KISHIELD

Security Audit

Pitano Token

April 13, 2022

Table of Contents

Audit Summary

This report has been prepared for Pitano 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	0xE833CF71263F79cF95E22bD74c60A6706e4651e3
Name	Pitano
Token Tracker	Pitano (PITANO)
Decimals	18
Supply	4,000,000,000
Platform	Binance Chain
compiler	v0.7.4+commit.3f05b770
Optimization	Yes with 200 runs
LicenseType	None
Language	Solidity
Codebase	https://bscscan.com/address/0xE833CF71263F79cF95E22bD74c60A6706e4651e3
Url	https://pitano.network

Main Contract Assessed

Name	Contract	Live
Pitano	0xE833CF71263F79cF95E22bD74c60A6706e4651e3	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
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 Pitano 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 0xf4F0E6eDaCcaD13071d1564F9B283F6fB4231663 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 transfer function is implemented correctly.
- Transfer is only allowed once initialDistributionFinished is set to true.
- The owner cannot stop Trading.
- The owner cannot change the max tx amount.
- The owner cannot set the fees over 25%.
- Any address with minterRole can add/remove new minters and mint new tokens.
- Team states that the mint function is used by the rebase mechanism.
- Once the owner renounces ownership of the contract, none of the following are applicable.
- Owner can add and remove WALLETS from the blacklist.
- Owner can add allow wallets to transfer before initialDistributionFinished.
- Owner can set wallets for fee exempt.
- Owner has minterRole and can mint new tokens.
- Owner can transfer BNB and tokens stuck on the contract.

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	0
Low	1
Info	3
Total	4

Findings

Public function that could be declared external

ID	Severity	Contract	Function
01	Informational	Pitano	Functions updateBlacklist, rescueToken, renounceMinter

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.

Division before Multiplication

ID	Severity	Contract	Function
02	Low	Pitano	function swapBack()

Description

Precision Loss. 'contractTokenBalance = _gonBalances[address(this)].div(_gonsPerFragment) => contractTokenBalance.mul(dynamicLiquidityFee).div(totalFee).div(2)' Division before multiplication can result in truncation and less accurate results

Recommendation

Multiplication should be performed before division to not lose precision.

Missing events arithmetic

ID	Severity	Contract	Function
03	Informational	Pitano	Missing events for mint, setSwapBackSettings, setTargetLiquidity, setFees

Description

Functions that change critical arithmetic parameters should emit an event.

Recommendation

Emit corresponding events for critical parameter changes.

Unused Private Function

ID	Severity	Contract	Function
04	Informational	Pitano	functions transferToAddressETH()

Description

These functions are private but never used by the contract logic.

Recommendation

We recommend deleting this function or setting the visibility to external if they are meant to be used.

Priviliged Functions (onlyOwner)

Function Name	Parameters	Visibility
updateBlacklist	address _user, bool _flag	public
rebase	uint256 epoch, int256 supplyDelta	external
transfer	none	external
transfer	none	external
setLP	address _address	external
transferFrom	none	external
swapBack	none	internal
decreaseAllowance	none	external
increaseAllowance	none	external
approve	none	external
setInitialDistributionFinished	none	external
enableTransfer	address _addr	external
setFeeExempt	address _addr	external
mint	none	external
setSwapBackSettings	bool _enabled, uint256 _num, uint256 _denom	external
setTargetLiquidity	uint256 target, uint256 accuracy	external
addMinter	address account	public

Function Name	Parameters	Visibility
removeMinter	address account	public
sendPresaleToken	calldata recipients, calldata values	external
setFeeReceivers	address _autoLiquidityReceiver, address _TreasuryReceiver, address _RiskFreeValueReceiver	external
setFees	uint256 _liquidityFee, uint256 _RiskFreeValue, uint256 _Treasury, uint256 _sellFee, uint256 _feeDenominator	external
clearStuckBalance	uint256 amountPercentage, address adr	external
rescueToken	address tokenAddress, uint256 tokens	public

Statistics

Liquidity Info

Parameter	Result
Pair Address	0xB7607cBC70C9893A1A6c23aE381bD3b241A47e0C
PITANO Reserves	0.00 PITANO
BNB Reserves	0.00 BNB
Liquidity Value	$0 USD

Token (PITANO) Holders Info

Parameter	Result
PITANO Percentage Burnt	0.00%
PITANO Amount Burnt	0 PITANO
Top 10 Percentage Own	100.00%
Top 10 Amount Owned	4,000,000,000 PITANO
Top 10 Aprox Value	$NaN USD

LP (PITANO/BNB) Holders Info

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

* All the data diplayed above was taken on-chain at block 16913930
* 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 16913930

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.