auditace.tech

AuditAce
FROM INCEPTION TO SUCCESS

Smart Contract Audit

FOR

TRUMP KING BSC

DATED : 12 March, 2024

AUDIT SUMMARY

Project name – TRUMP KING BSC

Date: 12 March, 2024

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	1
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/address/0x396be951eff2cbef24c5756639d67023947881aa#code

Token Information

Token Name : TRUMP KING BSC

Token Symbol: TRUMP KING

Decimals: 18

Token Supply: 470000000000000

Network: BscScan

Token Type: BEP-20

Token Address:
0x25c5d64C307ad2Cabc77058a31a8D21991a41E45

Checksum:
A2032c616934aeb47e6039f76b20d221

Owner:
0x35630F21491F774741539CA83b69A0C1E499937e
(at time of writing the audit)

Deployer:
0x35630F21491F774741539CA83b69A0C1E499937e

TOKEN OVERVIEW

Fees:

Buy Fee: 0-25%

Sell Fee: 0-25%

Transfer Fee: 0-25%

Fees Privilege: Owner

Ownership: Owned

Minting: No mint function

Max Tx Amount/ Max Wallet Amount: No

Blacklist: No

AUDIT METHODOLOGY

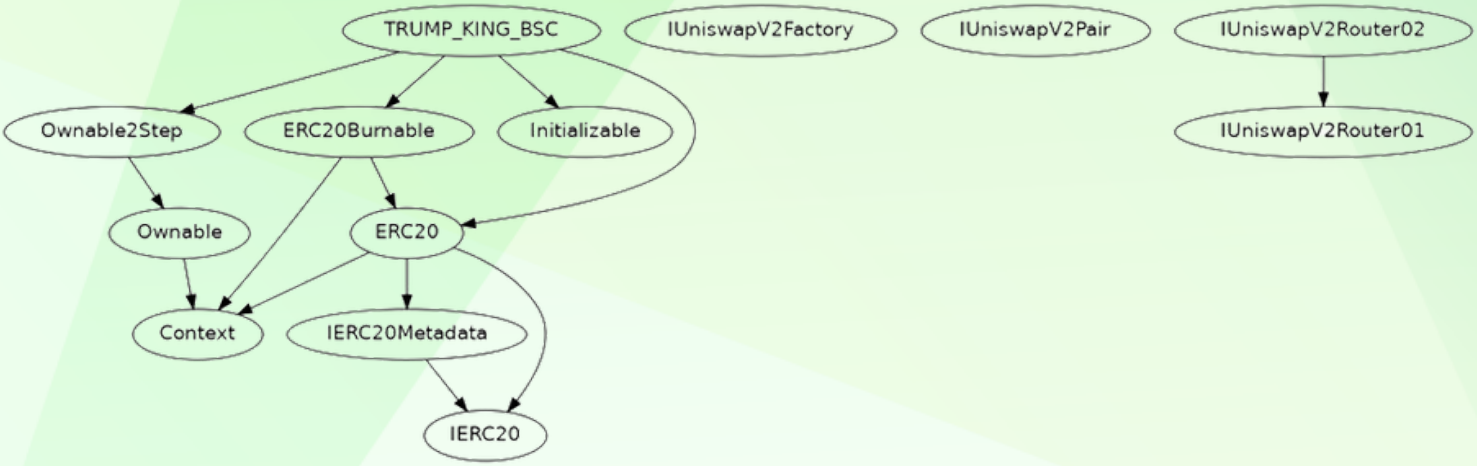
The auditing process will follow a routine as special considerations by Auditace:

- 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

INHERITANCE TREE



STATIC ANALYSIS

A static analysis of the code was performed using Slither.

No issues were found.

```
INFO:Detectors:
TRUMP_KING_BSC._transfer(address,address,uint256) (Token.sol#163-234) uses a Boolean constant improperly:
        -false || _developmentPending > 0 || _marketingPending > 0 (Token.sol#202)
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#misuse-of-a-boolean-constant
INFO:Detectors:
TRUMP_KING_BSC._transfer(address,address,uint256) (Token.sol#163-234) performs a multiplication on the result of a division:
        - fees = amount * totalFees[txType] / 10000 (Token.sol#182)
        - _developmentPending += fees * developmentFees[txType] / totalFees[txType] (Token.sol#185)
TRUMP_KING_BSC._transfer(address,address,uint256) (Token.sol#163-234) performs a multiplication on the result of a division:
        - fees = amount * totalFees[txType] / 10000 (Token.sol#182)
        - _marketingPending += fees * marketingFees[txType] / totalFees[txType] (Token.sol#187)
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#divide-before-multiply
INFO:Detectors:
Ownable2Step.transferOwnership(address).newOwner (Ownable2Step.sol#35) lacks a zero-check on :
                - _pendingOwner = newOwner (Ownable2Step.sol#36)
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#missing-zero-address-validation
INFO:Detectors:
Reentrancy in TRUMP_KING_BSC._updateRouterV2(address) (Token.sol#236-243):
        External calls:
        - pairV2 = IUniswapV2Factory(routerV2.factory()).createPair(address(this),routerV2.WETH()) (Token.sol#238)
        State variables written after the call(s):
        - _setAMMPair(pairV2,true) (Token.sol#240)
                - AMMPairs[pair] = isPair (Token.sol#252)
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#reentrancy-vulnerabilities-2
INFO:Detectors:
Reentrancy in TRUMP_KING_BSC._transfer(address,address,uint256) (Token.sol#163-234):
        External calls:
        - _swapTokensForCoin(token2Swap) (Token.sol#206)
                - routerV2.swapExactTokensForETHSupportingFeeOnTransferTokens(tokenAmount,0,path,address(this),block.timestamp) (Token.sol#99)
        External calls sending eth:
        - success = address(developmentAddress).send(developmentPortion) (Token.sol#211)
        Event emitted after the call(s):
        - developmentFeeSent(developmentAddress,developmentPortion) (Token.sol#213)
Reentrancy in TRUMP_KING_BSC._transfer(address,address,uint256) (Token.sol#163-234):
        External calls:
        - _swapTokensForCoin(token2Swap) (Token.sol#206)
                - routerV2.swapExactTokensForETHSupportingFeeOnTransferTokens(tokenAmount,0,path,address(this),block.timestamp) (Token.sol#99)
        External calls sending eth:
        - success = address(developmentAddress).send(developmentPortion) (Token.sol#211)
        - success = address(marketingAddress).send(marketingPortion) (Token.sol#220)
```

```
INFO:Detectors:
Reentrancy in TRUMP_KING_BSC._transfer(address,address,uint256) (Token.sol#163-234):
        External calls:
        - success = address(developmentAddress).send(developmentPortion) (Token.sol#211)
        State variables written after the call(s):
        - _developmentPending = 0 (Token.sol#216)
        Event emitted after the call(s):
        - developmentFeeSent(developmentAddress,developmentPortion) (Token.sol#213)
Reentrancy in TRUMP_KING_BSC._transfer(address,address,uint256) (Token.sol#163-234):
        External calls:
        - success = address(developmentAddress).send(developmentPortion) (Token.sol#211)
        - success = address(marketingAddress).send(marketingPortion) (Token.sol#220)
        State variables written after the call(s):
        - super._transfer(from,to,amount) (Token.sol#232)
                - _balances[from] = fromBalance - amount (ERC20.sol#231)
                - _balances[to] += amount (ERC20.sol#234)
        - _marketingPending = 0 (Token.sol#225)
        - _swapping = false (Token.sol#229)
        Event emitted after the call(s):
        - Transfer(from,to,amount) (ERC20.sol#237)
                - super._transfer(from,to,amount) (Token.sol#232)
        - marketingFeeSent(marketingAddress,marketingPortion) (Token.sol#222)
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#reentrancy-vulnerabilities-4
INFO:Detectors:
Variable IUniswapV2Router01.addLiquidity(address,address,uint256,uint256,uint256,uint256,address,uint256).amountADesired (IUniswapV2Router01.sol#10) is too
similar to IUniswapV2Router01.addLiquidity(address,address,uint256,uint256,uint256,uint256,address,uint256).amountBDesired (IUniswapV2Router01.sol#11)
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#variable-names-too-similar
INFO:Detectors:
TRUMP_KING_BSC.constructor() (Token.sol#59-77) uses literals with too many digits:
        - _mint(supplyRecipient,4700000000000000 * (10 ** decimals()) / 10) (Token.sol#75)
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#too-many-digits
INFO:Slither:Token.sol analyzed (13 contracts with 93 detectors), 53 result(s) found
```

FUNCTIONAL TESTING

1- Approve (passed):
https://testnet.bscscan.com/tx/0x0f689f6b9d2d696c92107731cf779ac007b1826ddfa063c18b22953d6e1051dc

2- Increase Allowance (passed):
https://testnet.bscscan.com/tx/0x589fed80dddb4ec089bde5b19d1346cf400e005dd00eae043db5f0bf7927a043

3- Decrease Allowance (passed):
https://testnet.bscscan.com/tx/0x2260f4f0501720f2acc311c41270b32f91d5a0fbe17b6b11e1970947b9a23ec5

4- Development Address Setup (passed):
https://testnet.bscscan.com/tx/0x21d980d5cf9cf4c5a7d41adb707a5064a7807a2e331270b615f6604633280a68

5- Marketing Address Setup (passed):
https://testnet.bscscan.com/tx/0x3ac146d7ead920e2e5108c750ea2fb7b4e9933aece2f072f76709a333ce99c03

6- Development Fees Setup (passed):
https://testnet.bscscan.com/tx/0xba7e3d248251acf98e4e8a7648a591f480ba5581ef795c9506e788e633df8684

7- Marketing Fees Setup (passed):
https://testnet.bscscan.com/tx/0x8b068681181 7f4896f72076e68ab2d650152287fdb4e20163a784bf682f8f594

POINTS TO NOTE

- The owner can transfer ownership.
- The owner can renounce ownership.
- The owner can set marketing/development address.
- The owner can set marketing/development fees of not more than 25%.
- The owner can exclude address from fees.
- The owner can set automated market maker pair.
- The Owner can update the swap threshhold value from 0.01% - 5%

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	1

MANUAL TESTING

Centralization – Missing Require Check

Severity: Medium

Subject: DevelopmentAddressSetup/MarketingAddressSetup

Status: Open

Overview:

The owner can set any arbitrary address excluding zero address as this is not recommended because if the owner sets the address to the contract address, then the ETH will not be sent to that address and the transaction will fail and this will lead to a potential honeypot in the contract.

```
function marketingAddressSetup(address _newAddress) public onlyOwner {
        require(_newAddress != address(0), "TaxesDefaultRouterWallet: Wallet tax
recipient cannot be a 0x0 address");

        marketingAddress = _newAddress;
        excludeFromFees(_newAddress, true);

        emit marketingAddressUpdated(_newAddress);
    }
function developmentAddressSetup(address _newAddress) public onlyOwner {
        require(_newAddress != address(0), "TaxesDefaultRouterWallet: Wallet tax
recipient cannot be a 0x0 address");

        developmentAddress = _newAddress;
        excludeFromFees(_newAddress, true);

        emit developmentAddressUpdated(_newAddress);
    }
```

Suggestion:

It is recommended that the address should not be able to set as a contract address.

MANUAL TESTING

Optimization

Severity: Optimization

Subject: Remove unused code

Status: Open

Overview:

Unused variables are allowed in Solidity, and they do not pose a direct security issue. It is the best practice to avoid them.

```
import "./IUniswapV2Pair.sol";
function _msgData() internal view virtual returns (bytes calldata) {
        return msg.data;
    }
```

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