Audit Report

BUSDX

January 2022

Type	BEP20
Network	BSC
Address	0xbfF60C4Ab0e632A48D879E79Ffb8cA400fDc3bF4
Audited by	© coinscope

Table of Contents

Table of Contents 1
Contract Review 3
Audit Updates 3
Contract Analysis 4
Contract Diagnostics 5
L01 - Public Function could be Declared External 6
Description 6
Recommendation 6
L02 - State Variables could be Declared Constant 7
Description 7
Recommendation 7
L04 - Conformance to Solidity Naming Conventions 8
Description 8
Recommendation 8
L11 - Unnecessary Boolean equality 9
Description 9
Recommendation 9
L07 - Missing Events Arithmetic 10
Description 10
Recommendation 10
L06 - Missing Events Access Control 11
Description 11
Recommendation 11
Contract Functions 12
Contract Flow 17
Domain Info 18

Summary 19

Disclaimer 21

About Coinscope 22

Contract Review

Contract Name	RewardStaking
Compiler Version	v0.8.11+commit.d7f03943
Optimization	200 runs
Licence	
Explorer	https://bscscan.com/token/0xbfF60C4Ab0e632A48D879E79Ffb8cA400fDc3bF4
Total Supply	277,787,983,744,415,950,000,000,000
Source	/Users/aravinth/Repo/codegama/blockchain/ido_projects/ido-frontend-jason/src/contracts/RewardStaking.sol, @openzeppelin/contracts/utils/math/SafeMath.sol, @openzeppelin/contracts/utils/introspection/IERC165.sol, @openzeppelin/contracts/utils/introspection/ERC165.sol, @openzeppelin/contracts/utils/Strings.sol, @openzeppelin/contracts/utils/Context.sol, @openzeppelin/contracts/token/ERC20/extensions/IERC20Metadata.sol, @openzeppelin/contracts/token/ERC20/IERC20.sol, @openzeppelin/contracts/token/ERC20/ERC20.sol, @openzeppelin/contracts/security/ReentrancyGuard.sol, @openzeppelin/contracts/security/Pausable.sol, @openzeppelin/contracts/access/Ownable.sol, @openzeppelin/contracts/access/IAccessControl.sol, @openzeppelin/contracts/access/AccessControl.sol
Domain	busdx.com

Audit Updates

Initial Audit	26th January 2022
Corrected	

Contract Analysis

● Critical ● Medium ● Minor ● Pass

Severity	Code	Description
●	ST	Contract Owner is not able to stop or pause transactions
●	OCTD	Contract Owner is not able to transfer tokens from specific address
●	OTUT	Owner Transfer User's Tokens
●	ULTW	Contract Owner is not able to increase the amount of liquidity taken by dev wallet more than a reasonable percent
●	BC	Contract Owner is not able to blacklist wallets from unstacking

Contract Diagnostics

Critical Medium Minor

Severity	Code	Description
	L01	Public Function could be Declared External
	L02	State Variables could be Declared Constant
	L04	Conformance to Solidity Naming Conventions
	L11	Unnecessary Boolean equality
	L07	Missing Events Arithmetic
	L06	Missing Events Access Control

L01 - Public Function could be Declared External

Criticality	minor
Location	contracts/RewardStaking.sol#L301,L297,L87

Description

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

```
unpause
pause
numberOfStakers
```

Recommendation

Use the external attribute for functions never called from the contract

L02 - State Variables could be Declared Constant

Criticality	minor
Location	contracts/RewardStaking.sol#L43,L42

Description

Constant state variables should be declared constant to save gas.

```
previousBalance
busdRewardAllocated
```

Recommendation

Add the constant attribute to state variables that never change.

L04 - Conformance to Solidity Naming Conventions

Criticality	minor
Location	contracts/RewardStaking.sol#L286,L279,L96 and 1 more

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.

```
_rewardRate
_rewardsDistribution
_amount
...
```

Recommendation

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

L11 - Unnecessary Boolean equality

Criticality	minor
Location	contracts/RewardStaking.sol#L254

Description

The comparison to boolean constants is redundant. Boolean constants can be used directly and do not need to be compared to true or false.

```
isStaking[recipient] == true
```

Recommendation

Remove the equality to the boolean constant.

L07 - Missing Events Arithmetic

Criticality	minor
Location	contracts/RewardStaking.sol#L286

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.

```
rewardRate = _rewardRate
```

Recommendation

Emit an event for critical parameter changes.

L06 - Missing Events Access Control

Criticality	minor
Location	contracts/RewardStaking.sol#L279

Description

Detected missing events for critical access control parameters. There are functions that have no event emitted, so it is difficult to track off-chain changes.

```
rewardsDistribution = _rewardsDistribution
```

Recommendation

Emit an event for critical parameter changes.

Contract Functions

Contract	Type	Bases		
	Function Name	**Visibility**	**Mutability**	**Modifiers**
AccessControl	Implementation	Context, IAccessControl, ERC165		
	supportsInterface	Public		-
	hasRole	Public		-
	_checkRole	Internal		
	getRoleAdmin	Public		-
	grantRole	Public	✓	onlyRole
	revokeRole	Public	✓	onlyRole
	renounceRole	Public	✓	-
	_setupRole	Internal	✓	
	_setRoleAdmin	Internal	✓	
	_grantRole	Internal	✓	
	_revokeRole	Internal	✓	
IAccessControl	Interface			
	hasRole	External		-
	getRoleAdmin	External		-
	grantRole	External	✓	-
	revokeRole	External	✓	-
	renounceRole	External	✓	-
Ownable	Implementation	Context		
	<Constructor>	Public	✓	-
	owner	Public		-
	renounceOwnership	Public	✓	onlyOwner
	transferOwnership	Public	✓	onlyOwner
	_transferOwnership	Internal	✓	

Pausable	Implementation	Context		
	<Constructor>	Public	✓	-
	paused	Public		-
	_pause	Internal	✓	whenNotPaused
	_unpause	Internal	✓	whenPaused
ReentrancyGuard	Implementation			
	<Constructor>	Public	✓	-
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	✓	
	_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		
ERC165	Implementation	IERC165		
	supportsInterface	Public		-
IERC165	Interface			
	supportsInterface	External		-
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		
Strings	Library			
	toString	Internal		
	toHexString	Internal		
	toHexString	Internal		
RewardStaking	Implementation	Ownable, AccessControl, ReentrancyGuard, Pausable		
	<Constructor>	Public	✓	-
	totalSupply	External		-
	balanceOf	External		-
	numberOfStakers	Public		-
	addGrandAmount	External	✓	onlyOwner
	removeGrandAmount	External	✓	onlyOwner
	removeBUSD	External	✓	onlyOwner
	timeStampDiff	Public		-
	rewardTokenPerAnnum	Public		-
	earned	Public		-
	busdEarned	Public		-
	stake	External	✓	nonReentrant whenNotPaused updateReward
	withdraw	Public	✓	nonReentrant updateReward
	getReward	Public	✓	nonReentrant updateReward
	exit	External	✓	-
	stakeRewardTokens	External	✓	nonReentrant whenNotPaused updateReward
	distributeBUSDReward	External	✓	onlyOwner
	setRewardsDistribution	External	✓	onlyOwner
	setRewardRate	External	✓	onlyOwner

	pause	Public	✓	onlyOwner
	unpause	Public	✓	onlyOwner

Contract Flow

Domain Info

Domain Name	busdx.com
Registry Domain ID	2643177086_DOMAIN_COM-VRSN
Creation Date	2021-09-23T19:59:46Z
Updated Date	2021-09-23T19:59:46.823625Z
Registry Expiry Date	
Registrar WHOIS Server	whois.squarespace.domains
Registrar URL	https://squarespace.domains
Registrar	Squarespace Domains, LLC
Registrar IANA ID	3827

The domain has been created 4 months before the creation of the audit.

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

Summary

BUSDX implements the fundamental stacking functionality. The admin can deposit BUSDX tokens and users can stack BUSDX to claim their rewards. The rewards are proportional to the stacking period and a configurable rate value.

The stacking contract provides an extra motivation to the holders by distributing BUSD to the users. The BSUD distribution is not forced by the contract. It is an optional feature that can be triggered by the contact owner.

The stacking operation can be stopped for all users including the contract owner. This is usually not an issue, since nobody can operate.

The function *addGrandAmount* gives the ability to the contract owner to provide BUSDX tokens to the contract and increase the “grant” balance. The grant balance is the amount of tokens that will be claimed as reward from the users. On the other hand, the function *removeGrandAmount* decreases the “grant” balance without removing the tokens. That means that the “grant” balance is potentially not equal to the BUSDX balance. If this functionality is misused by the contract owner, then the contract may end-up with stacked tokens.

The *removeGrandAmount* function could embody a check for not allowing the contract owner to decrease the “grant” balance less than the sum of all the awarded amounts.

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.

Coinscope 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 Coinscope 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 Coinscope 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 Coinscope team disclaims any liability for the resulting losses.

About Coinscope

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.

Coinscope is aiming to make crypto discoverable and efficient globally. It provides all the essential tools to assist users draw their own conclusions.

The Coinscope.co team

https://www.coinscope.co