Cyberscope

Audit Report

OracleBSC

July 2022

SHA256 922dbd25967e9d0fd12f181c215cf2938d1a15d4267e703c7a0b3c1d455b8671

Audited by © cyberscope

Table of Contents

Contract Review

Contract Name	OracleBSC
Test Deploy	https://testnet.bscscan.com/address/0xCcE2fE5b3f9cdd6a4F3340afB044E6B401c5212B
Domain	https://defilabs.farm

Audit Updates

Initial Audit	19th July 2022
Corrected	

Source Files

Filename	SHA256
@openzeppelin/contracts/math/SafeMath.sol	665f1eab7288dc1142b1330d74a42cf18bb24d1d9fbf1efbb17e0acb46a278dd
contracts/interfaces/IUniswapV2Factory.sol	cb44da301a37b2243045c14056e9a3e59e0609fbf71c03bea272a009bcfd0034
contracts/interfaces/IUniswapV2Pair.sol	7312bad047f9998b7e84fc2539bbf52dac7425078ca2fd961405018b1d89358f
contracts/OracleBSC.sol	922dbd25967e9d0fd12f181c215cf2938d1a15d4267e703c7a0b3c1d455b8671

Introduction

The core functionality of OracleBSC is to provide the pair price between sequential tokens. The pair reserves are received from a market maker DAO.

To be more specific there are two accessible functions.

- The function R which provides information about the sequential pairs exchange price.
- The function pairFor which provides the address of the pair for tokenA and tokenB.

Contract Diagnostics

● Critical ● Medium ● Minor

Severity	Code	Description
●	CR	Code Repetition
●	FFV	Fixed Fee Value
●	L04	Conformance to Solidity Naming Conventions
●	L14	Uninitialized Variables in Local Scope

CR - Code Repetition

Criticality	minor
Location	contract.sol#L46,L96

Description

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

This code segment is used on `getReserves` and `pairFor` functions.

```
address pair = IUniswapV2Factory(factory).getPair(tokenA, tokenB);
```

Recommendation

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

FFV - Fixed Fee Value

Criticality	minor
Location	contract.sol#L66

Description

The Oracle uses an arbitrary fee of 0.3%. This may be required to be changed in the future.

```
uint256 amountInWithFee = amountIn.mul(997);
```

Recommendation

Create an external set function that modifies the fee with the necessary check to limit the fee to a reasonable amount.

L04 - Conformance to Solidity Naming Conventions

Criticality	minor
Location	contracts/OracleBSC.sol#L99,98,27,97,72 contracts/interfaces/IUniswapV2Pair.sol#L19,36,18

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.

```
R
_factory
WETH
DOMAIN_SEPARATOR
MINIMUM_LIQUIDITY
PERMIT_TYPEHASH
_tokenA
_tokenB
```

Recommendation

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

L14 - Uninitialized Variables in Local Scope

Criticality	minor
Location	contracts/OracleBSC.sol#L56

Description

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

```
i
```

Recommendation

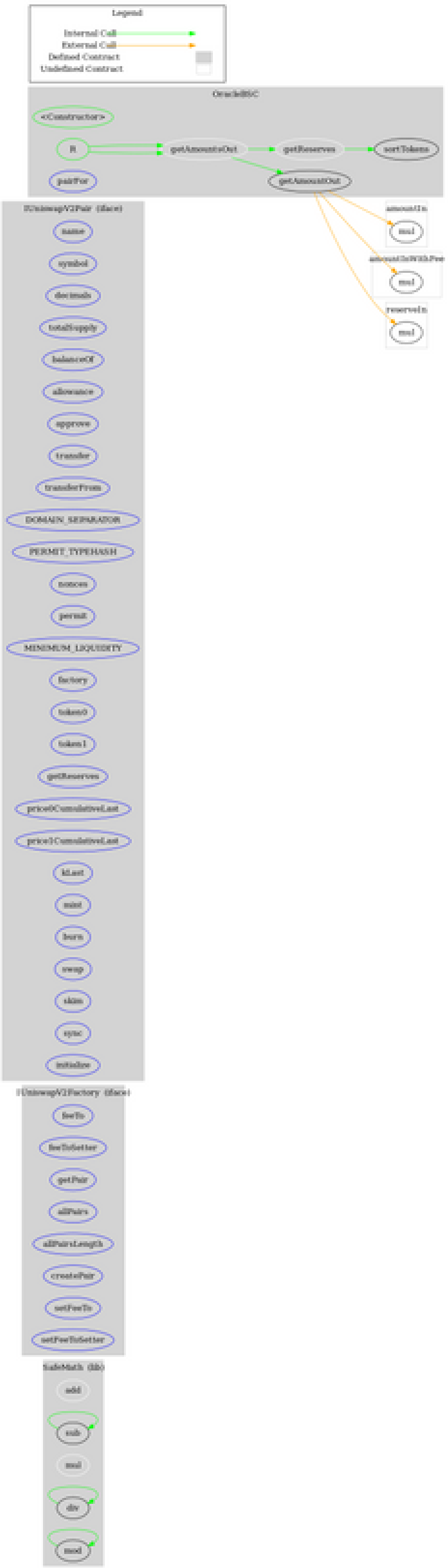
All the local scoped variables should be initialized.

Contract Functions

Contract	Type	Bases		
	Function Name	**Visibility**	**Mutability**	**Modifiers**
SafeMath	Library			
	add	Internal		
	sub	Internal		
	sub	Internal		
	mul	Internal		
	div	Internal		
	div	Internal		
	mod	Internal		
	mod	Internal		
IUniswapV2Factory	Interface			
	feeTo	External		-
	feeToSetter	External		-
	getPair	External		-
	allPairs	External		-
	allPairsLength	External		-
	createPair	External	✓	-
	setFeeTo	External	✓	-
	setFeeToSetter	External	✓	-
IUniswapV2Pair	Interface			
	name	External		-
	symbol	External		-
	decimals	External		-
	totalSupply	External		-
	balanceOf	External		-
	allowance	External		-

	approve	External	✓	-
	transfer	External	✓	-
	transferFrom	External	✓	-
	DOMAIN_SEPARATOR	External		-
	PERMIT_TYPEHASH	External		-
	nonces	External		-
	permit	External	✓	-
	MINIMUM_LIQUIDITY	External		-
	factory	External		-
	token0	External		-
	token1	External		-
	getReserves	External		-
	price0CumulativeLast	External		-
	price1CumulativeLast	External		-
	kLast	External		-
	mint	External	✓	-
	burn	External	✓	-
	swap	External	✓	-
	skim	External	✓	-
	sync	External	✓	-
	initialize	External	✓	-
OracleBSC	Implementation			
	<Constructor>	Public	✓	-
	sortTokens	Internal		
	getReserves	Internal		
	getAmountsOut	Internal		
	getAmountOut	Internal		
	R	Public		-
	pairFor	External		-

Contract Flow



Domain Info

Domain Name	defilabs.farm
Registry Domain ID	d44f7165186c43e6ab7e5570545b2f9e-DONUTS
Creation Date	2021-09-23T12:54:45Z
Updated Date	2022-07-18T09:44:52Z
Registry Expiry Date	2024-09-23T12:54:45Z
Registrar WHOIS Server	http://whois.cloudflare.com
Registrar URL	http://cloudflare.com
Registrar	Cloudflare, Inc
Registrar IANA ID	1910

The domain was created about 2 years before the creation of the audit.

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

Summary

OracleBSC provides information about onchain data in correlation with an amount and the pair data. The Smart Contract analysis reported no compiler error or critical issues. The contract Owner cannot access admin functions that can be used in a malicious way to disturb the users’.

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