Cyberscope

Audit Report

Zira

November 2022

Table of Contents

Contract Review

Contract Name	Zira
Compiler Version	v0.8.15+commit.e14f2714
Optimization	200 runs
Test Deploy	https://testnet.bscscan.com/token/0x9B56537f39a422bfBB37DF0c79707809538d1917
Symbol	Zira
Decimals	9
Total Supply	100,000,000,000,000
Domain	ziratoken.com

Source Files

Filename	**SHA256**
contract.sol	d19988662a0ce2afd8a3e0ea6693b62ef9e7900eb1218a25b1d8177ad1c88dbd

Audit Updates

Initial Audit	29th November 2022
Corrected	

Contract Analysis

● Critical ● Medium ● Minor / Informative ● Pass

Severity	Code	Description	Status
●	ST	Stops Transactions	Passed
●	OCTD	Transfers Contract's Tokens	Passed
●	OTUT	Transfers User's Tokens	Passed
●	ELFM	Exceeds Fees Limit	Passed
●	ULTW	Transfers Liquidity to Team Wallet	Passed
●	MT	Mints Tokens	Passed
●	BT	Burns Tokens	Passed
●	BC	Blacklists Addresses	Passed

Contract Diagnostics

● Critical   ● Medium   ● Minor / Informative

Severity	Code	Description	Status
●	L04	Conformance to Solidity Naming Conventions	Unresolved
●	L07	Missing Events Arithmetic	Unresolved
●	L12	Using Variables before Declaration	Unresolved
●	L13	Divide before Multiply Operation	Unresolved
●	L14	Uninitialized Variables in Local Scope	Unresolved

L04 - Conformance to Solidity Naming Conventions

Criticality	minor / informative
Location	contract.sol#L33,117,171,138,114,408,156,187,144,154,158,115,155,157,118,116
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.

```
WETH
_decimals
_taxWallets
_taxRates
startingSupply
_antiBlock
maxTransferTaxes
_hasLiqBeenAdded
_ratios
...
```

Recommendation

Follow the Solidity naming convention.
https://docs.soliditylang.org/en/v0.8.17/style-guide.html#naming-conventions.

L07 - Missing Events Arithmetic

Criticality	minor / informative
Location	contract.sol#L448,470,461
Status	Unresolved

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.

```
_maxWalletSize = (_tTotal * percent) / divisor
piSwapPercent = priceImpactSwapPercent
swapThreshold = (_tTotal * thresholdPercent) / thresholdDivisor
```

Recommendation

Emit an event for critical parameter changes.

L12 - Using Variables before Declaration

Criticality	minor / informative
Location	contract.sol#L778
Status	Unresolved

Description

The contract is using a variable before the declaration. This is usually happening either if it has not been declared yet or the variable has been declared in a different scope.

```
check
```

Recommendation

The variables should be declared before any usage of them.

L13 - Divide before Multiply Operation

Criticality	minor / informative
Location	contract.sol#L565,765
Status	Unresolved

Description

Performing divisions before multiplications may cause lose of prediction.

```
toLiquify = ((contractTokenBalance * ratios.liquidity) / ratios.totalSwap) / 2
feeAmount = (tAmount * currentFee) / masterTaxDivisor
```

Recommendation

The multiplications should be prior to the divisions.

L14 - Uninitialized Variables in Local Scope

Criticality	minor / informative
Location	contract.sol#L778,766,777
Status	Unresolved

Description

The are variables that are defined in the local scope and are not initialized.

```
check
values
checked
```

Recommendation

All the local scoped variables should be initialized.

Contract Functions

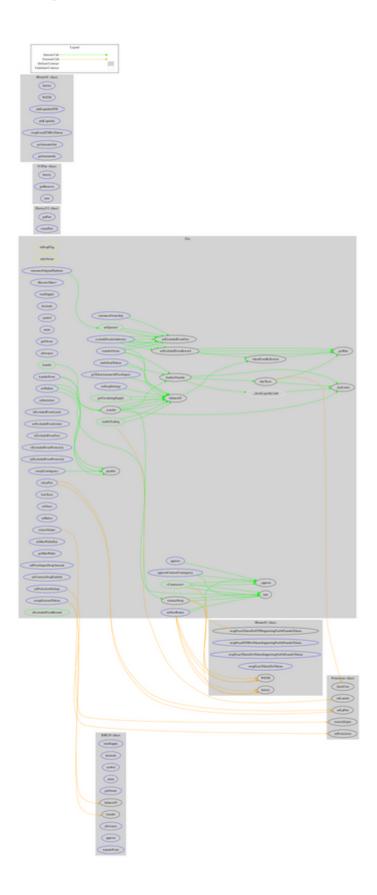| Contract	Type	Bases		
	Function Name	**Visibility**	**Mutability**	**Modifiers**
IERC20	Interface			
	totalSupply	External		-
	decimals	External		-
	symbol	External		-
	name	External		-
	getOwner	External		-
	balanceOf	External		-
	transfer	External	✓	-
	allowance	External		-
	approve	External	✓	-
	transferFrom	External	✓	-
IFactoryV2	Interface			
	getPair	External		-
	createPair	External	✓	-
IV2Pair	Interface			
	factory	External		-
	getReserves	External		-
	sync	External	✓	-
IRouter01	Interface			
	factory	External		-
	WETH	External		-
	addLiquidityETH	External	Payable	-
	addLiquidity	External	✓	-
	swapExactETHForTokens	External	Payable	-
	getAmountsOut	External		-
	getAmountsIn	External		-

IRouter02	Interface	IRouter01			
	swapExactTokensForETHSupporting FeeOnTransferTokens	External	✓	-	
	swapExactETHForTokensSupporting FeeOnTransferTokens	External	Payable	-	
	swapExactTokensForTokensSupporti ngFeeOnTransferTokens	External	✓	-	
	swapExactTokensForTokens	External	✓	-	
Protections	Interface				
	checkUser	External	✓	-	
	setLaunch	External	✓	-	
	setLpPair	External	✓	-	
	setProtections	External	✓	-	
	removeSniper	External	✓	-	
Zira	Implementation	IERC20			
	<Constructor>	Public	Payable	-	
	transferOwner	External	✓	onlyOwner	
	renounceOwnership	External	✓	onlyOwner	
	setOperator	Public	✓	-	
	renounceOriginalDeployer	External	✓	-	
	<Receive Ether>	External	Payable	-	
	totalSupply	External		-	
	decimals	External		-	
	symbol	External		-	
	name	External		-	
	getOwner	External		-	
	allowance	External		-	
	balanceOf	Public		-	
	transfer	Public	✓	-	
	approve	External	✓	-	
	_approve	Internal	✓		
	approveContractContingency	External	✓	onlyOwner	
	transferFrom	External	✓	-	

setNewRouter	External	✓	onlyOwner	
setLpPair	External	✓	onlyOwner	
setInitializer	External	✓	onlyOwner	
isExcludedFromLimits	External		-	
setExcludedFromLimits	External	✓	onlyOwner	
isExcludedFromFees	External		-	
setExcludedFromFees	Public	✓	onlyOwner	
isExcludedFromProtection	External		-	
setExcludedFromProtection	External	✓	onlyOwner	
getCirculatingSupply	Public		-	
removeSniper	External	✓	onlyOwner	
setProtectionSettings	External	✓	onlyOwner	
lockTaxes	External	✓	onlyOwner	
setTaxes	External	✓	onlyOwner	
setRatios	External	✓	onlyOwner	
setWallets	External	✓	onlyOwner	
setMaxWalletSize	External	✓	onlyOwner	
getMaxWallet	External		-	
getTokenAmountAtPriceImpact	External		-	
setSwapSettings	External	✓	onlyOwner	
setPriceImpactSwapAmount	External	✓	onlyOwner	
setContractSwapEnabled	External	✓	onlyOwner	
excludePresaleAddresses	External	✓	onlyOwner	
_hasLimits	Internal			
_transfer	Internal	✓		
contractSwap	Internal	✓	inSwapFlag	
_checkLiquidityAdd	Internal	✓		
enableTrading	Public	✓	onlyOwner	
sweepContingency	External	✓	onlyOwner	
sweepExternalTokens	External	✓	onlyOwner	
multiSendTokens	External	✓	onlyOwner	
isExcludedFromReward	Public		-	
setExcludedFromReward	Public	✓	onlyOwner	
tokenFromReflection	Public		-	
finalizeTransfer	Internal	✓		

	takeTaxes	Internal	✓	
	_getRate	Internal		

Contract Flow

Domain Info

Domain Name	ziratoken.com
Registry Domain ID	2740688777_DOMAIN_COM-VRSN
Creation Date	2022-11-25T01:00:20Z
Updated Date	2022-11-25T01:00:20Z
Registry Expiry Date	2023-11-25T01:00:20Z
Registrar WHOIS Server	whois.godaddy.com
Registrar URL	http://www.godaddy.com
Registrar	GoDaddy.com, LLC
Registrar IANA ID	146

The domain was created 4 days before the creation of the audit. It will expire in 12 months.

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

Summary

Zira is an interesting project that has a friendly and growing community. The Smart Contract analysis reported no compiler error or critical issues. The contract Owner can access some admin functions that can not be used in a malicious way to disturb the users' transactions. There is also a limit of max 20% buy/sell fees.

Disclaimer

The information provided in this report does not constitute investment, financial or trading advice and you should not treat any of the document's content as such. This report may not be transmitted, disclosed, referred to or relied upon by any person for any purposes nor may copies be delivered to any other person other than the Company without Cyberscope's prior written consent. This report is not nor should be considered an "endorsement" or "disapproval" of any particular project or team. This report is not nor should be regarded as an indication of the economics or value of any "product" or "asset" created by any team or project that contracts Cyberscope to perform a security assessment. This document does not provide any warranty or guarantee regarding the absolute bug-free nature of the technology analyzed, nor do they provide any indication of the technologies proprietors' business, business model or legal compliance. This report should not be used in any way to make decisions around investment or involvement with any particular project. This report represents an extensive assessment process intending to help our customers increase the quality of their code while reducing the high level of risk presented by cryptographic tokens and blockchain technology.

Blockchain technology and cryptographic assets present a high level of ongoing risk Cyberscope's position is that each company and individual are responsible for their own due diligence and continuous security Cyberscope's goal is to help reduce the attack vectors and the high level of variance associated with utilizing new and consistently changing technologies and in no way claims any guarantee of security or functionality of the technology we agree to analyze. The assessment services provided by Cyberscope are subject to dependencies and are under continuing development. You agree that your access and/or use including but not limited to any services reports and materials will be at your sole risk on an as-is where-is and as-available basis Cryptographic tokens are emergent technologies and carry with them high levels of technical risk and uncertainty. The assessment reports could include false positives false negatives and other unpredictable results. The services may access and depend upon multiple layers of third parties.

About Cyberscope

Cyberscope is a blockchain cybersecurity company that was founded with the vision to make web3.0 a safer place for investors and developers. Since its launch, it has worked with thousands of projects and is estimated to have secured tens of millions of investors' funds.

Cyberscope is one of the leading smart contract audit firms in the crypto space and has built a high-profile network of clients and partners.

The Cyberscope team

https://www.cyberscope.io