Cyberscope

Audit Report

WakandaFactory

September 2022

Type	BEP20
Network	BSC TESTNET
Address	0x6A506e21090690FACC73c76e34756fcF7A04f4aC
Audited by	© cyberscope

Table of Contents

Contract Review

Contract Name	WakandaFactory
Compiler Version	v0.6.6+commit.6c089d02
Testing Deploy	https://testnet.bscscan.com/token/0x6A506e21090690FACC73c76e34756fcF7A04f4aC

Audit Updates

Initial Audit	21st September 2022
Corrected	

Source Files

Filename	SHA256
helpers/IERC20.sol	64469bf9aef280453f36bf73598078a603b95f1ef20bc0ef8256e76b216c44d8
helpers/SafeMath.sol	51604361809b388e40152c7d360bd3cedf344615610b49a594228a03f7ff2d2f
swap/Wakanda_pair.sol	ff79583befc414db7acb61a9cfeb334e807b419b87a577808e1386d126b20aab

Introduction

WakandaFactory is an automated liquidity protocol powered by a constant product formula and implemented in a system of non-upgradeable smart contracts. It obviates the need for trusted intermediaries, prioritizing decentralization, censorship resistance, and security.

Each WakandaFactory smart contract, or pair, manages a liquidity pool made up of reserves of two ERC-20 tokens.

Anyone can become a liquidity provider for a pool by depositing an equivalent value of each underlying token in return for pool tokens. These tokens track pro-rata LP shares of the total reserves, and can be redeemed for the underlying assets at any time.

Roles

The "feeToSetter" role has the ability to set the address of the liquidity receiver. The liquidity is minted by the internal leverage mechanism of the pair contract.

Contract Diagnostics

● Critical   ● Medium   ● Minor / Informative

Severity	Code	Description	Status
●	L04	Conformance to Solidity Naming Conventions	Unresolved

L04 - Conformance to Solidity Naming Conventions

Criticality	minor / informative
Location	src/swap/Wakanda_pair.sol#L690,438,695,196
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.

```
_feeTo
_token0
_token1
_feeToSetter
DOMAIN_SEPARATOR
```

Recommendation

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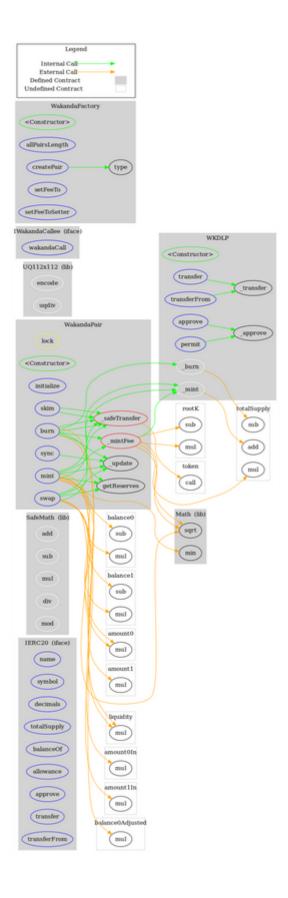
Contract Functions

Contract	Type	Bases		
	Function Name	Visibility	Mutability	Modifiers
IERC20	Interface			
	name	External		-
	symbol	External		-
	decimals	External		-
	totalSupply	External		-
	balanceOf	External		-
	allowance	External		-
	approve	External	✓	-
	transfer	External	✓	-
	transferFrom	External	✓	-
SafeMath	Library			
	add	Internal		
	sub	Internal		
	mul	Internal		
	div	Internal		
	mod	Internal		
WKDLP	Implementation			
	<Constructor>	Public	✓	-
	_mint	Internal	✓	
	_burn	Internal	✓	
	_approve	Private	✓	
	_transfer	Private	✓	
	approve	External	✓	-
	transfer	External	✓	-
	transferFrom	External	✓	-
	permit	External	✓	-

Math	Library			
	min	Internal		
	sqrt	Internal		
UQ112x112	Library			
	encode	Internal		
	uqdiv	Internal		
IWakandaCallee	Interface			
	wakandaCall	External	✓	-
WakandaPair	Implementation	WKDLP		
	getReserves	Public		-
	_safeTransfer	Private	✓	
	<Constructor>	Public	✓	-
	initialize	External	✓	-
	_update	Private	✓	
	_mintFee	Private	✓	
	mint	External	✓	lock
	burn	External	✓	lock
	swap	External	✓	lock
	skim	External	✓	lock
	sync	External	✓	lock
WakandaFactory	Implementation			
	<Constructor>	Public	✓	-
	allPairsLength	External		-
	createPair	External	✓	-
	setFeeTo	External	✓	-
	setFeeToSetter	External	✓	-

Contract Flow

Summary

The smart contract analysis reported no critical or compiler issues. This audit focused on investigating security issues and potential improvements.

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