Audit Report

Blue Horseshoe loves $BLUSHO

January 2022

Type	BEP20
Network	BSC TESTNET
Address	0xec6FD2a755F48849FB46dc3Dc83ACeeDba897D1E
Audited by	© coinscope

Table of Contents

Contract Review

Contract Name	BlushoToken
Compiler Version	v0.8.11+commit.d7f03943
Optimization	200 runs
Licence	
Explorer	https://testnet.bscscan.com/token/0xec6FD2a755F48849FB46dc3Dc83ACeeDba897D1E
Symbol	BLUSHO
Decimals	18
Total Supply	100,000,000
Source	/contracts/BlushoToken.sol, @openzeppelin/contracts/utils/Context.sol, @openzeppelin/contracts/token/ERC20/extensions/IERC20Metadata.sol, @openzeppelin/contracts/token/ERC20/IERC20.sol, @openzeppelin/contracts/access/Ownable.sol
Domain	blusho.finance

Audit Updates

Initial Audit	30th 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
●	ELFM	Contract Owner is not able to increase fees more than a reasonable percent (25%)
●	ULTW	Contract Owner is not able to increase the amount of liquidity taken by dev wallet more than a reasonable percent
●	MT	Contract Owner is not able to mint new tokens
●	BT	Contract Owner is not able to burn tokens from specific wallet
●	BC	Contract Owner is not able to blacklist wallets from selling

BC - Blacklisted Contracts

Criticality	medium
Location	contract.sol#L528

Description

The contract owner has the authority to stop contracts from transactions. The owner may take advantage of it by calling the `addBlacklistedWallet` function.

```
require(
    !_isBlacklistedWallet(sender),
    "BlushoToken: transfer from blacklisted wallet"
);
require(
    !_isBlacklistedWallet(recipient),
    "BlushoToken: transfer to blacklisted wallet"
);
```

Recommendation

The team should carefully manage the private keys of the owner's account. We strongly recommend a powerful security mechanism that will prevent a single user from accessing the contract admin functions. That risk can be prevented by temporarily locking the contract or renouncing ownership.

Contract Diagnostics

Critical Medium Minor

Severity	Code	Description
	CO	Code Optimization
	L01	Public Function could be Declared External
	L04	Conformance to Solidity Naming Conventions
	L11	Unnecessary Boolean equality
	L07	Missing Events Arithmetic

CO - Code Optimization

Criticality	minor
Location	contract.sol#L540

Description

There are code segments that could be optimized. A segment may be optimized so that it becomes a smaller size, consumes less memory, executes more rapidly, or performs fewer operations.

```
if (
    _isInPresale ||
    _isUnlimitedWallet(sender) ||
    _isUnlimitedWallet(recipient)
) {
    //do nothing if one of the participants is an unlimited address
}
```

Recommendation

Rewrite some code segments so the runtime will be more performant.

L01 - Public Function could be Declared External

Criticality	minor
Location	contracts/BlushoToken.sol#L953,L925,L851 and 12 more

Description

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

```
transferOwnershipToProjectWallet
addProjectWallet
setTaxProjectsSchedule
...
```

Recommendation

Use the external attribute for functions never called from the contract

L04 - Conformance to Solidity Naming Conventions

Criticality	minor
Location	contracts/BlushoToken.sol#L243,L236,L231 and 16 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.

```
_pendingProjectTaxesToBeBurned
_totalProjectWalletsBalance
_projectsTaxCycle
...
```

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/BlushoToken.sol#L737

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.

```
require(bool,string)(_isInPresale == true,BlushoToken: not in presale mode)
```

Recommendation

Remove the equality to the boolean constant.

L07 - Missing Events Arithmetic

Criticality	minor
Location	contracts/BlushoToken.sol#L851,L758,L720

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.

```
_taxProjectsSchedule = schedule
_taxDeveloper = tax
_transactionLimit = transactionLimit
```

Recommendation

Emit an event for critical parameter changes.

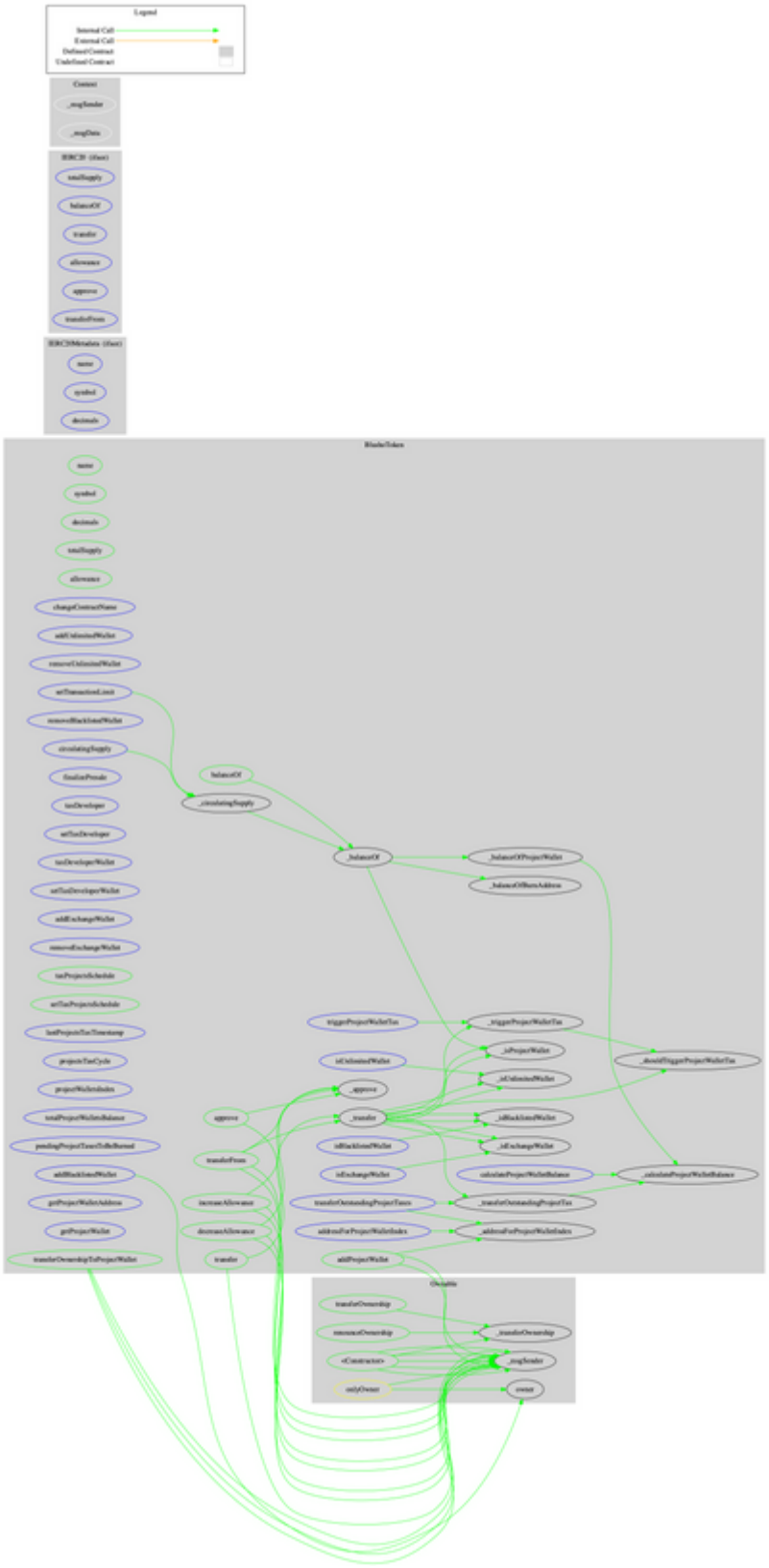
Contract Functions

Contract	Type	Bases		
	Function Name	**Visibility**	**Mutability**	**Modifiers**
Ownable	Implementation	Context		
	<Constructor>	Public	✓	-
	owner	Public		-
	renounceOwnership	Public	✓	onlyOwner
	transferOwnership	Public	✓	onlyOwner
	_transferOwnership	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		
BlushoToken	Implementation	IERC20Metadata, Ownable		
	<Constructor>	Public	✓	-
	name	Public		-

	symbol	Public		-
	decimals	Public		-
	totalSupply	Public		-
	balanceOf	Public		-
	_balanceOf	Internal		
	transfer	Public	✓	-
	allowance	Public		-
	approve	Public	✓	-
	transferFrom	Public	✓	-
	increaseAllowance	Public	✓	-
	decreaseAllowance	Public	✓	-
	_transfer	Internal	✓	
	_approve	Internal	✓	
	changeContractName	External	✓	onlyOwner
	isUnlimitedWallet	External		-
	_isUnlimitedWallet	Internal		
	addUnlimitedWallet	External	✓	onlyOwner
	removeUnlimitedWallet	External	✓	onlyOwner
	isBlacklistedWallet	External		-
	_isBlacklistedWallet	Internal		
	addBlacklistedWallet	External	✓	onlyOwner
	removeBlacklistedWallet	External	✓	onlyOwner
	setTransactionLimit	External	✓	onlyOwner
	finalizePresale	External	✓	onlyOwner
	taxDeveloper	External		-
	setTaxDeveloper	External	✓	onlyOwner
	taxDeveloperWallet	External		-
	setTaxDeveloperWallet	External	✓	onlyOwner
	isExchangeWallet	External		-
	_isExchangeWallet	Internal		
	addExchangeWallet	External	✓	onlyOwner
	removeExchangeWallet	External	✓	onlyOwner
	taxProjectsSchedule	Public		-
	setTaxProjectsSchedule	Public	✓	onlyOwner
	lastProjectsTaxTimestamp	External		-

	projectsTaxCycle	External		-
	projectWalletsIndex	External		-
	totalProjectWalletsBalance	External		-
	pendingProjectTaxesToBeBurned	External		-
	_addressForProjectWalletIndex	Internal		
	addressForProjectWalletIndex	External		-
	addProjectWallet	Public	✓	-
	transferOwnershipToProjectWallet	Public	✓	-
	getProjectWalletAddress	External		-
	getProjectWallet	External		-
	_shouldTriggerProjectWalletTax	Internal		
	_triggerProjectWalletTax	Internal	✓	
	triggerProjectWalletTax	External	✓	-
	transferOutstandingProjectTaxes	External	✓	-
	_calculateProjectWalletBalance	Internal		
	calculateProjectWalletBalance	External		-
	_balanceOfProjectWallet	Internal		
	_isProjectWallet	Internal		
	_transferOutstandingProjectTax	Internal	✓	
	_balanceOfBurnAddress	Internal		
	_circulatingSupply	Internal		
	circulatingSupply	External		-

Contract Flow



Domain Info

Domain Name	blusho.finance
Registry Domain ID	815f0ac41e5f4b52b113013c21ac4bbd-DONUTS
Creation Date	2022-01-10T06:04:34Z
Updated Date	2022-01-15T06:05:34Z
Registry Expiry Date	2023-01-10T06:04:34Z
Registrar WHOIS Server	whois.namecheap.com
Registrar URL	https://www.namecheap.com/
Registrar	NameCheap, Inc.
Registrar IANA ID	1068

The domain has been created 20 days before the creation of the audit. It will expire in 11 months.

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

Summary

Blue Horseshoe loves $BLUSHO. $BLUSHO is aiming to build a community driven marketing platform for DeFi communities. It has a novel implementation where users can create wallets and move funds to these wallets. Blue Horseshoe will rank those wallets and give the chance to these wallets to stand out. The Smart Contract analysis reported only one issue. The contract owner can blacklist addresses. Apart from this, 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 10% fees.

The "created wallet" projects does not interfere with the normal transactions of the users. It's the user's choice to issue a transaction to a project wallet.

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