KISHIELD

Security Audit

BJcoin Token

April 14, 2022

Table of Contents

Audit Summary

This report has been prepared for BJcoin Token on the Binance Chain network. KISHIELD provides both client-centered and user-centered examination of the smart contracts and their current status when applicable. This report represents the security assessment made to find issues and vulnerabilities on the source code along with the current liquidity and token holder statistics of the protocol.

A comprehensive examination has been performed, utilizing Cross Referencing, Static Analysis, In-House Security Tools, and line-by-line Manual Review.

The auditing process pays special attention to the following considerations:

- Ensuring contract logic meets the specifications and intentions of the client without exposing the user's funds to risk.
- Testing the smart contracts against both common and uncommon attack vectors.
- Inspecting liquidity and holders statistics to inform the current status to both users and client when applicable.
- Assessing the codebase to ensure compliance with current best practices and industry standards.
- Verifying contract functions that allow trusted and/or untrusted actors to mint, lock, pause, and transfer assets.
- Thorough line-by-line manual review of the entire codebase by industry experts.

Project Overview

Token Summary

Parameter	Result
Address	0x60F500E174E2Ea3A07b7071EC8982d268a4f81C0
Name	BJcoin
Token Tracker	BJcoin (BJ coin)
Decimals	18
Supply	2,000,000,000
Platform	Binance Chain
compiler	v0.6.12+commit.27d51765
Optimization	Yes with 200 runs
LicenseType	MIT
Language	Solidity
Codebase	https://bscscan.com/address/0x60F500E174E2Ea3A07b7071EC8982d268a4f81C0
Url	http://bluejohncoin.com/

Main Contract Assessed

Name	Contract	Live
BJcoin	0x60F500E174E2Ea3A07b7071EC8982d268a4f81C0	Yes

Smart Contract Vulnerability Checks

Vulnerability	Automatic Scan	Manual Scan	Result
Unencrypted Private Data On-Chain	Complete	Complete	Low / No Risk
Code With No Effects	Complete	Complete	Low / No Risk
Message call with hardcoded gas amount	Complete	Complete	Low / No Risk
Hash Collisions With Multiple Variable Length Arguments	Complete	Complete	Low / No Risk
Unexpected Ether balance	Complete	Complete	Low / No Risk
Presence of unused variables	Complete	Complete	Low / No Risk
Right-To-Left-Override control character (U+202E)	Complete	Complete	Low / No Risk
Typographical Error	Complete	Complete	Low / No Risk
DoS With Block Gas Limit	Complete	Complete	Low / No Risk
Arbitrary Jump with Function Type Variable	Complete	Complete	Low / No Risk
Insufficient Gas Griefing	Complete	Complete	Low / No Risk
Incorrect Inheritance Order	Complete	Complete	Low / No Risk
Write to Arbitrary Storage Location	Complete	Complete	Low / No Risk
Requirement Violation	Complete	Complete	Low / No Risk
Missing Protection against Signature Replay Attacks	Complete	Complete	Low / No Risk
Weak Sources of Randomness from Chain Attributes	Complete	Complete	Low / No Risk

Vulnerability	Automatic Scan	Manual Scan	Result
Authorization through tx.origin	Complete	Complete	Low / No Risk
Delegatecall to Untrusted Callee	Complete	Complete	Low / No Risk
Use of Deprecated Solidity Functions	Complete	Complete	Low / No Risk
Assert Violation	Complete	Complete	Low / No Risk
Reentrancy	Complete	Complete	Low / No Risk
Unprotected SELFDESTRUCT Instruction	Complete	Complete	Low / No Risk
Unprotected Ether Withdrawal	Complete	Complete	Low / No Risk
Unchecked Call Return Value	Complete	Complete	Low / No Risk
Outdated Compiler Version	Complete	Complete	Low / No Risk
Integer Overflow and Underflow	Complete	Complete	Low / No Risk
Function Default Visibility	Complete	Complete	Low / No Risk

Contract Ownership

The contract ownership of BJcoin is not currently renounced. The ownership of the contract grants special powers to the protocol creators, making them the sole addresses that can call sensible ownable functions that may alter the state of the protocol.

The current owner is the address 0xa9bA6265D5a11B91579fEFA26D7F458eA89a744d which can be viewed from:
HERE

The owner wallet has the power to call the functions displayed on the priviliged functions chart below, if the owner wallet is compromised this privileges could be exploited.

We recommend the team to renounce ownership at the right timing if possible, or gradually migrate to a timelock with governing functionalities in respect of transparency and safety considerations.

Important Notes To The Users:

- The owner cannot mint tokens after intial deployment.
- The owner cannot stop Trading.
- The onwer can regain ownership after lock.
- Once the owner renounces ownership of the contract, none of the following are applicable.
- The owner can change the liquidity, funding, burn, and tax fee with no restrictions.
- The owner can add/remove addresses from fees and rewards.
- The owner can change the max tx amount with no restrictions.
- No high-risk Exploits/Vulnerabilities Were Found in token Source Code other than owner privileges

Audit Passed

Findings Summary

Classification of Issues

Severity	Description
High	Exploits, vulnerabilities or errors that will certainly or probabilistically lead towards loss of funds, control, or impairment of the contract and its functions. Issues under this classification are recommended to be fixed with utmost urgency
Medium	Bugs or issues with that may be subject to exploit, though their impact is somewhat limited.Issues under this classification are recommended to be fixed as soon as possible.
Low	Effects are minimal in isolation and do not pose a significant danger to the project or its users. Issues under this classification are recommended to be fixed nonetheless.
Info	Consistency, syntax or style best practices. Generally pose a negligible level of risk, if any.

Findings

Severity	Found
High	0
Medium	2
Low	1
Info	4
Total	7

Findings

Possible to gain ownership after renouncing the contract ownership

ID	Severity	Contract	Function
01	Medium	BJcoin	function lock(uint256 time) public virtual onlyOwner && function unlock()

Description

Logical Issue, Privilege. An owner can regain ownership even after renouncing to it. If an owner calls the lock function his address is saved in the _previousOwner variable. Then, if after renouncing ownership the _previousOwner calls the unlock function the owner of the contract is set to address of _previousOwner.

Recommendation

We advise updating/removing lock and unlock functions in the contract as this functions logic voids the point of renouncing ownership.

Owner can reclaim ownership immediately after the lock

ID	Severity	Contract	Function
02	Medium	BJcoin	function function unlock()

Description

Logical Issue, Privilege. Once the onwer calls the lock function _lockTime is set with the current time plus a an extra time, the unlock() function checks if the caller is the previous owner (this has security implications stated above) and has a require statement 'require(now < _lockTime);' the comparion is wrong. The previous owner can regain ownership while the current timestamp is less than the _lockTime. This leads to the owner being able to reclaim ownership immediately after the ownership was locked. Also if the owner does not reclaim before lockTime is less than the current timestamp, they could never unlock.

Recommendation

We advise updating/removing lock and unlock functions in the contract as this functions logic voids the point of renouncing ownership.

Variables could be declared as constant

ID	Severity	Contract	Function
03	Informational	BJcoin	variables _decimals, _name, _symbol, _tTotal, numTokensSellToAddToLiquidity

Description

Gas Optimization. Variables that are never changed could be declared as constant.

Recommendation

We recommend declaring those variables as constant.

Division before Multiplication

ID	Severity	Contract	Function
04	Low	BJcoin	function _tokenTransfer()

Description

Precision Loss. 'fundingPiece = fundingAmt.div(7) => _transferStandard(sender,charityWallet,fundingPiece.mul(5))' Division before multiplication can result in truncation and less accurate results

Recommendation

Multiplication should be performed before division to not lose precision.

Public function that could be declared external

ID	Severity	Contract	Function
05	Informational	BJcoin	Functions renounceOwnership, transferOwnership, geUnlockTime, lock, unlock, excludeFromReward, excludeFromFee, includeInFee, setSwapAndLiquifyEnabled

Description

Gas Optimization. Public function that could be declared external

Recommendation

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

Missing events arithmetic

ID	Severity	Contract	Function
06	Informational	BJcoin	Missing events for setLiqFee, setFundingFee, setTaxFee, setBurnFee, setMaxTxPercent

Description

Functions that change critical arithmetic parameters should emit an event.

Recommendation

Emit corresponding events for critical parameter changes.

Too many digits

ID	Severity	Contract	Function
07	Informational	BJcoin	Variables _tTotal, _maxTxAmount

Description

Literals with many digits are difficult to read and review.

Recommendation

Make use of scientific notation, use underscores, and/or use ether suffix.

Priviliged Functions (onlyOwner)

Function Name	Parameters	Visibility
renounceOwnership	none	public
transferOwnership	address newOwner	public
lock	uint256 time	public
excludeFromReward	address account	public
includeInReward	address account	external
swapAndLiquify	none	private
excludeFromFee	address account	public
includeInFee	address account	public
setdevWalletWallet	address newWallet	external
setcharityWalletWallet	address newWallet	external
setLiqFee	uint256 newVal	external
setFundingFee	uint256 newVal	external
setTaxFee	uint256 newVal	external
setBurnFee	uint256 newVal	external
setMaxTxPercent	uint256 maxTxPercent	external
setSwapAndLiquifyEnabled	bool _enabled	public

Statistics

Liquidity Info

Parameter	Result
Pair Address	0xB78D617b3CD363B0E0c187351b6341330C4b89cF
BJ coin Reserves	0.00 BJ coin
BNB Reserves	0.00 BNB
Liquidity Value	$0 USD

Token (BJ coin) Holders Info

Parameter	Result
BJ coin Percentage Burnt	0.00%
BJ coin Amount Burnt	0 BJ coin
Top 10 Percentage Own	100.00%
Top 10 Amount Owned	2,000,000 BJ coin
Top 10 Aprox Value	$NaN USD

LP (BJ coin/BNB) Holders Info

Parameter	Result
BJ coin/BNB % Burnt	0.00%
BJ coin/BNB Amount Burnt	0 BJ coin
Top 10 Percentage Owned	0.00%
Top 10 Amount Owned	0 BJ coin
Locked Tokens Percentage	0.00%
Locked Tokens Amount	0 BJ coin

* All the data diplayed above was taken on-chain at block 16919174
* The tokens on industry-standard burn wallets are not included on the top 10 wallets calculations

Liquidity Ownership

The token does not have liquidity at the moment of the audit, block 16919174

KISHIELD

Disclaimer

KISHIELD has conducted an independent audit to verify the integrity of and highlight any vulnerabilities or errors, intentional or unintentional, that may be present in the codes that were provided for the scope of this audit. This audit report does not constitute agreement, acceptance or advocation for the Project that was audited, and users relying on this audit report should not consider this as having any merit for financial advice in any shape, form or nature. The contracts audited do not account for any economic developments that may be pursued by the Project in question, and that the veracity of the findings thus presented in this report relate solely to the proficiency, competence, aptitude and discretion of our independent auditors, who make no guarantees nor assurance that the contracts are completely free of exploits, bugs, vulnerabilities or deprecation of technologies.

All information provided in this report does not constitute financial or investment advice, nor should it be used to signal that any persons reading this report should invest their funds without sufficient individual due diligence regardless of the findings presented in this report. Information is provided ‘as is’, and KISHIELD is under no covenant to the completeness, accuracy or solidity of the contracts audited. In no event will KISHIELD or its partners, employees, agents or parties related to the provision of this audit report be liable to any parties for, or lack thereof, decisions and/or actions with regards to the information provided in this audit report.

The assessment services provided by KISHIELD is subject to dependencies and under continuing development. You agree that your access and/or use, including but not limited to any services, reports, and materials, will be at your sole risk on an as-is, where-is, and as-available basis. Cryptographic tokens are emergent technologies and carry with them high levels of technical risk and uncertainty. The assessment reports could include false positives, false negatives, and other unpredictable results. The services may access, and depend upon, multiple layers of third-parties.