auditace.tech

AuditAce
FROM INCEPTION TO SUCCESS

Smart Contract Audit

FOR

CMK

DATED : 21 July 23'

MANUAL TESTING

Centralization – Excessive fees

Severity: High
function: enableTrading
Status: Not Resolved
Overview:
The smart contract owner is able to include an arbitrary address in fees. Meaning that this address has to pay 30% fees on all actions (swaps and wallet to wallet transfers)
by including liquidity pool in fees, all holders have to pay up to 30% tax on buy/sells (60% tax in total)

```
function setWalletsIncludedFromFee(address wallet) external onlyOwner {
    require(wallet != address(0), "address variable can not be zero address");
    require(!isIncludedFromFee[wallet], "This wallet is excluded");
    isIncludedFromFee[wallet] = true;
    emit WalletsIncludedFromFee(wallet);
}
```

Suggestion
Ensure that fees are in a more reasonable range. Usually 0-10% is suggested as the upper bound of buy/sell/transfer fees

AUDIT SUMMARY

Project name – CMK

Date: 21 July, 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/0xcC0420B63e65284aF06f1490Aeb68Dde3F20246B

Token Information

Token Name :CryptoMarioKart

Token Symbol:CMK

Decimals: 18

Token Supply: 5,000,000

Token Address:
0xCf79fEb331bE62b7D0840CcD434503BA1ECDfF44

Checksum:
0ad074296cf18ede7f8ece0ad8a48dd57f0b6540

Owner: 0x6C3BF808628200a745cB6A4ae3eed0e7cdd3434E
(at time of writing the audit)

Deployer: 0x320A43b1783245Ce0F33cC978c263fC2b9FF674A

TOKEN OVERVIEW

Fees:

Buy Fees: 0-3%

Sell Fees: 0-3%

Transfer Fees: 0-3%

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 including wallets in fees

enabling trades

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

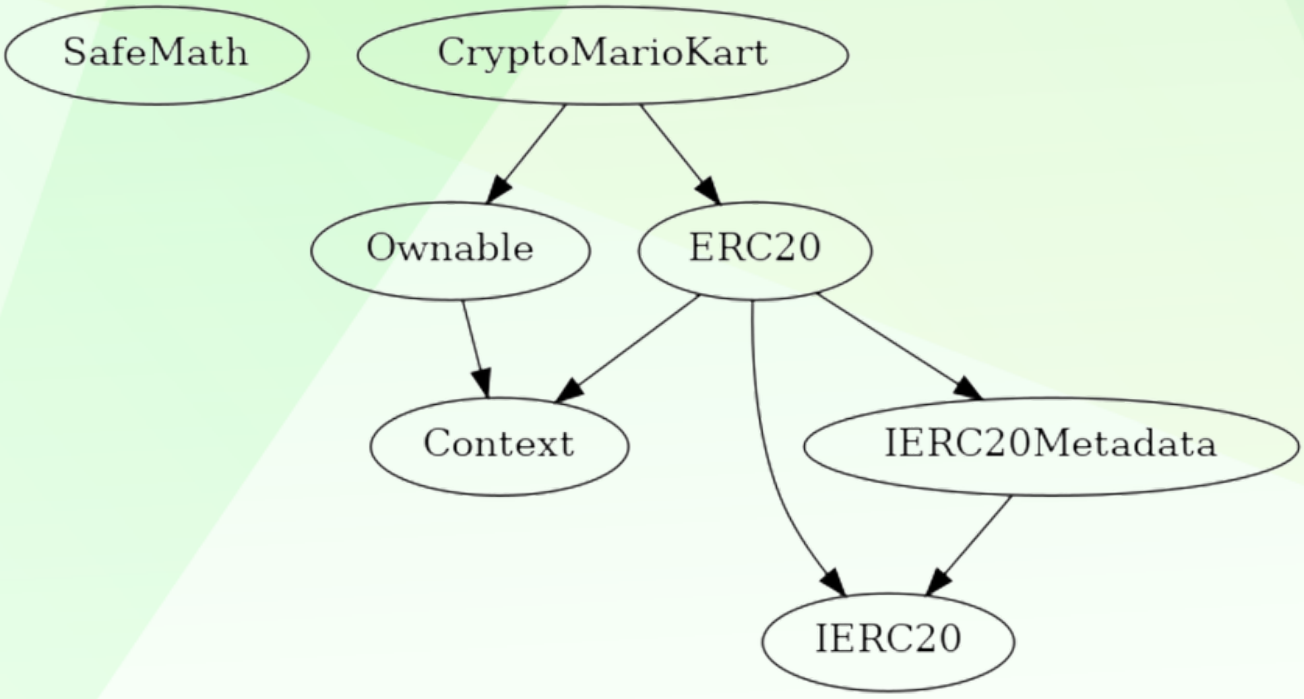
CLASSIFICATION OF RISK

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 include a wallet in fees. Included wallets have to pay 3% fee on all actions (buy/sell swaps and transfers)**
- Owner is not able to blacklist an arbitrary address.
- Owner is not able to disable trades
- Owner is not able to mint new tokens
- Owner is not able to set maximum wallet and maximum buy/sell limits

CONTRACT ASSESMENT

Contract	Type	Bases		
└	**Function Name**	**Visibility**	**Mutability**	**Modifiers**
SafeMath	Library			
└	tryAdd	Internal 🔒		
└	trySub	Internal 🔒		
└	tryMul	Internal 🔒		
└	tryDiv	Internal 🔒		
└	tryMod	Internal 🔒		
└	add	Internal 🔒		
└	sub	Internal 🔒		
└	mul	Internal 🔒		
└	div	Internal 🔒		
└	mod	Internal 🔒		
└	sub	Internal 🔒		

CONTRACT ASSESMENT

└	div	Internal 🔒		
└	mod	Internal 🔒		

Context	Implementation		
└	_msgSender	Internal 🔒	
└	_msgData	Internal 🔒	

Ownable	Implementation	Context	
└	<Constructor>	Public ❗	🛑 NO ❗
└	owner	Public ❗	NO ❗
└	_checkOwner	Internal 🔒	
└	renounceOwnership	Public ❗	🛑	onlyOwner
└	transferOwnership	Public ❗	🛑	onlyOwner
└	_transferOwnership	Internal 🔒	🛑	

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

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 ❗		NO ❗
└	transfer	Public ❗	🛑	NO ❗
└	allowance	Public ❗		NO ❗
└	approve	Public ❗	🛑	NO ❗
└	transferFrom	Public ❗	🛑	NO ❗
└	increaseAllowance	Public ❗	🛑	NO ❗
└	decreaseAllowance	Public ❗	🛑	NO ❗
└	_transfer	Internal 🔒	🛑	
└	_mint	Internal 🔒	🛑	
└	_burn	Internal 🔒	🛑	
└	_approve	Internal 🔒	🛑	
└	_spendAllowance	Internal 🔒	🛑	
└	_beforeTokenTransfer	Internal 🔒	🛑	
└	_afterTokenTransfer	Internal 🔒	🛑	
CryptoMarioKart	Implementation	ERC20, Ownable		
└	<Constructor>	Public ❗	🛑	ERC20
└	setWalletsIncludedFromFee	External ❗	🛑	onlyOwner
└	unsetWalletsIncludedFromFee	External ❗	🛑	onlyOwner
└	recoverTokensFromContract	External ❗	🛑	onlyOwner
└	recoverEthFromContract	External ❗	🛑	onlyOwner
└	_transfer	Internal 🔒	🛑	

Legend

Symbol	Meaning
🛑	Function can modify state
💲	Function is payable

STATIC ANALYSIS

```
Context._msgData() (contracts/Token.sol#239-241) is never used and should be removed
ERC20._burn(address,uint256) (contracts/Token.sol#709-725) is never used and should be removed
SafeMath.add(uint256,uint256) (contracts/Token.sol#94-96) is never used and should be removed
SafeMath.div(uint256,uint256,string) (contracts/Token.sol#188-193) is never used and should be removed
SafeMath.mod(uint256,uint256) (contracts/Token.sol#152-154) is never used and should be removed
SafeMath.mod(uint256,uint256,string) (contracts/Token.sol#210-215) is never used and should be removed
SafeMath.sub(uint256,uint256) (contracts/Token.sol#108-110) is never used and should be removed
SafeMath.sub(uint256,uint256,string) (contracts/Token.sol#169-174) is never used and should be removed
SafeMath.tryAdd(uint256,uint256) (contracts/Token.sol#23-29) is never used and should be removed
SafeMath.tryDiv(uint256,uint256) (contracts/Token.sol#65-70) is never used and should be removed
SafeMath.tryMod(uint256,uint256) (contracts/Token.sol#77-82) is never used and should be removed
SafeMath.tryMul(uint256,uint256) (contracts/Token.sol#48-58) is never used and should be removed
SafeMath.trySub(uint256,uint256) (contracts/Token.sol#36-41) is never used and should be removed
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#dead-code

Pragma version^0.8.0 (contracts/Token.sol#5) allows old versions
Pragma version^0.8.0 (contracts/Token.sol#222) allows old versions
Pragma version^0.8.0 (contracts/Token.sol#248) allows old versions
Pragma version^0.8.0 (contracts/Token.sol#331) allows old versions
Pragma version^0.8.0 (contracts/Token.sol#411) allows old versions
Pragma version^0.8.0 (contracts/Token.sol#439) allows old versions
Pragma version^0.8.17 (contracts/Token.sol#801) 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

Parameter CryptoMarioKart.recoverTokensFromContract(address)._tokenAddress (contracts/Token.sol#852) is not in mixedCase
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#conformance-to-solidity-naming-conventions

Reentrancy in CryptoMarioKart.recoverEthFromContract() (contracts/Token.sol#858-862):
        External calls:
        - address(owner()).transfer(balance) (contracts/Token.sol#860)
        Event emitted after the call(s):
        - ETHRecovered(balance) (contracts/Token.sol#861)
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#reentrancy-vulnerabilities-4

CryptoMarioKart.devWallet (contracts/Token.sol#809) should be immutable
CryptoMarioKart.rewardPool (contracts/Token.sol#810) should be immutable
CryptoMarioKart.taxDev (contracts/Token.sol#805) should be immutable
CryptoMarioKart.taxRewardPool (contracts/Token.sol#806) should be immutable
CryptoMarioKart.taxTeam (contracts/Token.sol#804) should be immutable
CryptoMarioKart.teamWallet (contracts/Token.sol#808) 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/0xc772b1a9cdcc4f1d1c0c8615eac93c8cb6f306287907927a6fc6d4d8caabf2e4

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

https://testnet.bscscan.com/tx/0x816beeba9388884d4b607d6eea389be47170da7da089afd284a7397c735a54f5

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

https://testnet.bscscan.com/tx/0xc5ec65fc1a8a6bdde5a7527fed7b14840cf7f2e3fbb051252dcc8ff3d3982874

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

https://testnet.bscscan.com/tx/0x0ef45e67610558ee5cb7a2bbb5ce4bb1f2ae5ec182443d058e9534fdbd70d6dc

5- Buying when not excluded from fees (0-3% tax)(passed):

https://testnet.bscscan.com/tx/0x49a6ed213f2a1515568f01fb7da009261ba5e2ad6feefad4d18b7bfa899ebe1c

6- Selling when not excluded from fees (0-3% tax)(passed):

https://testnet.bscscan.com/tx/0x5b28462fc069127730a1635db14f943d7ee9901941cc096c97b448be4265cf10

FUNCTIONAL TESTING

7- Transferring when not excluded from fees (0-3% tax) (passed):

https://testnet.bscscan.com/tx/0x4dc15715e1eecbbf77b840182101e79d4b662e3edb5922a8fb63d5e162b138a4

MANUAL TESTING

Centralization – Excessive fees

Severity: High
function: enableTrading
Status: Not Resolved
Overview:
The smart contract owner is able to include an arbitrary address in fees. Meaning that this address has to pay 30% fees on all actions (swaps and wallet to wallet transfers)
by including liquidity pool in fees, all holders have to pay up to 30% tax on buy/sells (60% tax in total)

```
function setWalletsIncludedFromFee(address wallet) external onlyOwner {
    require(wallet != address(0), "address variable can not be zero address");
    require(!isIncludedFromFee[wallet], "This wallet is excluded");
    isIncludedFromFee[wallet] = true;
    emit WalletsIncludedFromFee(wallet);
}
```

Suggestion
Ensure that fees are in a more reasonable range. Usually 0-10% is suggested as the upper bound of buy/sell/transfer fees

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