AuditAce
FROM INCEPTION TO SUCCESS

Smart Contract Audit

FOR

POCHITA

DATED : 6 June 23'

FUNCTIONAL TESTING

Centralization – Trades must be enabled

Severity: High

function: EnableTrading

Status: Resovled (owned by safu developer)

Overview:

The smart contract owner must enable trades for holders. If trading remain disabled, no one would be able to buy/sell/transfer tokens.

```
function EnableTrading() external onlyOwner {
    require(!tradingEnabled, "Cannot re-enable trading");
    tradingEnabled = true;
    swapEnabled = true;
    genesis_block = block.number;
}
```

Suggestion

To mitigate this centralization issue, we propose the following options:

1. Renounce Ownership: Consider relinquishing control of the smart contract by renouncing ownership. This would remove the ability for a single entity to manipulate the router, reducing centralization risks.
2. Multi-signature Wallet: Transfer ownership to a multi-signature wallet. This would require multiple approvals for any changes to the mainRouter, adding an additional layer of security and reducing the centralization risk.
3. Transfer ownership to a trusted and valid 3rd party in order to guarantee enabling of the trades

AUDIT SUMMARY

Project name – POCHITA

Date: 6 June, 2023

Scope of Audit- Audit Ace was consulted to conduct the smart contract audit of the solidity source codes.

Audit Status: Passed

Issues Found

Status	Critical	High	Medium	Low	Suggestion
Open	0	0	0	0	0
Acknowledged	0	0	0	0	0
Resolved	0	1	0	0	0

USED TOOLS

Tools:

1- Manual Review:
A line by line code review has been performed by audit ace team.

2- BSC Test Network: All tests were conducted on the BSC Test network, and each test has a corresponding transaction attached to it. These tests can be found in the "Functional Tests" section of the report.

3- Slither :
The code has undergone static analysis using Slither.

Testnet version:
Contract has been tested on binance smart chain testnet which can be found in below link:
https://testnet.bscscan.com/token/0xcae191a63de3ff60d9ca03230d773f1e1155aa1b

Token Information

Token Name : Pochita Inu

Token Symbol: POCHITA

Decimals: 18

Token Supply: 1,000,000,000,000

Token Address:
0x56F41E03dDb2345736c63F2C3a92c12f6aEd9B56

Checksum:
0d0e6bc06f515a1ad622d942af16c4611db4d8b9

Owner:
0x21BF0d263A8c9528D4379b881db49b72c09acBDd
(at time of writing the audit)

Deployer:
0x21BF0d263A8c9528D4379b881db49b72c09acBDd

TOKEN OVERVIEW

Fees:

Buy Fees: 2%

Sell Fees: 2%

Transfer Fees: 2%

Fees Privilege: Static fees

Ownership: Owned (safu developer for 14 days)

Minting: None

Max Tx Amount/ Max Wallet Amount: No

Blacklist: No

Other Privileges: - changing swap threshold

- enabling trades

- initial distribution of the tokens

AUDIT METHODOLOGY

The auditing process will follow a routine as special considerations by Auditace:

- Review of the specifications, sources, and instructions provided to Auditace to make sure the contract logic meets the intentions of the client without exposing the user's funds to risk.
- Manual review of the entire codebase by our experts, which is the process of reading source code line-by-line in an attempt to identify potential vulnerabilities.
- Specification comparison is the process of checking whether the code does what the specifications, sources, and instructions provided to Auditace describe.
- Test coverage analysis determines whether the test cases are covering the code and how much code isexercised when we run the test cases.
- Symbolic execution is analysing a program to determine what inputs cause each part of a program to execute.
- Reviewing the codebase to improve maintainability, security, and control based on the established industry and academic practices.

VULNERABILITY CHECKLIST

- [x] Return values of low-level calls
- [x] Private modifier
- [x] Multiple Sends
- [x] Using Suicide
- [x] Gas Limitand Loops
- [x] Address hardcoded
- [x] Exception Disorder
- [x] Using inline assembly
- [x] Divide before multiply
- [x] Missing Zero Address Validation
- [x] Compiler version not fixed
- [x] **Gasless Send**
- [x] Using block.timestamp
- [x] Re-entrancy
- [x] Tautology or contradiction
- [x] Timestamp Dependence
- [x] Revert/require functions
- [x] Use of tx.origin
- [x] Integer overflow/underflow
- [x] Dangerous strict equalities
- [x] Using SHA3
- [x] Using throw

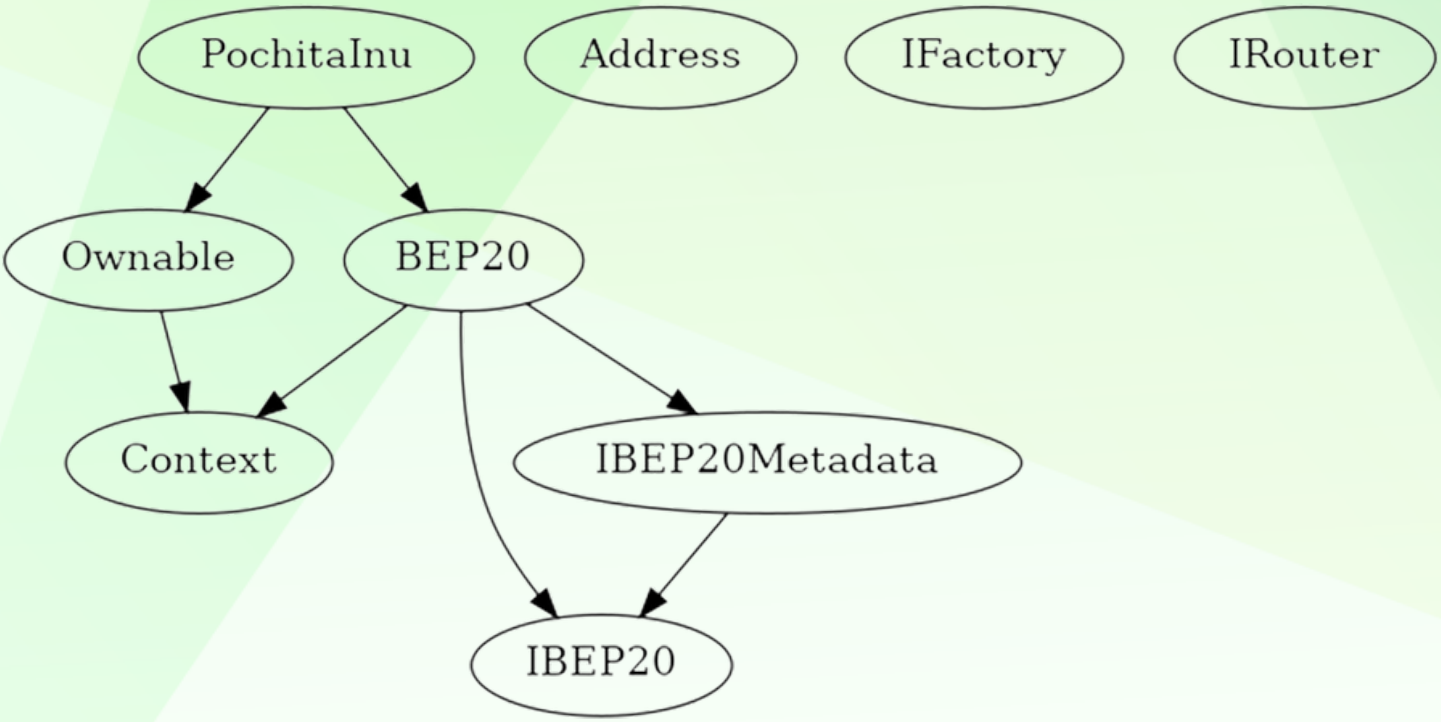
CLASSIFICATION OF RISK

Severity	Description
Critical	These vulnerabilities could be exploited easily and can lead to asset loss, data loss, asset, or data manipulation. They should be fixed right away.
High-Risk	A vulnerability that affects the desired outcome when using a contract, or provides the opportunity to use a contract in an unintended way.
Medium-Risk	A vulnerability that could affect the desired outcome of executing the contract in a specific scenario.
Low-Risk	A vulnerability that does not have a significant impact on possible scenarios for the use of the contract and is probably subjective.
Gas Optimization /Suggestion	A vulnerability that has an informational character but is not affecting any of the code.

Findings

Severity	Found
Critical	0
High-Risk	1
Medium-Risk	0
Low-Risk	0
Gas Optimization / Suggestions	0

INHERITANCE TREE



POINTS TO NOTE

- owner is not able to set change buy/sell/transfer fees (2% static)
- owner is not able to blacklist an arbitrary wallet
- owner is not able to set limit for buy/sell/transfer/holding amounts
- owner is not able to mint new tokens
- owner is not able to disable trades
- owner can exclude/include an address from fees
- owner can change internal swap thershold
- owner can enable/disable internal swap (I.e marketing BNB and auto-liquidity, not trades)
- owner can claim stuck tokens
- owner can exclude/include an address from rewards
- owner can transfer ownership
- owner can renounce ownership

CONTRACT ASSESMENT

Contract	Type	Bases		
└	**Function Name**	**Visibility**	**Mutability**	**Modifiers**
Context	Implementation			
└	_msgSender	Internal 🔒		
└	_msgData	Internal 🔒		
IBEP20	Interface			
└	totalSupply	External ❗		NO ❗
└	balanceOf	External ❗		NO ❗
└	transfer	External ❗	🛑	NO ❗
└	allowance	External ❗		NO ❗
└	approve	External ❗	🛑	NO ❗
└	transferFrom	External ❗	🛑	NO ❗
IBEP20Metadata	Interface	IBEP20		
└	name	External ❗		NO ❗
└	symbol	External ❗		NO ❗
└	decimals	External ❗		NO ❗
BEP20	Implementation	Context, IBEP20, IBEP20Metadata		
└	<Constructor>	Public ❗	🛑	NO ❗
└	name	Public ❗		NO ❗
└	symbol	Public ❗		NO ❗
└	decimals	Public ❗		NO ❗
└	totalSupply	Public ❗		NO ❗
└	balanceOf	Public ❗		NO ❗
└	transfer	Public ❗	🛑	NO ❗
└	allowance	Public ❗		NO ❗
└	approve	Public ❗	🛑	NO ❗
└	transferFrom	Public ❗	🛑	NO ❗
└	increaseAllowance	Public ❗	🛑	NO ❗
└	decreaseAllowance	Public ❗	🛑	NO ❗
└	_transfer	Internal 🔒	🛑	
└	_tokengeneration	Internal 🔒	🛑	
└	_approve	Internal 🔒	🛑	
Address	Library			
└	sendValue	Internal 🔒	🛑	
Ownable	Implementation	Context		

CONTRACT ASSESMENT

└	<Constructor>	Public ❗	🔴	NO ❗
└	owner	Public ❗			NO ❗
└	renounceOwnership	Public ❗	🔴	onlyOwner
└	transferOwnership	Public ❗	🔴	onlyOwner
└	_setOwner	Private 🔐	🔴	
IFactory	Interface			
└	createPair	External ❗	🔴	NO ❗
IRouter	Interface			
└	factory	External ❗			NO ❗
└	WETH	External ❗			NO ❗
└	addLiquidityETH	External ❗	💸	NO ❗
└	swapExactTokensForETHSupportingFeeOnTransferTokens	External ❗	🔴	NO ❗
PochitaInu	Implementation	BEP20, Ownable		
└	<Constructor>	Public ❗	🔴	BEP20
└	approve	Public ❗	🔴	NO ❗
└	transferFrom	Public ❗	🔴	NO ❗
└	increaseAllowance	Public ❗	🔴	NO ❗
└	decreaseAllowance	Public ❗	🔴	NO ❗
└	transfer	Public ❗	🔴	NO ❗
└	_transfer	Internal 🔒	🔴	
└	Liquify	Private 🔐	🔴	lockTheSwap
└	swapTokensForETH	Private 🔐	🔴	
└	addLiquidity	Private 🔐	🔴	
└	updateLiquidityProvide	External ❗	🔴	onlyOwner
└	updateLiquidityTreshhold	External ❗	🔴	onlyOwner
└	EnableTrading	External ❗	🔴	onlyOwner
└	updatedeadline	External ❗	🔴	onlyOwner
└	updateMarketingWallet	External ❗	🔴	onlyOwner
└	AddExemptFee	External ❗	🔴	onlyOwner
└	RemoveExemptFee	External ❗	🔴	onlyOwner
└	AddExemptFee	External ❗	🔴	onlyOwner
└	RemoveExemptFee	External ❗	🔴	onlyOwner
└	rescueBNB	External ❗	🔴	onlyOwner
└	rescueBSC20	External ❗	🔴	onlyOwner
└	<Receive Ether>	External ❗	💸	NO ❗

CONTRACT ASSESMENT

Legend

Symbol	Meaning
	Function can modify state
	Function is payable

STATIC ANALYSIS

```
Reentrancy in PochitaInu.transferFrom(address,address,uint256) (contracts/Token.sol#421-429):
        External calls:
        - _transfer(sender,recipient,amount) (contracts/Token.sol#422)
                - router.addLiquidityETH{value: ethAmount}(address(this),tokenAmount,0,0,deadWallet,block.timestamp) (contracts/Token.sol#553-560)
                - (success) = recipient.call{value: amount}() (contracts/Token.sol#296)
                - router.swapExactTokensForETHSupportingFeeOnTransferTokens(tokenAmount,0,path,address(this),block.timestamp) (contracts/Token.sol#545)
                - address(marketingWallet).sendValue(marketingAmt) (contracts/Token.sol#531)
        External calls sending eth:
        - _transfer(sender,recipient,amount) (contracts/Token.sol#422)
                - router.addLiquidityETH{value: ethAmount}(address(this),tokenAmount,0,0,deadWallet,block.timestamp) (contracts/Token.sol#553-560)
                - (success) = recipient.call{value: amount}() (contracts/Token.sol#296)
        Event emitted after the call(s):
        - Approval(owner,spender,amount) (contracts/Token.sol#288)
                - _approve(sender,_msgSender(),currentAllowance - amount) (contracts/Token.sol#426)
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#reentrancy-vulnerabilities-3

Context._msgData() (contracts/Token.sol#27-30) is never used and should be removed
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#dead-code

Pragma version^0.8.17 (contracts/Token.sol#20) necessitates a version too recent to be trusted. Consider deploying with 0.6.12/0.7.6/0.8.16
solc-0.8.20 is not recommended for deployment
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#incorrect-versions-of-solidity

Low level call in Address.sendValue(address,uint256) (contracts/Token.sol#293-298):
        - (success) = recipient.call{value: amount}() (contracts/Token.sol#296)
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#low-level-calls

Variable BEP20._balances (contracts/Token.sol#69) is not in mixedCase
Variable BEP20._allowances (contracts/Token.sol#71) is not in mixedCase
Function IRouter.WETH() (contracts/Token.sol#342) is not in mixedCase
Function PochitaInu.Liquify(uint256,PochitaInu.Taxes) (contracts/Token.sol#500-534) is not in mixedCase
Parameter PochitaInu.updateLiquidityTreshhold(uint256).new_amount (contracts/Token.sol#568) is not in mixedCase
Function PochitaInu.EnableTrading() (contracts/Token.sol#575-580) is not in mixedCase
Parameter PochitaInu.updatedeadline(uint256)._deadline (contracts/Token.sol#582) is not in mixedCase
Function PochitaInu.AddExemptFee(address) (contracts/Token.sol#593-595) is not in mixedCase
Parameter PochitaInu.AddExemptFee(address)._address (contracts/Token.sol#593) is not in mixedCase
Function PochitaInu.RemoveExemptFee(address) (contracts/Token.sol#597-599) is not in mixedCase
Parameter PochitaInu.RemoveExemptFee(address)._address (contracts/Token.sol#597) is not in mixedCase
Function PochitaInu.AddExemptFee(address[]) (contracts/Token.sol#601-605) is not in mixedCase
Function PochitaInu.RemoveExemptFee(address[]) (contracts/Token.sol#607-611) is not in mixedCase
Variable PochitaInu.genesis_block (contracts/Token.sol#374) is not in mixedCase
Constant PochitaInu.deadWallet (contracts/Token.sol#379) is not in UPPER_CASE_WITH_UNDERSCORES
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#conformance-to-solidity-naming-conventions

Redundant expression "this (contracts/Token.sol#28)" inContext (contracts/Token.sol#22-31)
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#redundant-statements

PochitaInu.launchtax (contracts/Token.sol#376) should be constant
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#state-variables-that-could-be-declared-constant

PochitaInu.pair (contracts/Token.sol#366) should be immutable
PochitaInu.router (contracts/Token.sol#365) should be immutable
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#state-variables-that-could-be-declared-immutable
```

Result => A static analysis of contract's source code has been performed using slither,

No major issues were found in the output

FUNCTIONAL TESTING

1- Adding liquidity (passed):

https://testnet.bscscan.com/tx/0x7b2d2b9418bd0ad5d3d71d014c6d00949a24ae8110827e18a6c5071384843e6c

2- Buying when excluded from fees (0% tax) (passed):

https://testnet.bscscan.com/tx/0xa35508be9577c0c899f622c247f9d4a71654020a83e6d88cebc60076eacdf6c6

3- Selling when excluded from fees (0% tax) (passed):

https://testnet.bscscan.com/tx/0x2403205d02a14b6bd33dfab2dfefcd1a97c79a57df61ceb5854d87172b447b3b

4- Transferring when excluded from fees (0% tax) (passed):

https://testnet.bscscan.com/tx/0x2e5f9452ce673d962f08984f5d8007fb476fbbfa817ae30165d93b817a6299e1

5- Buying when not excluded from fees (2% tax) (passed):

https://testnet.bscscan.com/tx/0xd49b125dba4c7953145ca4f21eac849fb0e3389f557a8ef22c119e45fb91644c

6- Selling when not excluded from fees (2% tax) (passed):

https://testnet.bscscan.com/tx/0x406b0952041141a4a875e2d0b623b83128dc6e37cae13e950d7e030d1b67a5a1

FUNCTIONAL TESTING

7- Transferring when not excluded from fees (2% tax) (passed):

https://testnet.bscscan.com/tx/0xe56697319e053de60482d5f466e1116cc4aae395f434f04c7f251c232243da68

8- Auto liquidity, Marketing fee (passed):

https://testnet.bscscan.com/tx/0x406b0952041141a4a875e2d0b623b83128dc6e37cae13e950d7e030d1b67a5a1

FUNCTIONAL TESTING

Centralization – Trades must be enabled

Severity: High

function: EnableTrading

Status: Resovled (owned by safu developer)

Overview:

The smart contract owner must enable trades for holders. If trading remain disabled, no one would be able to buy/sell/transfer tokens.

```
function EnableTrading() external onlyOwner {
    require(!tradingEnabled, "Cannot re-enable trading");
    tradingEnabled = true;
    swapEnabled = true;
    genesis_block = block.number;
}
```

Suggestion

To mitigate this centralization issue, we propose the following options:

1. Renounce Ownership: Consider relinquishing control of the smart contract by renouncing ownership. This would remove the ability for a single entity to manipulate the router, reducing centralization risks.
2. Multi-signature Wallet: Transfer ownership to a multi-signature wallet. This would require multiple approvals for any changes to the mainRouter, adding an additional layer of security and reducing the centralization risk.
3. Transfer ownership to a trusted and valid 3rd party in order to guarantee enabling of the trades

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

ABOUT AUDITACE

We specializes in providing thorough and reliable audits for Web3 projects. With a team of experienced professionals, we use cutting-edge technology and rigorous methodologies to evaluate the security and integrity of blockchain systems. We are committed to helping our clients ensure the safety and transparency of their digital assets and transactions.

https://auditace.tech/

https://t.me/Audit_Ace

https://twitter.com/auditace_

https://github.com/Audit-Ace