



Cyberscope

Audit Report

GenericStakeFactory

September 2022

Type BEP20

Network BSC

Address 0xb2240DfCba543244B018eF9f22DeE8Ae7cac4dD7

Audited by © cyberscope

Table of Contents

Table of Contents	1
Contract Review	2
Audit Updates	2
Source Files	3
Introduction	4
Contract Diagnostics	5
L01 - Public Function could be Declared External	6
Description	6
Recommendation	6
L04 - Conformance to Solidity Naming Conventions	7
Description	7
Recommendation	7
L07 - Missing Events Arithmetic	8
Description	8
Recommendation	8
L08 - Tautology or Contradiction	9
Description	9
Recommendation	9
Contract Flow	13
Summary	14
Disclaimer	15
About Cyberscope	16

Contract Review

Contract Name	GenericStakeFactory
Compiler Version	v0.6.12+commit.27d51765
Optimization	99999 runs
Explorer	https://bscscan.com/token/0xb2240DfCba543244B018eF9f22DeE8Ae7cac4dD7

Audit Updates

Initial Audit	22nd September 2022
Corrected	

Source Files

Filename	SHA256
contracts/access/Ownable.sol	b9f957b42bdcf3d3499be4c94558152e91658e34a1fe5a5e8f0972ce20e15ed7
contracts/math/SafeMath.sol	f5421275a1e2b5a0dd0592a4ce1a09cefc339fceb42e822e0f711a5c66933ae8
contracts/utils/Address.sol	11ad5e3e21434e00c4ceba1f5a977b7a68bdd7d16b849276ce4ff4495129eec7
contracts/utils/Context.sol	9a3d1e5be0f0ace13e2d9aa1d0a1c3a6574983983ad5de94fc412f878bf7fe89
contracts/utils/ReentrancyGuard.sol	3fc7968f4a1937caf3c96dffbac350398f86faad96288502e02c3a2b9f245e39
src/farm/GenericStake.sol	06477467676480b4dd899e462bdd869f01d76a732d2c2524edbfa8b3d7bcf0c8
src/farm/GenericStakeFactory.sol	3a96a65ecfe878f12be23900abb85a12363ecb174e0f142f4544e7c0429007ea
src/helpers/IBEP20.sol	5f8366fc3b9a5a8e25a639f2cf8534b5e017ffdce91c597dd7668e557c2fe272
src/helpers/SafeBEP20.sol	aba52f299dbdf14cfd80413ea56012290bfee253c99a09d5e9bc2bf09246d42e

Introduction

The contract GenericStakeFactory is responsible for the initialization of the Wakanda pool. The contract provides one method, which is accessible from the owner. The function accepts the required arguments in order to initialize the pool.

Contract Diagnostics

● Critical ● Medium ● Minor / Informative

Severity	Code	Description	Status
●	L01	Public Function could be Declared External	Unresolved
●	L04	Conformance to Solidity Naming Conventions	Unresolved
●	L07	Missing Events Arithmetic	Unresolved
●	L08	Tautology or Contradiction	Unresolved

L01 - Public Function could be Declared External

Criticality	minor / informative
Location	contract/GenericStake.sol#L200
Status	Unresolved

Description

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

```
availableRewards
```

Recommendation

Use the external attribute for functions never called from the contract.

L04 - Conformance to Solidity Naming Conventions

Criticality	minor / informative
Location	contract/GenericStake.sol#L86,127,91,290,235,90,87,304,89,88,330,225,171,268,18,269,46,303,92 contract/GenericStakeFactory.sol#L34,33,29,35,32,30,31
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.

```
_stakedToken  
_amount  
_poolLimitPerUser  
_rewardPerBlock  
_tokenAddress  
_bonusEndBlock  
_rewardToken  
_tokenAmount  
_startBlock  
...
```

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 / informative
Location	contract/GenericStake.sol#L85
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.

```
rewardPerBlock = _rewardPerBlock
```

Recommendation

Emit an event for critical parameter changes.

L08 - Tautology or Contradiction

Criticality	minor / informative
Location	contract/GenericStakeFactory.sol#L28
Status	Unresolved

Description

Detects expressions that are tautologies or contradictions. For instance, an uint variable will always be greater than or equal to zero.

```
require(bool)(_stakedToken.totalSupply() >= 0)
require(bool)(_rewardToken.totalSupply() >= 0)
```

Recommendation

Fix the incorrect comparison by changing the value type or the comparison.

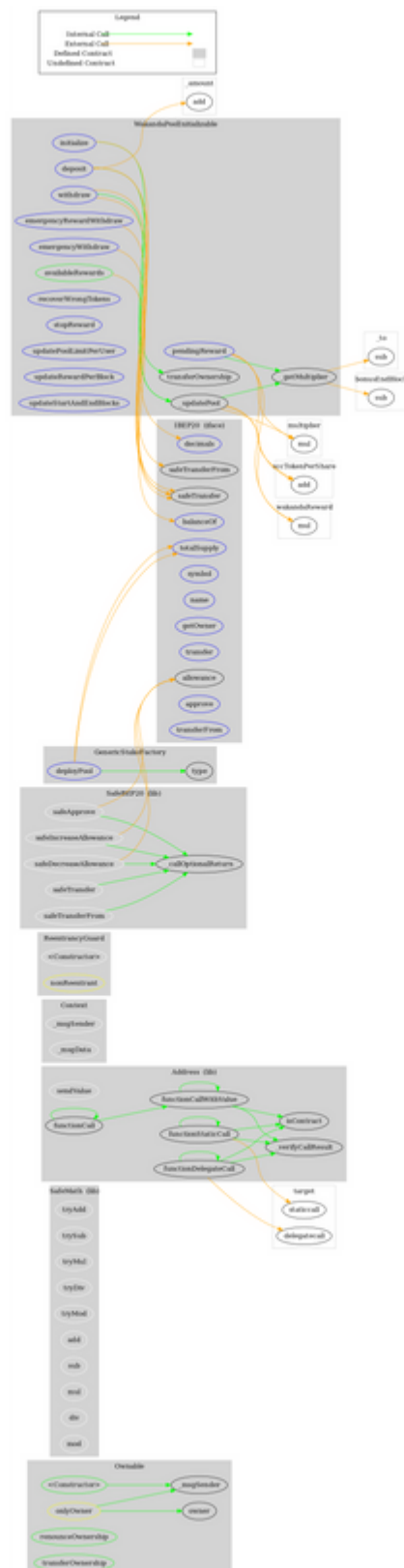
Contract Functions

Contract	Type	Bases		
	Function Name	Visibility	Mutability	Modifiers
Ownable	Implementation	Context		
	<Constructor>	Internal	✓	
	owner	Public		-
	renounceOwnership	Public	✓	onlyOwner
	transferOwnership	Public	✓	onlyOwner
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		
Address	Library			
	isContract	Internal		
	sendValue	Internal	✓	
	functionCall	Internal	✓	
	functionCall	Internal	✓	
	functionCallWithValue	Internal	✓	
	functionCallWithValue	Internal	✓	
	functionStaticCall	Internal		

	functionStaticCall	Internal		
	functionDelegateCall	Internal	✓	
	functionDelegateCall	Internal	✓	
	_verifyCallResult	Private		
Context	Implementation			
	_msgSender	Internal		
	_msgData	Internal		
ReentrancyGuard	Implementation			
	<Constructor>	Internal	✓	
WakandaPool initializable	Implementation	Ownable, Reentrancy Guard		
	<Constructor>	Public	✓	-
	initialize	External	✓	-
	deposit	External	✓	nonReentrant
	withdraw	External	✓	nonReentrant
	availableRewards	Public		-
	emergencyWithdraw	External	✓	nonReentrant
	emergencyRewardWithdraw	External	✓	onlyOwner
	recoverWrongTokens	External	✓	onlyOwner
	stopReward	External	✓	onlyOwner
	updatePoolLimitPerUser	External	✓	onlyOwner
	updateRewardPerBlock	External	✓	onlyOwner
	updateStartAndEndBlocks	External	✓	onlyOwner
	pendingReward	External		-
	_updatePool	Internal	✓	
	_getMultiplier	Internal		
GenericStakeFactory	Implementation	Ownable		
	<Constructor>	Public	✓	-
	deployPool	External	✓	onlyOwner

IBEP20	Interface			
	totalSupply	External		-
	decimals	External		-
	symbol	External		-
	name	External		-
	getOwner	External		-
	balanceOf	External		-
	transfer	External	✓	-
	allowance	External		-
	approve	External	✓	-
	transferFrom	External	✓	-
SafeBEP20	Library			
	safeTransfer	Internal	✓	
	safeTransferFrom	Internal	✓	
	safeApprove	Internal	✓	
	safeIncreaseAllowance	Internal	✓	
	safeDecreaseAllowance	Internal	✓	
	_callOptionalReturn	Private	✓	

Contract Flow



Summary

The GenericStakeFactory operates as an initializer for the Wakanda pool. The Smart Contract analysis reported no compiler error or critical issues. This audit focused on investigating possible 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>