AuditAce
FROM INCEPTION TO SUCCESS

Smart Contract Audit

FOR

Unicorn Super Market Maker

DATED : 12 June 23'

HIGH RISK

Centralization – Trades must be enabled

Severity: High

function: enableTrading

Status: Open

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 {
    tradingActive = true;
    swapEnabled = true;
}
```

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 trade

AUDIT SUMMARY

Project name – Unicorn Super Market Maker

Date: 12 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	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/0x1AB2665fC56D3aD1e730C65a935B2546653ACdE2

Token Information

Token Name : Unicorn Super MarketMaker

Token Symbol:Unicorn

Decimals: 9

Token Supply: 1,000,000,000

Token Address:
0x03c1709ed160380B332F6b4BBC756ceA39a06656

Checksum:
e9be41dddc13646770a7c6becb239d023ebd8e33

Owner:
0x1943e14C6b4bC3D8F481Cf7061c49849E25De7Fb
(at time of writing the audit)

Deployer:
0x0cd8b4C87a8dd063Af404eaDC27d79628f165092

TOKEN OVERVIEW

Fees:

Buy Fees: 10%

Sell Fees: 10%

Transfer Fees: 0%

Fees Privilege: None

Ownership: owned

Minting: No mint function

Max Tx Amount/ Max Wallet Amount: No

Blacklist: No

Other Privileges: 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

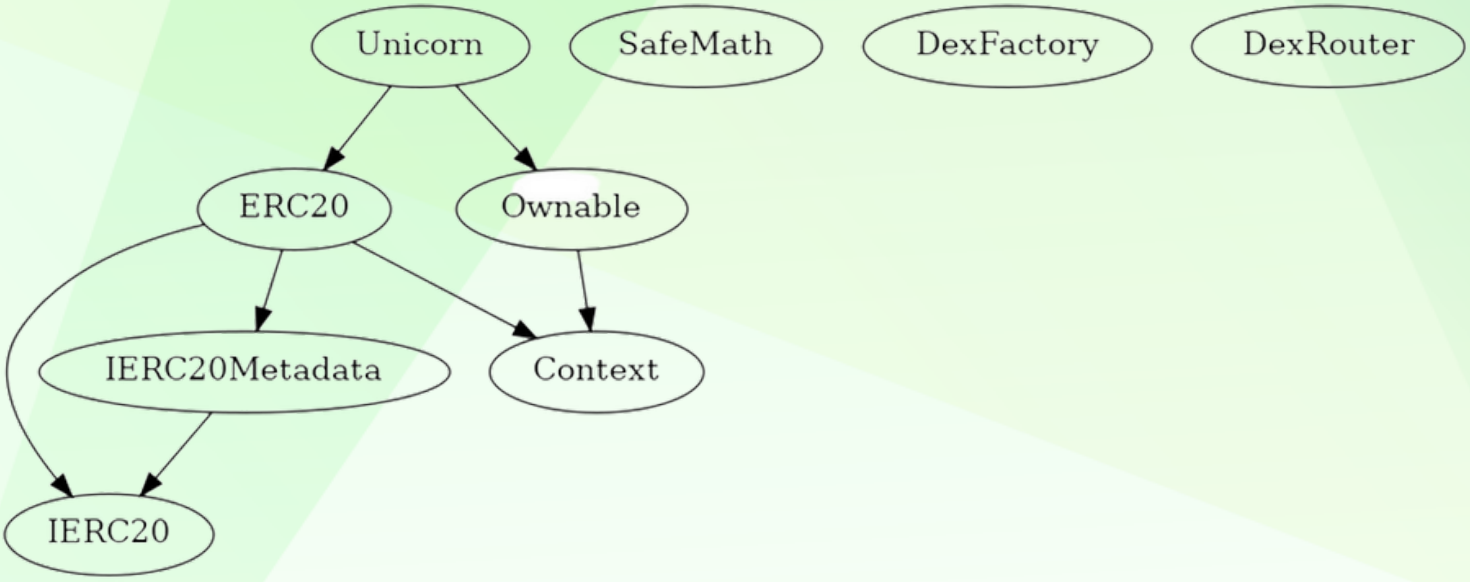
CLASSIFICATION OF RISK

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 change buy/sell/transfer fees (5% static)
- 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 mint new tokens
- Owner is not able to disable trades
- Owner has 100% of total supply after deployment

STATIC ANALYSIS

```
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#reentrancy-vulnerabilities-3

Context._msgData() (contracts/Token.sol#106-108) is never used and should be removed
ERC20._burn(address,uint256) (contracts/Token.sol#421-437) is never used and should be removed
SafeMath.add(uint256,uint256) (contracts/Token.sol#605-607) is never used and should be removed
SafeMath.div(uint256,uint256) (contracts/Token.sol#647-649) is never used and should be removed
SafeMath.div(uint256,uint256,string) (contracts/Token.sol#699-704) is never used and should be removed
SafeMath.mod(uint256,uint256) (contracts/Token.sol#663-665) is never used and should be removed
SafeMath.mod(uint256,uint256,string) (contracts/Token.sol#721-726) is never used and should be removed
SafeMath.mul(uint256,uint256) (contracts/Token.sol#633-635) is never used and should be removed
SafeMath.sub(uint256,uint256) (contracts/Token.sol#619-621) is never used and should be removed
SafeMath.sub(uint256,uint256,string) (contracts/Token.sol#680-685) is never used and should be removed
SafeMath.tryAdd(uint256,uint256) (contracts/Token.sol#534-540) is never used and should be removed
SafeMath.tryDiv(uint256,uint256) (contracts/Token.sol#576-581) is never used and should be removed
SafeMath.tryMod(uint256,uint256) (contracts/Token.sol#588-593) is never used and should be removed
SafeMath.tryMul(uint256,uint256) (contracts/Token.sol#559-569) is never used and should be removed
SafeMath.trySub(uint256,uint256) (contracts/Token.sol#547-552) 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#8) 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 Unicorn.internalSwap() (contracts/Token.sol#972-979):
        - (success) = marketingWallet.call{value: address(this).balance}() (contracts/Token.sol#978)
Low level call in Unicorn.withdrawStuckETH() (contracts/Token.sol#991-994):
        - (success) = address(msg.sender).call{value: address(this).balance}() (contracts/Token.sol#992)
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#low-level-calls

Function DexRouter.WETH() (contracts/Token.sol#833) is not in mixedCase
Event UnicornmarketingWalletChanged(address) (contracts/Token.sol#881) is not in CapWords
Parameter Unicorn.setmarketingWallet(address)._newmarketing (contracts/Token.sol#899) is not in mixedCase
Parameter Unicorn.setSwapTokensAtAmount(uint256)._newAmount (contracts/Token.sol#905) is not in mixedCase
Parameter Unicorn.setWhitelistStatus(address,bool)._wallet (contracts/Token.sol#918) is not in mixedCase
Parameter Unicorn.setWhitelistStatus(address,bool)._status (contracts/Token.sol#918) is not in mixedCase
Parameter Unicorn.checkWhitelist(address)._wallet (contracts/Token.sol#923) is not in mixedCase
Parameter Unicorn.swapToETH(uint256)._amount (contracts/Token.sol#981) is not in mixedCase
Parameter Unicorn.withdrawStuckTokens(address).BEP20_token (contracts/Token.sol#996) is not in mixedCase
Constant Unicorn._totalSupply (contracts/Token.sol#858) is not in UPPER_CASE_WITH_UNDERSCORES
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#conformance-to-solidity-naming-conventions

Unicorn.slitherConstructorVariables() (contracts/Token.sol#853-1002) uses literals with too many digits:
        - swapTokensAtAmount = _totalSupply / 100000 (contracts/Token.sol#873)
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#too-many-digits

Unicorn.pairAddress (contracts/Token.sol#862) should be immutable
Unicorn.uniswapRouter (contracts/Token.sol#861) 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

CONTRACT ASSESMENT

Contract	Type	Bases		
└	**Function Name**	**Visibility**	**Mutability**	**Modifiers**
IERC20	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 🔒		
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 ❗
└	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 🔒	🛑	

CONTRACT ASSESMENT

SafeMath	Library			
└	tryAdd	Internal 🔒		
└	trySub	Internal 🔒		
└	tryMul	Internal 🔒		
└	tryDiv	Internal 🔒		
└	tryMod	Internal 🔒		
└	add	Internal 🔒		
└	sub	Internal 🔒		
└	mul	Internal 🔒		
└	div	Internal 🔒		
└	mod	Internal 🔒		
└	sub	Internal 🔒		
└	div	Internal 🔒		
└	mod	Internal 🔒		
Ownable	Implementation	Context		
└	<Constructor>	Public ❗	🛑	NO ❗
└	owner	Public ❗		NO ❗
└	_checkOwner	Internal 🔒		
└	renounceOwnership	Public ❗	🛑	onlyOwner
└	transferOwnership	Public ❗	🛑	onlyOwner
└	_transferOwnership	Internal 🔒	🛑	
DexFactory	Interface			
└	createPair	External ❗	🛑	NO ❗
DexRouter	Interface			
└	factory	External ❗		NO ❗
└	WETH	External ❗		NO ❗
└	addLiquidityETH	External ❗	💵	NO ❗
└	swapExactTokensForETHSupportingFeeOnTransferTokens	External ❗	🛑	NO ❗
Unicorn	Implementation	ERC20, Ownable		
└	<Constructor>	Public ❗	🛑	ERC20
└	setmarketingWallet	External ❗	🛑	onlyOwner
└	setSwapTokensAtAmount	External ❗	🛑	onlyOwner
└	toggleSwapping	External ❗	🛑	onlyOwner
└	setWhitelistStatus	External ❗	🛑	onlyOwner
└	checkWhitelist	External ❗		NO ❗
└	startTrading	External ❗	🛑	onlyOwner
└	_takeTax	Internal 🔒	🛑	
└	_transfer	Internal 🔒	🛑	

CONTRACT ASSESMENT

└	internalSwap	Internal 🔒	🛑		
└	swapToETH	Internal 🔒	🛑		
└	withdrawStuckETH	External ❗	🛑	onlyOwner
└	withdrawStuckTokens	External ❗	🛑	onlyOwner
└	<Receive Ether>	External ❗	💵	NO ❗

Symbol	Meaning
🛑	Function can modify state
💵	Function is payable

FUNCTIONAL TESTING

1- Adding liquidity (passed):

https://testnet.bscscan.com/tx/0xe71834721aef6e2bb2efab0e8803bbe548e25267d04785e0b9f408978afdb109

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

https://testnet.bscscan.com/tx/0xe5bbb1be1d20995b819892513fd78a3e2627803a722ced833aac29fea8b07d71

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

https://testnet.bscscan.com/tx/0x9aac4b4ee6961c6877614cdec7bcb810baa837b3198e496ec839389dac09cb27

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

https://testnet.bscscan.com/tx/0x4cf322065a417a1336a1f1890409803ebd9306c6d5ffc19c8818e6ccb173fd21

5- Buying when not excluded from fees (10% tax) (passed):

https://testnet.bscscan.com/tx/0x80d3b6ca0223efe2e71882a577eb189f26c0760793ef3febf548d289967eee70

6- Selling when not excluded from fees (10% tax) (passed):

https://testnet.bscscan.com/tx/0x7426cfa328ff3d0471633ad07395c91c9aed3f7c0ac8c90d3f1c453e1fdeba87

FUNCTIONAL TESTING

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

https://testnet.bscscan.com/tx/0xb9c52bb6b03c4856f9b7030dc493229ebfa2071522f6f6c962cac72e2903b4ea

8- Internal swap (BNB Fees and auto-liquidity) (passed):

https://testnet.bscscan.com/address/0x0cd8b4c87a8dd063af404eadc27d79628f165092#internaltx

MANUAL TESTING

Centralization – Trades must be enabled

Severity: High

function: enableTrading

Status: Open

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 {
    tradingActive = true;
    swapEnabled = true;
}
```

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 trade

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