contract can be converted into a honeypot and prevent users from selling if the owner abuses the admin functions. There are also some findings regarding the numbers calculation precision.

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