auditace.tech

AuditAce

FROM INCEPTION TO SUCCESS

Smart Contract Audit

FOR

ASEC

DATED : 13 June 23'

HIGH RISK FINDING

Centralization – Trades must be enabled

Severity: High

function: enableTrading

Status: Not Resolved

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() public onlyOwner {
    require(!tradingEnabled, "Trading already enabled!");
    tradingEnabled = 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 trades

AUDIT SUMMARY

Project name – FSEC

Date: 13 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:
Contract has been tested on binance smart chain testnet which can be found in below link:
https://testnet.bscscan.com/token/0xeC29579C7d0284A61edCc32A31642C686261abFE

Token Information

Token Name : AntiSEC

Token Symbol: ASEC

Decimals: 18

Token Supply: 500,000,000,000

Token Address:
0x9Df6Ec8EAF159B6D1d0A689E7e04b28e7817d4fF

Checksum:
3939bbcfb4f12229165b8412cb8898843805b775

Owner:
0x7f98dD4F67AF4E7B8fAc0334b30aD1058224a3AA

Deployer:
0x7f98dD4F67AF4E7B8fAc0334b30aD1058224a3AA

TOKEN OVERVIEW

Fees:

Buy Fees: 0-12%

Sell Fees: 0-12%

Transfer Fees: 0-12%

Fees Privilege: Owner

Ownership: Owned

Minting: None

Max Tx Amount/ Max Wallet Amount: No

Blacklist: No

Other Privileges: - initial distribution of the token

- enabling trades manual

- 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

- ✓ 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

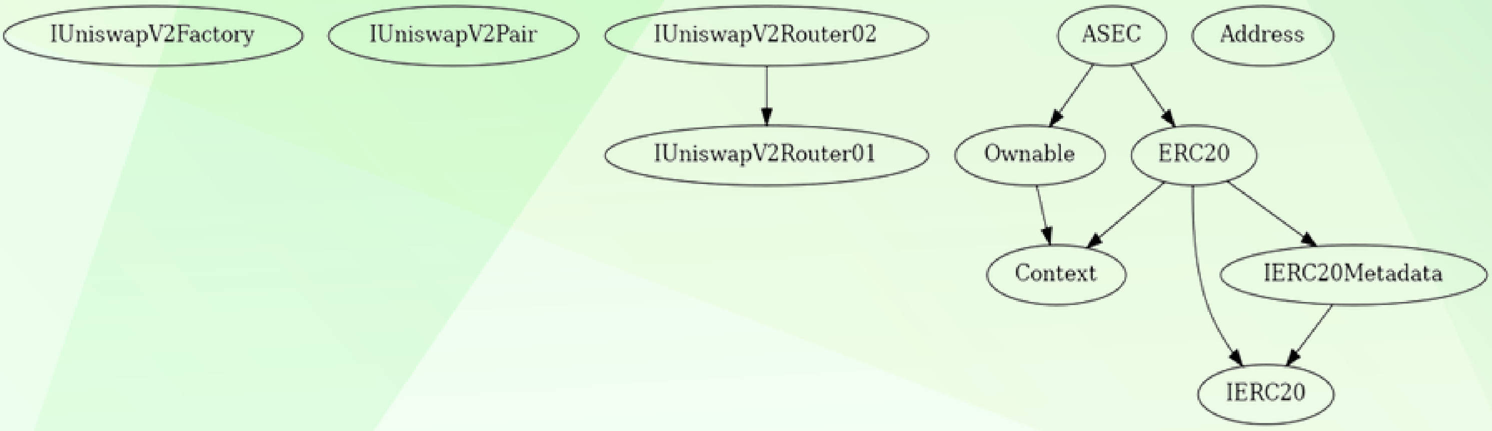
CLASSIFICATION OF RISK

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

INHERITANCE TREE



POINTS TO NOTE

- Sum of buy and sell fee can not exceed 12% (buy + sell <= 12%)
- Owner is able to change transfer fee in range (0-12%)
- 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
- Owner must enable trades manually

CONTRACT ASSESMENT

```
|  Contract  |        Type        |       Bases      |                  |                 |
|:----------:|:-------------------:|:----------------:|:----------------:|:---------------:|
|     └      |  **Function Name**  |  **Visibility**  |  **Mutability**  |  **Modifiers**  |
||||||
| **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 ❗ |
| └ | PERMIT_TYPEHASH | External ❗ |   |NO ❗ |
| └ | nonces | External ❗ |   |NO ❗ |
| └ | permit | External ❗ | 🛑  |NO ❗ |
| └ | MINIMUM_LIQUIDITY | External ❗ |   |NO ❗ |
| └ | factory | External ❗ |   |NO ❗ |
| └ | token0 | External ❗ |   |NO ❗ |
| └ | token1 | External ❗ |   |NO ❗ |
| └ | getReserves | External ❗ |   |NO ❗ |
| └ | price0CumulativeLast | External ❗ |   |NO ❗ |
| └ | price1CumulativeLast | External ❗ |   |NO ❗ |
| └ | kLast | External ❗ |   |NO ❗ |
| └ | mint | External ❗ | 🛑  |NO ❗ |
| └ | burn | External ❗ | 🛑  |NO ❗ |
| └ | swap | External ❗ | 🛑  |NO ❗ |
| └ | skim | External ❗ | 🛑  |NO ❗ |
| └ | sync | External ❗ | 🛑  |NO ❗ |
```

CONTRACT ASSESMENT

```
| └ | initialize | External ❗️ | 🛑  |NO ❗️ |
||||||
| **IUniswapV2Router01** | Interface |  |||
| └ | factory | External ❗️ |   |NO ❗️ |
| └ | WETH | External ❗️ |   |NO ❗️ |
| └ | addLiquidity | External ❗️ | 🛑  |NO ❗️ |
| └ | addLiquidityETH | External ❗️ |  💵 |NO ❗️ |
| └ | removeLiquidity | External ❗️ | 🛑  |NO ❗️ |
| └ | removeLiquidityETH | External ❗️ | 🛑  |NO ❗️ |
| └ | removeLiquidityWithPermit | External ❗️ | 🛑  |NO ❗️ |
| └ | removeLiquidityETHWithPermit | External ❗️ | 🛑  |NO ❗️ |
| └ | swapExactTokensForTokens | External ❗️ | 🛑  |NO ❗️ |
| └ | swapTokensForExactTokens | External ❗️ | 🛑  |NO ❗️ |
| └ | swapExactETHForTokens | External ❗️ |  💵 |NO ❗️ |
| └ | swapTokensForExactETH | External ❗️ | 🛑  |NO ❗️ |
| └ | swapExactTokensForETH | External ❗️ | 🛑  |NO ❗️ |
| └ | swapETHForExactTokens | External ❗️ |  💵 |NO ❗️ |
| └ | quote | External ❗️ |   |NO ❗️ |
| └ | getAmountOut | External ❗️ |   |NO ❗️ |
| └ | getAmountIn | External ❗️ |   |NO ❗️ |
| └ | getAmountsOut | External ❗️ |   |NO ❗️ |
| └ | getAmountsIn | External ❗️ |   |NO ❗️ |
||||||
| **IUniswapV2Router02** | Interface | IUniswapV2Router01 |||
| └ | removeLiquidityETHSupportingFeeOnTransferTokens | External ❗️ | 🛑  |NO ❗️ |
| └ | removeLiquidityETHWithPermitSupportingFeeOnTransferTokens | External ❗️ | 🛑  |NO ❗️ |
| └ | swapExactTokensForTokensSupportingFeeOnTransferTokens | External ❗️ | 🛑  |NO ❗️ |
| └ | swapExactETHForTokensSupportingFeeOnTransferTokens | External ❗️ |  💵 |NO ❗️ |
| └ | swapExactTokensForETHSupportingFeeOnTransferTokens | External ❗️ | 🛑  |NO ❗️ |
||||||
| **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 ❗️ |
```

CONTRACT ASSESMENT

```
||||||
| **Address** | Library |  |||
| └ | isContract | Internal 🔒 |   | |
| └ | sendValue | Internal 🔒 | 🛑  | |
| └ | functionCall | Internal 🔒 | 🛑  | |
| └ | functionCall | Internal 🔒 | 🛑  | |
| └ | functionCallWithValue | Internal 🔒 | 🛑  | |
| └ | functionCallWithValue | Internal 🔒 | 🛑  | |
| └ | functionStaticCall | Internal 🔒 |   | |
| └ | functionStaticCall | Internal 🔒 |   | |
| └ | functionDelegateCall | Internal 🔒 | 🛑  | |
| └ | functionDelegateCall | Internal 🔒 | 🛑  | |
| └ | verifyCallResultFromTarget | Internal 🔒 |   | |
| └ | verifyCallResult | Internal 🔒 |   | |
| └ | _revert | Private 🔐 |   | |
||||||
| **Context** | Implementation |  |||
| └ | _msgSender | Internal 🔒 |   | |
| └ | _msgData | Internal 🔒 |   | |
||||||
| **Ownable** | Implementation | Context |||
| └ | <Constructor> | Public ❗️ | 🛑  |NO ❗️ |
| └ | owner | Public ❗️ |   |NO ❗️ |
| └ | renounceOwnership | Public ❗️ | 🛑  | onlyOwner |
| └ | transferOwnership | Public ❗️ | 🛑  | onlyOwner |
||||||
| **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 🔒 | 🛑  | |
```

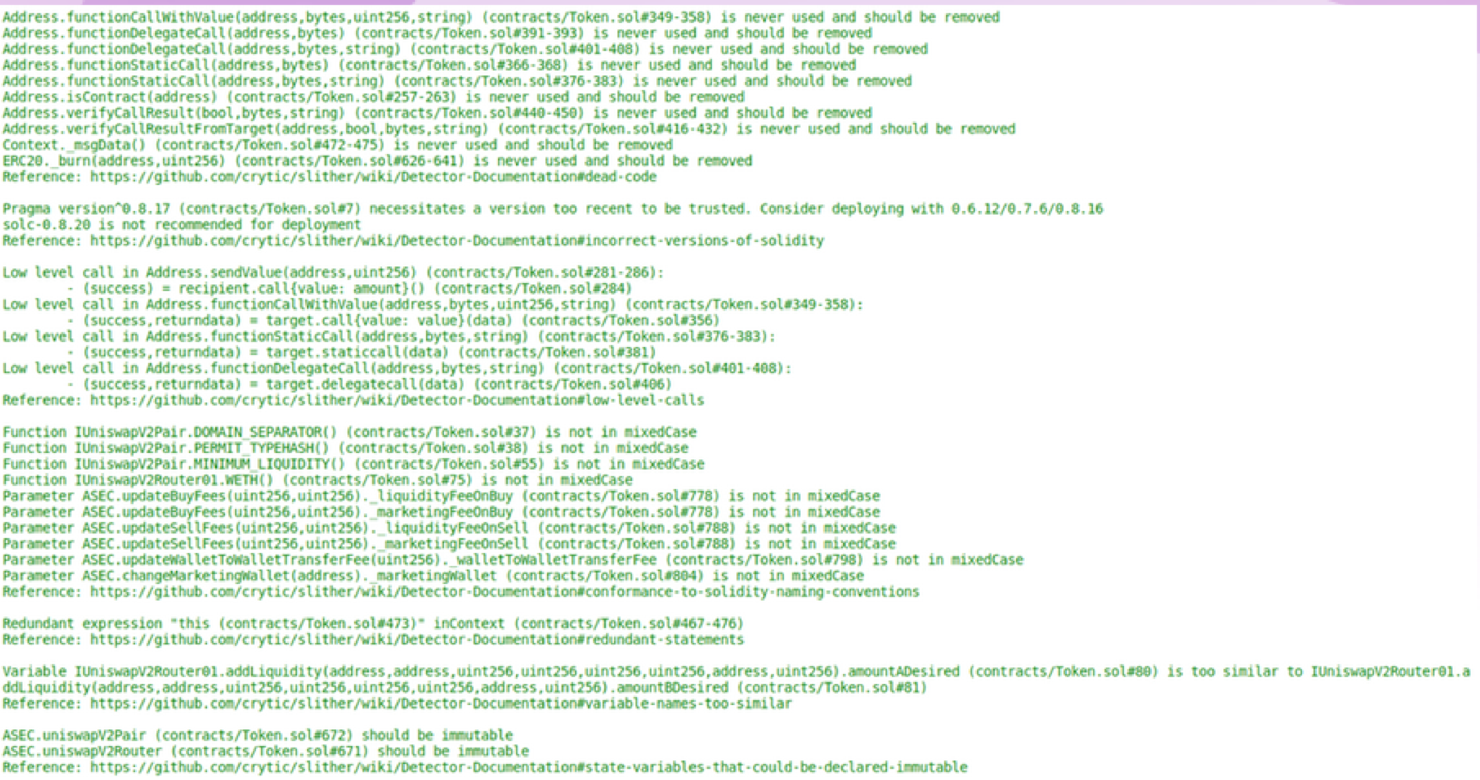
CONTRACT ASSESMENT

```
| └ | _approve | Internal 🔒 | 🛑  | |
| └ | _beforeTokenTransfer | Internal 🔒 | 🛑  | |
| └ | _afterTokenTransfer | Internal 🔒 | 🛑  | |
||||||
| **ASEC** | Implementation | ERC20, Ownable |||
| └ | <Constructor> | Public ❗️ | 🛑  | ERC20 |
| └ | <Receive Ether> | External ❗️ | 💵 |NO ❗️ |
| └ | enableTrading | Public ❗️ | 🛑  | onlyOwner |
| └ | claimStuckTokens | External ❗️ | 🛑  | onlyOwner |
| └ | excludeFromFees | External ❗️ | 🛑  | onlyOwner |
| └ | isExcludedFromFees | Public ❗️ |   |NO ❗️ |
| └ | updateBuyFees | External ❗️ | 🛑  | onlyOwner |
| └ | updateSellFees | External ❗️ | 🛑  | onlyOwner |
| └ | updateWalletToWalletTransferFee | External ❗️ | 🛑  | onlyOwner |
| └ | changeMarketingWallet | External ❗️ | 🛑  | onlyOwner |
| └ | _transfer | Internal 🔒 | 🛑  | |
| └ | setSwapTokensAtAmount | External ❗️ | 🛑  | onlyOwner |
| └ | swapAndLiquify | Private 🔐 | 🛑  | |
| └ | swapAndSendMarketing | Private 🔐 | 🛑  | |


### Legend

|  Symbol  |  Meaning  |
|:--------:|-----------|
|    🛑    | Function can modify state |
|    💵    | Function is payable |
```

STATIC ANALYSIS



```
Address.functionCallWithValue(address,bytes,uint256,string) (contracts/Token.sol#349-358) is never used and should be removed
Address.functionDelegateCall(address,bytes) (contracts/Token.sol#391-393) is never used and should be removed
Address.functionDelegateCall(address,bytes,string) (contracts/Token.sol#401-408) is never used and should be removed
Address.functionStaticCall(address,bytes) (contracts/Token.sol#366-368) is never used and should be removed
Address.functionStaticCall(address,bytes,string) (contracts/Token.sol#376-383) is never used and should be removed
Address.isContract(address) (contracts/Token.sol#257-263) is never used and should be removed
Address.verifyCallResult(bool,bytes,string) (contracts/Token.sol#440-450) is never used and should be removed
Address.verifyCallResultFromTarget(address,bool,bytes,string) (contracts/Token.sol#416-432) is never used and should be removed
Context._msgData() (contracts/Token.sol#472-475) is never used and should be removed
ERC20._burn(address,uint256) (contracts/Token.sol#626-641) 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#7) 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 Address.sendValue(address,uint256) (contracts/Token.sol#281-286):
        - (success) = recipient.call{value: amount}() (contracts/Token.sol#284)
Low level call in Address.functionCallWithValue(address,bytes,uint256,string) (contracts/Token.sol#349-358):
        - (success,returndata) = target.call{value: value}(data) (contracts/Token.sol#356)
Low level call in Address.functionStaticCall(address,bytes,string) (contracts/Token.sol#376-383):
        - (success,returndata) = target.staticcall(data) (contracts/Token.sol#381)
Low level call in Address.functionDelegateCall(address,bytes,string) (contracts/Token.sol#401-408):
        - (success,returndata) = target.delegatecall(data) (contracts/Token.sol#406)
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#low-level-calls

Function IUniswapV2Pair.DOMAIN_SEPARATOR() (contracts/Token.sol#37) is not in mixedCase
Function IUniswapV2Pair.PERMIT_TYPEHASH() (contracts/Token.sol#38) is not in mixedCase
Function IUniswapV2Pair.MINIMUM_LIQUIDITY() (contracts/Token.sol#55) is not in mixedCase
Function IUniswapV2Router01.WETH() (contracts/Token.sol#75) is not in mixedCase
Parameter ASEC.updateBuyFees(uint256,uint256)._liquidityFeeOnBuy (contracts/Token.sol#778) is not in mixedCase
Parameter ASEC.updateBuyFees(uint256,uint256)._marketingFeeOnBuy (contracts/Token.sol#778) is not in mixedCase
Parameter ASEC.updateSellFees(uint256,uint256)._liquidityFeeOnSell (contracts/Token.sol#788) is not in mixedCase
Parameter ASEC.updateSellFees(uint256,uint256)._marketingFeeOnSell (contracts/Token.sol#788) is not in mixedCase
Parameter ASEC.updateWalletToWalletTransferFee(uint256)._walletToWalletTransferFee (contracts/Token.sol#798) is not in mixedCase
Parameter ASEC.changeMarketingWallet(address)._marketingWallet (contracts/Token.sol#804) is not in mixedCase
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#conformance-to-solidity-naming-conventions

Redundant expression "this (contracts/Token.sol#473)" inContext (contracts/Token.sol#467-476)
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#redundant-statements

Variable IUniswapV2Router01.addLiquidity(address,address,uint256,uint256,uint256,uint256,address,uint256).amountADesired (contracts/Token.sol#80) is too similar to IUniswapV2Router01.a
ddLiquidity(address,address,uint256,uint256,uint256,uint256,address,uint256).amountBDesired (contracts/Token.sol#81)
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#variable-names-too-similar

ASEC.uniswapV2Pair (contracts/Token.sol#672) should be immutable
ASEC.uniswapV2Router (contracts/Token.sol#671) 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/0xc0a7637cdb7a856bdf16b6537cc9caf0f2a5c140aae17624cb449ee94a07c845

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

https://testnet.bscscan.com/tx/0xbeb36c67709b77068a3d80d8542781dbb88444be8b1cd3d92c95140033e268b9

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

https://testnet.bscscan.com/tx/0x957956dc1f2d02932c2119b827050ab07685413d1dc2527d393e62cb3924c7e6

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

https://testnet.bscscan.com/tx/0x6485a800d91a7d38f6fc3934eda97a8f7da7aac15530a863d70629d6cb10b847

5- Buying when not excluded from fees (0-12% tax) (passed):

https://testnet.bscscan.com/tx/0x99c25805f4a3099d2a96cdce8fc995c6c9558b61c2028079745ef28eebb8a54e

6- Selling when not excluded from fees (0-12% tax) (passed):

https://testnet.bscscan.com/tx/0x55e61723f80354c0eba625c8e3e8b1623d195a7c3d06c06e83b695a390a7695d

FUNCTIONAL TESTING

7- Transferring when not excluded from fees (0-12% tax) **(passed):** https://testnet.bscscan.com/tx/0x4953aa8afbafc494976e132f32332143dc7818fb7630180e8d7f2d25b6728b71

8- Internal swap (BNB to marketing wallet + auto-liquidity) **(passed):** https://testnet.bscscan.com/tx/0x55e61723f80354c0eba625c8e3e8b1623d195a7c3d06c06e83b695a390a7695d

FUNCTIONAL TESTING

Centralization – Trades must be enabled

Severity: **High**

function: enableTrading

Status: Not Resolved

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() public onlyOwner {
    require(!tradingEnabled, "Trading already enabled!");
    tradingEnabled = 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 trades

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