auditace.tech

AuditAce
FROM INCEPTION TO SUCCESS

Smart Contract Audit

FOR

Ketaicoin

DATED : 9 august 23'

MANUAL TESTING

Centralization – Excessive fees

Severity: High

function: updateTax

Status: Not Resolved

Overview:

Owner is able to put upto 50% tax on buy and sells separately.

```
function updateTax(uint256 _buyTax, uint256 _sellTax) external onlyOwner {
  buyTax = _buyTax;
  sellTax = _sellTax;
  totalTax = _buyTax + _sellTax;
  require(buyTax <= 49, "buy Fees cannot exceed 49%");
  require(sellTax <= 49, "buy Fees cannot exceed 49%");
  emit UpdateTax(buyTax, sellTax);
}
```

Suggestion

Consider reducing the upper bound of maximum buy/sell tax. Usually 10% is suggested to be a reasonable upperbound limit for buy/sell/transfer tax.

```
function updateTax(uint256 _buyTax, uint256 _sellTax) external onlyOwner {
  buyTax = _buyTax;
  sellTax = _sellTax;
  totalTax = _buyTax + _sellTax;
  require(buyTax <= 10, "buy Fees cannot exceed 10%");
  require(sellTax <= 10, "buy Fees cannot exceed 10%");
  emit UpdateTax(buyTax, sellTax);
}
```

AUDIT SUMMARY

Project name –Ketaicoin

Date: 9 august, 2023

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

Audit Status: **Passed with High Risk**

Issues Found

Status	Critical	High	Medium	Low	Suggestion
Open	0	1	0	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 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:
The tests were performed using the contract deployed on the BSC Testnet, which can be found at the following address:
https://testnet.bscscan.com/token/0x346616967C2DD603f6f023155182866f90c2c81A

Token Information

Token Name : Ketaicoin

Token Symbol: Ketaicoin

Decimals: 18

Token Supply: 8,000,000

Token Address:
0xEF676F869b3F79A56D31Af069e3B1e53B4116D02

Checksum:
9e2bd80d31502d9e11717b040953c2164fd5bdbf

Owner:
0x7e4b3b0078bF47B98420E86B6Db97BE6CFff25C0
(at time of writing the audit)

Deployer:
0x7e4b3b0078bF47B98420E86B6Db97BE6CFff25C0

TOKEN OVERVIEW

Fees:

Buy Fees: 0-49%

Sell Fees: 0-49%

Transfer Fees: 0%

Fees Privilege: owner

Ownership: owned

Minting: No mint function

Max Tx Amount/ Max Wallet Amount: no

Blacklist: No

Other Privileges: Initial distribution of the tokens modifying fees

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

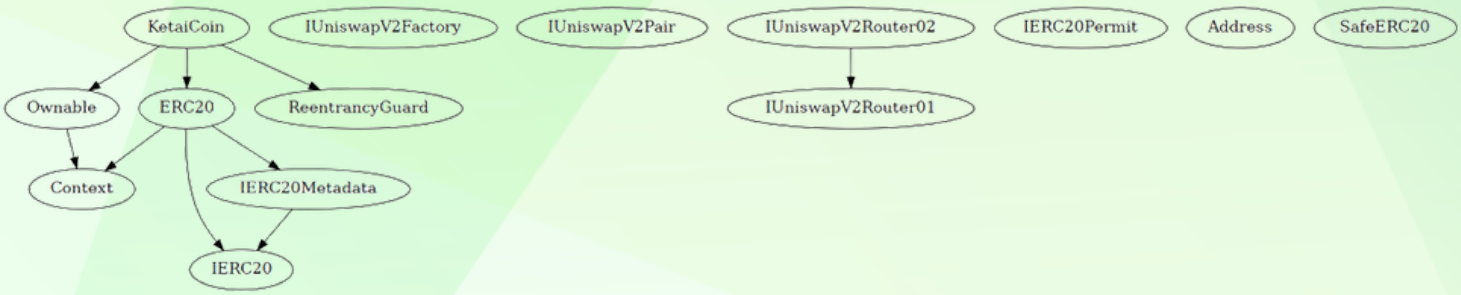
CLASSIFICATION OF RISK

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 able to update buy and sell fees (0-49%)**
- **Owner is not able to set fee on transfers**
- Owner is not able to blacklist an address
- Owner is not able to set maximum wallet and maximum buy/sell limits
- Owner is not able to mint new tokens
- Owner is not able to disable trades

CONTRACT ASSESMENT

Contract	Type	Bases		
└	**Function Name**	**Visibility**	**Mutability**	**Modifiers**
Context	Implementation			
└	_msgSender	Internal 🔒		
└	_msgData	Internal 🔒		
IUniswapV2Factory	Interface			
└	feeTo	External ❗		NO ❗
└	feeToSetter	External ❗		NO ❗
└	getPair	External ❗		NO ❗
└	allPairs	External ❗		NO ❗
└	allPairsLength	External ❗		NO ❗
└	createPair	External ❗	🛑	NO ❗
└	setFeeTo	External ❗	🛑	NO ❗
└	setFeeToSetter	External ❗	🛑	NO ❗
IUniswapV2Pair	Interface			
└	name	External ❗		NO ❗
└	symbol	External ❗		NO ❗
└	decimals	External ❗		NO ❗
└	totalSupply	External ❗		NO ❗
└	balanceOf	External ❗		NO ❗
└	allowance	External ❗		NO ❗
└	approve	External ❗	🛑	NO ❗
└	transfer	External ❗	🛑	NO ❗
└	transferFrom	External ❗	🛑	NO ❗
└	DOMAIN_SEPARATOR	External ❗		NO ❗

CONTRACT ASSESMENT

└	PERMIT_TYPEHASH	External ❗	INO ❗
└	nonces	External ❗	INO ❗
└	permit	External ❗	🛑 INO ❗
└	MINIMUM_LIQUIDITY	External ❗	INO ❗
└	factory	External ❗	INO ❗
└	token0	External ❗	INO ❗
└	token1	External ❗	INO ❗
└	getReserves	External ❗	INO ❗
└	price0CumulativeLast	External ❗	INO ❗
└	price1CumulativeLast	External ❗	INO ❗
└	kLast	External ❗	INO ❗
└	mint	External ❗	🛑 INO ❗
└	burn	External ❗	🛑 INO ❗
└	swap	External ❗	🛑 INO ❗
└	skim	External ❗	🛑 INO ❗
└	sync	External ❗	🛑 INO ❗
└	initialize	External ❗	🛑 INO ❗
||||||			
IUniswapV2Router01	Interface	|||	
└	factory	External ❗	INO ❗
└	WETH	External ❗	INO ❗
└	addLiquidity	External ❗	🛑 INO ❗
└	addLiquidityETH	External ❗	💸 INO ❗
└	removeLiquidity	External ❗	🛑 INO ❗
└	removeLiquidityETH	External ❗	🛑 INO ❗
└	removeLiquidityWithPermit	External ❗	🛑 INO ❗
└	removeLiquidityETHWithPermit	External ❗	🛑 INO ❗
└	swapExactTokensForTokens	External ❗	🛑 INO ❗
└	swapTokensForExactTokens	External ❗	🛑 INO ❗
└	swapExactETHForTokens	External ❗	💸 INO ❗
└	swapTokensForExactETH	External ❗	🛑 INO ❗
└	swapExactTokensForETH	External ❗	🛑 INO ❗

CONTRACT ASSESMENT

└	swapETHForExactTokens	External ❗	💱 INO ❗
└	quote	External ❗	INO ❗
└	getAmountOut	External ❗	INO ❗
└	getAmountIn	External ❗	INO ❗
└	getAmountsOut	External ❗	INO ❗
└	getAmountsIn	External ❗	INO ❗

IUniswapV2Router02	Interface	IUniswapV2Router01			
└	removeLiquidityETHSupportingFeeOnTransferTokens	External ❗	🛑 INO ❗		
└	removeLiquidityETHWithPermitSupportingFeeOnTransferTokens	External ❗	🛑 INO ❗		
└	swapExactTokensForTokensSupportingFeeOnTransferTokens	External ❗	🛑 INO ❗		
└	swapExactETHForTokensSupportingFeeOnTransferTokens	External ❗	💱 INO ❗		
└	swapExactTokensForETHSupportingFeeOnTransferTokens	External ❗	🛑 INO ❗		

IERC20Permit	Interface				
└	permit	External ❗	🛑 INO ❗		
└	nonces	External ❗	INO ❗		
└	DOMAIN_SEPARATOR	External ❗	INO ❗		

Address	Library				
└	isContract	Internal 🔒			
└	sendValue	Internal 🔒	🛑		
└	functionCall	Internal 🔒	🛑		
└	functionCall	Internal 🔒	🛑		
└	functionCallWithValue	Internal 🔒	🛑		
└	functionCallWithValue	Internal 🔒	🛑		
└	functionStaticCall	Internal 🔒			
└	functionStaticCall	Internal 🔒			
└	functionDelegateCall	Internal 🔒	🛑		

CONTRACT ASSESMENT

└	functionDelegateCall	Internal 🔒	🛑		
	└	verifyCallResultFromTarget	Internal 🔒			
	└	verifyCallResult	Internal 🔒			
	└	_revert	Private 🔐			

IERC20	Interface			
	└	totalSupply	External ❗		NO ❗	
	└	balanceOf	External ❗		NO ❗	
	└	transfer	External ❗	🛑	NO ❗	
	└	allowance	External ❗		NO ❗	
	└	approve	External ❗	🛑	NO ❗	
	└	transferFrom	External ❗	🛑	NO ❗	

SafeERC20	Library			
	└	safeTransfer	Internal 🔒	🛑		
	└	safeTransferFrom	Internal 🔒	🛑		
	└	safeApprove	Internal 🔒	🛑		
	└	safeIncreaseAllowance	Internal 🔒	🛑		
	└	safeDecreaseAllowance	Internal 🔒	🛑		
	└	safePermit	Internal 🔒	🛑		
	└	_callOptionalReturn	Private 🔐	🛑		

IERC20Metadata	Interface	IERC20		
	└	name	External ❗		NO ❗	
	└	symbol	External ❗		NO ❗	
	└	decimals	External ❗		NO ❗	

ERC20	Implementation	Context, IERC20, IERC20Metadata		
	└	<Constructor>	Public ❗	🛑	NO ❗	
	└	name	Public ❗		NO ❗	
	└	symbol	Public ❗		NO ❗	
	└	decimals	Public ❗		NO ❗	
	└	totalSupply	Public ❗		NO ❗	

CONTRACT ASSESMENT

└	balanceOf	Public ❗	INO ❗
└	transfer	Public ❗	🛑 INO ❗
└	allowance	Public ❗	INO ❗
└	approve	Public ❗	🛑 INO ❗
└	transferFrom	Public ❗	🛑 INO ❗
└	increaseAllowance	Public ❗	🛑 INO ❗
└	decreaseAllowance	Public ❗	🛑 INO ❗
└	_transfer	Internal 🔒	🛑
└	_mint	Internal 🔒	🛑
└	_burn	Internal 🔒	🛑
└	_approve	Internal 🔒	🛑
└	_spendAllowance	Internal 🔒	🛑
└	_beforeTokenTransfer	Internal 🔒	🛑
└	_afterTokenTransfer	Internal 🔒	🛑

Ownable	Implementation	Context
└	<Constructor>	Public ❗	🛑 INO ❗
└	owner	Public ❗	INO ❗
└	_checkOwner	Internal 🔒	
└	renounceOwnership	Public ❗	🛑	onlyOwner
└	transferOwnership	Public ❗	🛑	onlyOwner
└	_transferOwnership	Internal 🔒	🛑

ReentrancyGuard	Implementation	
└	<Constructor>	Public ❗	🛑 INO ❗
└	_nonReentrantBefore	Private 🔐	🛑
└	_nonReentrantAfter	Private 🔐	🛑
└	_reentrancyGuardEntered	Internal 🔒	

KetaiCoin	Implementation	ERC20, Ownable, ReentrancyGuard
└	<Constructor>	Public ❗	🛑	ERC20
└	<Receive Ether>	External ❗	💵 INO ❗
└	<Fallback>	External ❗	💵 INO ❗

CONTRACT ASSESMENT

└	getRouterAddress	Public ❗		NO ❗
└	claimStuckTokens	External ❗	🛑	onlyOwner
└	excludeFromFees	External ❗	🛑	onlyOwner
└	isExcludedFromFees	Public ❗		NO ❗
└	setAutomatedMarketMakerPair	Public ❗	🛑	onlyOwner
└	isAutomatedMarketMakerPair	Public ❗		NO ❗
└	updateTax	External ❗	🛑	onlyOwner
└	toggleSwapBack	External ❗	🛑	onlyOwner
└	setSwapTokensAtAmount	External ❗	🛑	onlyOwner
└	_transfer	Internal 🔒	🛑	
└	ForceSwapBack	External ❗	🛑	NO ❗
└	_autoswapBack	Internal 🔒	🛑	
└	outBNB	Internal 🔒	🛑	nonReentrant

Legend

Symbol	Meaning
🛑	Function can modify state
💲	Function is payable

STATIC ANALYSIS

```
INFO:Detectors:
Pragma version0.8.17 (contracts/Token.sol#7) allows old versions
solc-0.8.17 is not recommended for deployment
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#incorrect-versions-of-solidity
INFO:Detectors:
Low level call in Address.sendValue(address,uint256) (contracts/Token.sol#372-383):
        - (success) = recipient.call{value: amount}() (contracts/Token.sol#378)
Low level call in Address.functionCallWithValue(address,bytes,uint256,string) (contracts/Token.sol#420-440):
        - (success,returndata) = target.call{value: value}(data) (contracts/Token.sol#430-432)
Low level call in Address.functionStaticCall(address,bytes,string) (contracts/Token.sol#454-467):
        - (success,returndata) = target.staticcall(data) (contracts/Token.sol#459)
Low level call in Address.functionDelegateCall(address,bytes,string) (contracts/Token.sol#481-494):
        - (success,returndata) = target.delegatecall(data) (contracts/Token.sol#486)
Low level call in KetaiCoin.outBNB(address,uint256) (contracts/Token.sol#1198-1207):
        - (success) = address(_to).call{value: amount}() (contracts/Token.sol#1204)
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#low-level-calls
INFO:Detectors:
Function IUniswapV2Pair.DOMAIN_SEPARATOR() (contracts/Token.sol#83) is not in mixedCase
Function IUniswapV2Pair.PERMIT_TYPEHASH() (contracts/Token.sol#85) is not in mixedCase
Function IUniswapV2Pair.MINIMUM_LIQUIDITY() (contracts/Token.sol#116) is not in mixedCase
Function IUniswapV2Router01.WETH() (contracts/Token.sol#158) is not in mixedCase
Function IERC20Permit.DOMAIN_SEPARATOR() (contracts/Token.sol#364) is not in mixedCase
Parameter KetaiCoin.updateTax(uint256,uint256)._buyTax (contracts/Token.sol#1082) is not in mixedCase
Parameter KetaiCoin.updateTax(uint256,uint256)._sellTax (contracts/Token.sol#1082) is not in mixedCase
Function KetaiCoin.ForceSwapBack() (contracts/Token.sol#1162-1168) is not in mixedCase
Parameter KetaiCoin.outBNB(address,uint256)._to (contracts/Token.sol#1198) is not in mixedCase
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#conformance-to-solidity-naming-conventions
INFO:Detectors:
Variable IUniswapV2Router01.addLiquidity(address,address,uint256,uint256,uint256,uint256,address,uint256).amountADesired (contracts/Token.sol#163) is too similar to IUniswapV2Router01.ad
dLiquidity(address,address,uint256,uint256,uint256,uint256,address,uint256).amountBDesired (contracts/Token.sol#164)
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#variable-names-too-similar
INFO:Detectors:
KetaiCoin.marketingWallet (contracts/Token.sol#965) should be constant
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#state-variables-that-could-be-declared-constant
INFO:Detectors:
KetaiCoin.marketingWalletShares (contracts/Token.sol#967) should be immutable
KetaiCoin.setSwapTokensLimit (contracts/Token.sol#970) should be immutable
KetaiCoin.taxDenominator (contracts/Token.sol#960) should be immutable
KetaiCoin.uniswapV2Pair (contracts/Token.sol#975) should be immutable
KetaiCoin.uniswapV2Router (contracts/Token.sol#974) 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/0xf7241f4d2db9d9b4b36f936bfd75bc99172dab83eeeda1da7c6d800f2030be92

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

https://testnet.bscscan.com/tx/0xd8d7059e671b86b2fd6f53168af1554d1d5353b457490b1f291fe4db2c0683ca

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

https://testnet.bscscan.com/tx/0x512fbb3f30f370597ae0b74dcb1889cba28449df04ede3f0ca5f177c0c5a4f32

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

https://testnet.bscscan.com/tx/0x5cca435a21bd976afc5792f082cf5ff1824ac5bf7465903f744dd994706d22a5

5- Buying when not excluded from fees (0-49% tax) (passed):

https://testnet.bscscan.com/tx/0x1a0384d775093abeeca9b219335af0d4794a394a92f5071b314a2a6858925215

6- Selling when not excluded from fees (0-49% tax) (passed):

https://testnet.bscscan.com/tx/0x4a7fc91a6848f894cacda471387240f563545a6a4c7d011e08d0e41f8842621b

FUNCTIONAL TESTING

7- Transferring (0% tax) (passed):

https://testnet.bscscan.com/tx/0xca4ad4aaf0f81f26e58506bf61e651a32c837cf973614014a028104896d09116

8- Internal swap(ETH sent to marketing wallet) (passed):

https://testnet.bscscan.com/tx/0x4a7fc91a6848f894cacda471387240f563545a6a4c7d011e08d0e41f8842621b

MANUAL TESTING

Centralization – Excessive fees

Severity: High

function: updateTax

Status: Not Resolved

Overview:

Owner is able to put upto 50% tax on buy and sells separately.

```
function updateTax(uint256 _buyTax, uint256 _sellTax) external onlyOwner {
  buyTax = _buyTax;
  sellTax = _sellTax;
  totalTax = _buyTax + _sellTax;
  require(buyTax <= 49, "buy Fees cannot exceed 49%");
  require(sellTax <= 49, "buy Fees cannot exceed 49%");
  emit UpdateTax(buyTax, sellTax);
}
```

Suggestion

Consider reducing the upper bound of maximum buy/sell tax. Usually 10% is suggested to be a reasonable upperbound limit for buy/sell/transfer tax.

```
function updateTax(uint256 _buyTax, uint256 _sellTax) external onlyOwner {
  buyTax = _buyTax;
  sellTax = _sellTax;
  totalTax = _buyTax + _sellTax;
  require(buyTax <= 10, "buy Fees cannot exceed 10%");
  require(sellTax <= 10, "buy Fees cannot exceed 10%");
  emit UpdateTax(buyTax, sellTax);
}
```

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