auditace.tech

AuditAce

FROM INCEPTION TO SUCCESS

Smart Contract Audit

FOR

Laika Inu

DATED : 18 Apr 23'

AUDIT SUMMARY

Project name – Laika Inu

Date: 18 April, 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	1	0	0
Acknowledged	0	0	0	0	0
Resolved	0	0	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 done on BSC Test network, each test has its transaction has attached to it.

3- Slither : Static Analysis

Testnet Link: all tests were done using this contract, tests are done on BSC Testnet

https://testnet.bscscan.com/address/0x917B82143055c1a4dFaD59184d67A015DfC94Fd7

Token Information

Token Name : Laika Inu

Token Symbol: LKI

Decimals: 9

Token Supply: 420,000,000,000,000,000

Token Address:
0x2921E2CEf9a1EF9024aD64326F89e6FdD786Ae40

Checksum:
3847c2879d783db21e83b6658dd6191d4649441e

Owner:
0xD315d294238D9e5164d9336C80541E883F1058aC
(at time of audit)

Deployer:
0xD315d294238D9e5164d9336C80541E883F1058aC

TOKEN OVERVIEW

Fees:

Buy Fees: 10%

Sell Fees: 10%

Transfer Fees: 10%

Fees Privilige: None

Ownership : Owned

Minting: No mint function

Max Tx Amount/ Max Wallet Amount: No

Blacklist: No

Other Priviliges: excluding from fees - including in fees - changing swap threshold

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.

auditace.tech

VULNERABILITY CHECKLIST

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

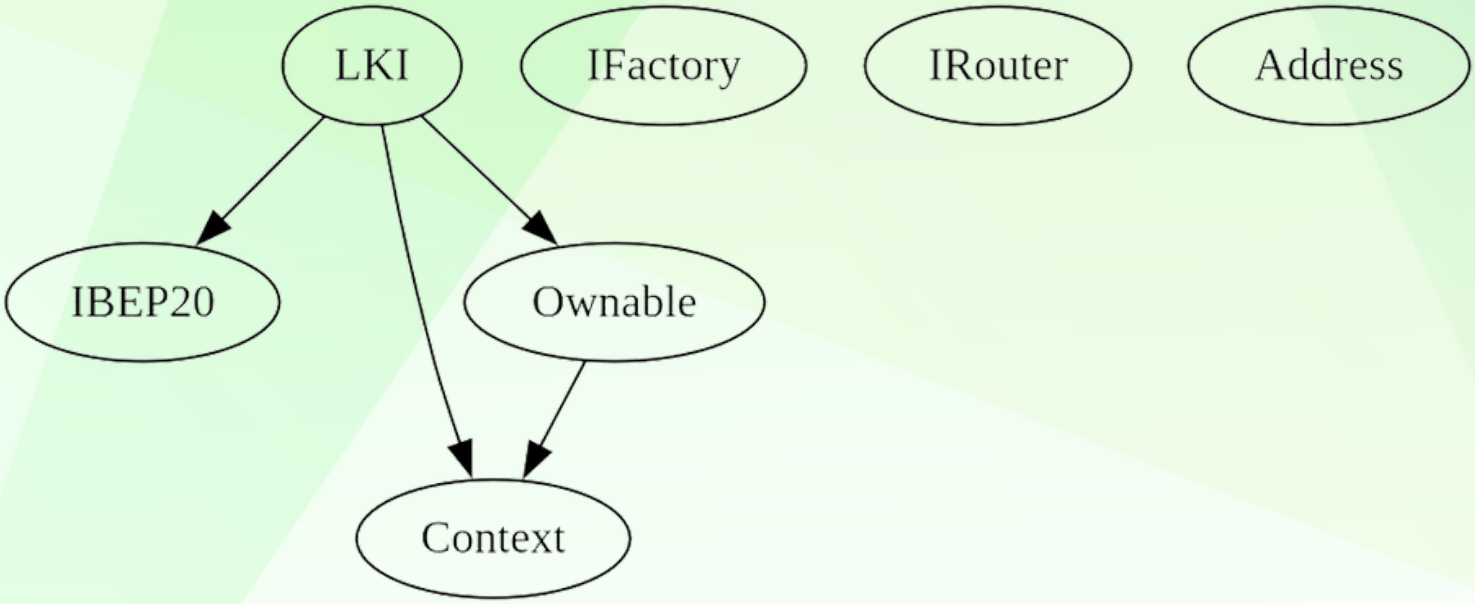
CLASSIFICATION OF RISK

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	0
Medium-Risk	1
Low-Risk	0
Gas Optimization / Suggestions	0

INHERITANCE TREE



POINTS TO NOTE

- Owner is not able to modify fees (10% buy/sell/transfers)
- Owner must enable trading for investors to be able to trade
- Owner is not able to set max buy/sell/transfer/hold amount
- Owner is not able to blacklist an arbitrary wallet
- Owner is not able to disable trades
- Owner is not able to mint new tokens

CONTRACT ASSESMENT

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

CONTRACT ASSESMENT

└	allowance	Public ❗		NO❗
└	approve	Public ❗	🛑	NO❗
└	transferFrom	Public ❗	🛑	NO❗
└	increaseAllowance	Public ❗	🛑	NO❗
└	decreaseAllowance	Public ❗	🛑	NO❗
└	transfer	Public ❗	🛑	NO❗
└	isExcludedFromReward	Public ❗		NO❗
└	reflectionFromToken	Public ❗		NO❗
└	tokenFromReflection	Public ❗		NO❗
└	excludeFromReward	Public ❗	🛑	onlyOwner
└	includeInReward	External ❗	🛑	onlyOwner
└	excludeFromFee	Public ❗	🛑	onlyOwner
└	includeInFee	Public ❗	🛑	onlyOwner
└	isExcludedFromFee	Public ❗		NO❗
└	_reflectRfi	Private 🔐	🛑	
└	_takeMarketing	Private 🔐	🛑	
└	_getValues	Private 🔐		
└	_getTValues	Private 🔐		
└	_getRValues	Private 🔐		
└	_getRate	Private 🔐		
└	_getCurrentSupply	Private 🔐		
└	_approve	Private 🔐	🛑	
└	_transfer	Private 🔐	🛑	
└	_tokenTransfer	Private 🔐	🛑	
└	swapAndLiquify	Private 🔐	🛑	lockTheSwap
└	swapTokensForBNB	Private 🔐	🛑	
└	bulkExcludeFee	External ❗	🛑	onlyOwner
└	updateMarketingWallet	External ❗	🛑	onlyOwner
└	updateSwapTokensAtAmount	External ❗	🛑	onlyOwner
└	rescueBNB	External ❗	🛑	onlyOwner
└	rescueAnyBEP20Tokens	Public ❗	🛑	onlyOwner
└	<Receive Ether>	External ❗	💵	NO❗

Legend

Symbol	Meaning
🛑	Function can modify state
💵	Function is payable

STATIC ANALYSIS

```
Reentrancy in LKI.transferFrom(address,address,uint256) (contracts/Token.sol#258-273):
        External calls:
        - _transfer(sender,recipient,amount) (contracts/Token.sol#263)
                - (success) = recipient.call{value: amount}() (contracts/Token.sol#131)
                - router.swapExactTokensForETHSupportingFeeOnTransferTokens(tokenAmount,0,path,address(this),block.timestamp) (contracts/Token.sol#543-549)
                - address(marketingWallet).sendValue(deltaBalance) (contracts/Token.sol#530)
        External calls sending eth:
        - _transfer(sender,recipient,amount) (contracts/Token.sol#263)
                - (success) = recipient.call{value: amount}() (contracts/Token.sol#131)
        Event emitted after the call(s):
        - Approval(owner,spender,amount) (contracts/Token.sol#468)
                - _approve(sender,_msgSender(),currentAllowance - amount) (contracts/Token.sol#270)
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#reentrancy-vulnerabilities-3

LKI.includeInReward(address) (contracts/Token.sol#348-359) has costly operations inside a loop:
        - _excluded.pop() (contracts/Token.sol#355)
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#costly-operations-inside-a-loop

Context._msgData() (contracts/Token.sol#45-48) is never used and should be removed
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#dead-code

LKI._rTotal (contracts/Token.sol#159) is set pre-construction with a non-constant function or state variable:
        - (MAX - (MAX % _tTotal))
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#function-initializing-state

Pragma version^0.8.17 (contracts/Token.sol#6) necessitates a version too recent to be trusted. Consider deploying with 0.6.12/0.7.6/0.8.16
solc-0.8.19 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#125-136):
        - (success) = recipient.call{value: amount}() (contracts/Token.sol#131)
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#low-level-calls

Function IRouter.WETH() (contracts/Token.sol#101) is not in mixedCase
Struct LKI.valuesFromGetValues (contracts/Token.sol#183-191) is not in CapWords
Parameter LKI.rescueAnyBEP20Tokens(address,address,uint256)._tokenAddr (contracts/Token.sol#582) is not in mixedCase
Parameter LKI.rescueAnyBEP20Tokens(address,address,uint256)._to (contracts/Token.sol#583) is not in mixedCase
Parameter LKI.rescueAnyBEP20Tokens(address,address,uint256)._amount (contracts/Token.sol#584) is not in mixedCase
Constant LKI._decimals (contracts/Token.sol#155) is not in UPPER_CASE_WITH_UNDERSCORES
Constant LKI._name (contracts/Token.sol#166) is not in UPPER_CASE_WITH_UNDERSCORES
Constant LKI._symbol (contracts/Token.sol#167) 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#46)" inContext (contracts/Token.sol#40-49)
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#redundant-statements

LKI._tTotal (contracts/Token.sol#158) should be constant
LKI.deadWallet (contracts/Token.sol#163) should be constant
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#state-variables-that-could-be-declared-constant

LKI.pair (contracts/Token.sol#153) should be immutable
LKI.router (contracts/Token.sol#152) 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

Router (PCS V2):
0xD99D1c33F9fC3444f8101754aBC46c52416550D1

All the functionalities have been tested, no issues were found

1- Adding liquidity (passed):
https://testnet.bscscan.com/tx/0xa9810837391d4f0326a1cb1537e0fcaa2c4f5d674d288227fd33f08aab70cec2

2- Buying when excluded (0% tax) (passed):
https://testnet.bscscan.com/tx/0x8a2b7db38e4dda21269e6561cb3e044b104e37d34bb62bd4f5b32262b61657ac

3- Selling when excluded (0% tax) (passed):
https://testnet.bscscan.com/tx/0xdb6e2c7001e083ef88f8f0c54501f1a47731d76e6d5a77b9bdf03ab9c4df7a89

4- Transferring when excluded (0% tax) (passed):
https://testnet.bscscan.com/tx/0xfdcd5efb9458d8029fa2315bade79573abcb535af449cb9b7c945516472c23be

5- Buying when not excluded (upto 10% tax) (passed):
https://testnet.bscscan.com/tx/0x25a1d85afa6651a7b1ffed3e65f75bc3bb53a5cb10e1862382df7cd8ee7557c5

6- Selling when not excluded (upto 10% tax) (passed):
https://testnet.bscscan.com/tx/0xb6b961d6abffa494316a9ee0c53225f88e518191283c2d01f3e485b939e8d7a2

FUNCTIONAL TESTING

7- Transferring when not excluded (10% tax) (passed):
https://testnet.bscscan.com/tx/0xdd43f9140709850d4befe97b428560250cad90c8cbd7d11bbf211a4491c621d1

8- Internal swap (passed):
Marketing wallet received BNB
https://testnet.bscscan.com/address/0xc6775a043a41fb16c92f048471e424e3d05e5017#internaltx

MANUAL TESTING

Logical – Invalid condition for updating Swap threshold

Severity: Medium
Function: updateSwapTokensAtAmount
Lines: 529
Status: Not Resolved
Overview:
Current condition indicates that swap threshold must stay less than 1e15 which is 1/420 or 0.2% of supply, however revert error message shows that swap threshold can be set up to 1% of supply

```
function updateSwapTokensAtAmount(uint256 amount) external onlyOwner {
  require(amount <= 1e15, "Cannot set swap threshold amount higher than 1%                    of tokens");
  swapTokensAtAmount = amount * 10**_decimals;
}
```

Recommendation:
change the code to match the condition

```
function updateSwapTokensAtAmount(uint256 amount) external onlyOwner {
  require(amount <= totalSupply() / 100, "Cannot set swap threshold amount higher than 1%            of tokens");
  swapTokensAtAmount = amount * 10**_decimals;
}
```

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