Ether Authority

www.EtherAuthority.io
audit@etherauthority.io

SMART CONTRACT

Security Audit Report

Customer:	CateCoin
Website:	https://catecoin.club
Platform:	Binance Smart Chain
Language:	Solidity
Date:	June 16th, 2021

Table of contents

Email: audit@EtherAuthority.io

THIS IS SECURITY AUDIT REPORT DOCUMENT AND WHICH MAY CONTAIN INFORMATION WHICH IS CONFIDENTIAL. WHICH INCLUDES ANY POTENTIAL VULNERABILITIES AND MALICIOUS CODES WHICH CAN BE USED TO EXPLOIT THE SOFTWARE. THIS MUST BE REFERRED INTERNALLY AND ONLY SHOULD BE MADE AVAILABLE TO PUBLIC AFTER ISSUES ARE RESOLVED.

Email: audit@EtherAuthority.io

Introduction

We were contracted by the CateCoin team to perform the Security audit of the CateCoin Token smart contract code. The audit has been performed using manual analysis as well as using automated software tools. This report presents all the findings regarding the audit performed on June 16th, 2021.

The purpose of this audit was to address the following:

- Ensure that all claimed functions exist and function correctly.
- Identify any security vulnerabilities that may be present in the smart contract.

Project Background

CateCoin launched CateCoin with the intention to add real value to the meme world. CateCoin will allow meme creators to create and earn with their memes in a Decentralised way.

Audit scope

Name	**Code Review and Security Analysis Report for CateCoin Token Smart Contract**
Platform	**BSC / Solidity**
File	cate.sol
Smart Contract Online Code	https://bscscan.com/address/0x451329F2FCb88C398A4cDD4A8a98780B4D62873C#code
File MD5 Hash	A95F7722BEF9DD05755A0F71EEBDC465
Audit Date	June 16th, 2021
Revised contract code	https://bscscan.com/address/0xe4fae3faa8300810c835970b9187c268f55d998f#code
Revision Date	July 7th, 2021

Claimed Smart Contract Features

Claimed Feature Detail	Our Observation
Name: CateCoin	**YES, This is valid.**
Symbol: CATE	**YES, This is valid.**
Decimal: 9	**YES, This is valid.**
TaxFee: 1%	**YES, This is valid. Owner can change this fee.**
LiquidityFee: 2%	**YES, This is valid. Owner can change this fee.**
Owner can withdraw BNB from the smart contract.	**YES, This is valid.**
The owner can control following functions: • includeInReward: Owner can check includeInReward. • setRouterAddress: Owner can set router address. • excludeFromReward: Owner can check if the account is excluded or not. • includeInFee: Owner can check include fee. • setTaxFeePercent: Owner can set Tax Fee Percent. • setLiquidityFeePercent: Owner can set Liquidity Fee Percent. • setMaxTxPercent: Owner can set Max Tx Percent. • setSwapAndLiquifyEnabled: Owner can set Swap And Liquify Enabled.	**YES, This is valid. The smart contract owner control these functions, so the owner must handle the private key of the owner's wallet very securely. Because if the private key is compromised, then it will create problems.**

• transferAnyBEP20Tokens: Function to allow admin to claim *other* BEP20 tokens sent to this contract (by mistake).The Owner cannot transfer out CateCoin from this smart contract. • setWalletBanStatus: Owner can ban users till February 7th, 2424.	

Audit Summary

According to the standard audit assessment, Customer`s solidity smart contract is **secured**. These contracts also have owner functions (described in the centralization section below), which does not make everything 100% decentralized. Thus, the owner must execute those smart contract functions as per the business plan.

We used various tools like MythX, Slither and Remix IDE. At the same time this finding is based on critical analysis of the manual audit.
All issues found during automated analysis were manually reviewed and applicable vulnerabilities are presented in the Audit overview section. General overview is presented in AS-IS section and all identified issues can be found in the Audit overview section.

We found 0 critical, 0 high, 0 medium and 4 low and some very low level issues.

Technical Quick Stats

Main Category	Subcategory	Result
Contract Programming	Solidity version not specified	Passed
	Solidity version too old	Moderated
	Integer overflow/underflow	Passed
	Function input parameters lack of check	Passed
	Function input parameters check bypass	Passed
	Function access control lacks management	Passed
	Critical operation lacks event log	Moderated
	Human/contract checks bypass	Passed
	Random number generation/use vulnerability	Passed
	Fallback function misuse	Passed
	Race condition	Passed
	Logical vulnerability	Passed
	Other programming issues	Passed
Code Specification	Function visibility not explicitly declared	Passed
	Var. storage location not explicitly declared	Passed
	Use keywords/functions to be deprecated	Passed
	Other code specification issues	Passed
Gas Optimization	“Out of Gas” Issue	Passed
	High consumption ‘for/while’ loop	Moderated
	High consumption ‘storage’ storage	Passed
	Assert() misuse	Passed
Business Risk	The maximum limit for mintage not set	Passed
	“Short Address” Attack	Passed
	“Double Spend” Attack	Passed

Overall Audit Result: **PASSED**

Email: audit@EtherAuthority.io

Code Quality

This audit scope has 1 smart contract. This smart contract also contains Libraries, Smart contracts inherits and Interfaces. This is a compact and well written contract.

The libraries in the CateCoin Token are part of its logical algorithm. A library is a different type of smart contract that contains reusable code. Once deployed on the blockchain (only once), it is assigned a specific address and its properties / methods can be reused many times by other contracts in the CateCoin Token.

The CateCoin team has **not** provided scenario and unit test scripts, which would have helped to determine the integrity of the code in an automated way.

Some code parts are **not well** commented on smart contracts.

Documentation

We were given CateCoin Token smart contract code in the form of a BscScan web link. The hashes of that code are mentioned above in the table.

As mentioned above, some code parts are **not well** commented. So it is difficult to quickly understand the programming flow as well as complex code logic. Comments are very helpful in understanding the overall architecture of the protocol.

Another source of information was its official website https://catecoin.club/ which provided rich information about the project architecture and tokenomics.

Use of Dependencies

As per our observation, the libraries are used in this smart contract infrastructure that are based on well known industry standard open source projects. And their core code blocks are written well.

Apart from libraries, its functions are used in external smart contract calls.

AS-IS overview

(1) Interface

(a) Token

(b) IERC20

(c) IUniswapV2Factory

(d) IUniswapV2Pair

(e) IUniswapV2Router01

(f) IUniswapV2Router02

(g) IERC20Metadata

(2) Inherited contracts

(a) Context

(b) Ownable

(c) IERC20

(3) Usages

(a) using SafeMath for uint256;

(b) using Address for address;

(4) Events

(a) event OwnershipTransferred(address indexed previousOwner,address indexed newOwner);

(b) event MinTokensBeforeSwapUpdated(uint256 minTokensBeforeSwap);

(c) event SwapAndLiquifyEnabledUpdated(bool enabled);

(d) event SwapAndLiquify(uint256 tokensSwapped,uint256 ethReceived, uint256 tokensIntoLiqudity);

(e) event WalletBanStatusUpdated(address user, bool banned);

(5) Functions

Sl.	Functions	Type	Observation	Conclusion
1	lockTheSwap	modifier	Passed	No Issue
2	setRouterAddress	write	access only Owner	No Issue
3	name	read	Passed	No Issue
4	symbol	read	Passed	No Issue
5	decimals	read	Passed	No Issue
6	totalSupply	read	Passed	No Issue
7	balanceOf	read	Passed	No Issue
8	transfer	write	access only Owner	No Issue
9	allowance	read	Passed	No Issue
10	approve	write	Passed	No Issue
11	transferFrom	write	Passed	No Issue
12	increaseAllowance	write	Passed	No Issue
13	decreaseAllowance	write	Passed	No Issue
14	isExcludedFromReward	read	Passed	No Issue
15	totalFees	read	Passed	No Issue
16	deliver	write	external instead of public	Refer Audit Findings
17	reflectionFromToken	write	external instead of public	Refer Audit Findings
18	tokenFromReflection	read	Passed	No Issue
19	excludeFromReward	write	access only Owner	No Issue
20	includeInReward	external	Infinite loop possibility	Refer Audit Findings
21	_transferBothExcluded	write	Passed	No Issue
22	excludeFromFee	write	Missing Events	No Issue
23	includeInFee	write	Missing Events	No Issue
24	setTaxFeePercent	external	Missing Events	No Issue
25	setLiquidityFeePercent	external	Missing Events	No Issue
26	setBurnFeePercent	external	Removed	No Issue
27	setSwapAndLiquifyEnabled	external	Missing Events	No Issue
28	rescueBNBFromContract	external	Missing Events	No Issue
29	transferAnyBEP20Tokens	write	Missing Events	No Issue
30	burn	external	Removed	No Issue
31	_burn	internal	Removed	No Issue
32	setWalletBanStatus	external	access only Owner	No Issue
33	_reflectFee	write	Passed	No Issue
34	_getValues	internal	Passed	No Issue
35	_getTValues	read	Passed	No Issue
36	_getRValues	write	Passed	No Issue
37	_getRate	read	Passed	No Issue
38	_getCurrentSupply	read	Passed	No Issue

39	_takeLiquidity	write	Passed	No Issue
40	calculateTaxFee	read	Passed	No Issue
41	calculateLiquidityFee	read	Passed	No Issue
42	calculateBurnFee	read	Removed	No Issue
43	removeAllFee	write	Passed	No Issue
44	restoreAllFee	write	Passed	No Issue
45	isExcludedFromFee	read	Passed	No Issue
46	_approve	write	Passed	No Issue
47	_transfer	write	Passed	No Issue
48	swapAndLiquify	write	Passed	No Issue
49	swapTokensForEth	write	Passed	No Issue
50	addLiquidity	write	Centralized risk in addLiquidity	Refer Audit Findings
51	_tokenTransfer	write	Passed	No Issue
52	_transferStandard	write	Passed	No Issue
53	_transferToExcluded	write	Passed	No Issue
54	_transferFromExcluded	write	Passed	No Issue
55	owner	read	Passed	No Issue
56	onlyOwner	modifier	Passed	No Issue
57	renounceOwnership	write	access only Owner	No Issue
58	transferOwnership	write	access only Owner	No Issue
59	geUnlockTime	read	Passed	No Issue
60	_msgSender	internal	Passed	No Issue
61	_msgData	internal	Passed	No Issue

Severity Definitions

Risk Level	Description
Critical	Critical vulnerabilities are usually straightforward to exploit and can lead to token loss etc.
High	High-level vulnerabilities are difficult to exploit; however, they also have significant impact on smart contract execution, e.g. public access to crucial functions
Medium	Medium-level vulnerabilities are important to fix; however, they can't lead to tokens lose
Low	Low-level vulnerabilities are mostly related to outdated, unused etc. code snippets, that can't have significant impact on execution
Lowest / Code Style / Best Practice	Lowest-level vulnerabilities, code style violations and info statements can't affect smart contract execution and can be ignored.

Audit Findings

Critical

No critical severity vulnerabilities were found.

High

No high severity vulnerabilities were found.

Medium

No Medium severity vulnerabilities were found.

Low

(1) Infinite loop possibility:

```
function includeInReward(address account) external onlyOwner() {
    require(_isExcluded[account], "Account is already excluded");
    for (uint256 i = 0; i < _excluded.length; i++) {
        if (_excluded[i] == account) {
            _excluded[i] = _excluded[_excluded.length - 1];
            _tOwned[account] = 0;
            _isExcluded[account] = false;
            _excluded.pop();
            break;
        }
    }
}
```

If there are so many excluded wallets, then this logic will fail, as it might hit the block's gas limit. If there are very limited exceptions, then this will work, but will cost more gas.

Resolution: We suggest excluding limited wallets only.

(2) Make variables constant:

```
string private _name = "CateCoin";
string private _symbol = "CATE";
uint8 private _decimals = 9;
```

Following variables will be unchanged. So, please make it constant. It will save some gas.

- name
- symbol
- decimals

Resolution: Declare those variables as constant. Just put a constant keyword.

(3) Centralized risk in addLiquidity:

```
function addLiquidity(uint256 tokenAmount, uint256 ethAmount) private {
    // approve token transfer to cover all possible scenarios
    _approve(address(this), address(uniswapV2Router), tokenAmount);

    // add the liquidity
    uniswapV2Router.addLiquidityETH{value: ethAmount}(
        address(this),
        tokenAmount,
        0, // slippage is unavoidable
        0, // slippage is unavoidable
        owner(),
        block.timestamp
    );
}
```

In addLiquidityETH function, owner gets CATE Tokens from the Pool. If the private key of the owner's wallet is compromised, then it will create a problem.

Resolution: Ideally this can be a governance smart contract. On another hand, the owner can accept this risk and handle the private key very securely.

.

(4) Missing Events:

Missing Events log for some functions:

- excludeFromFee
- excludeFromReward
- includeInFee
- includeInReward
- setLiquidityFeePercent
- setMaxTxPercent
- setTaxFeePercent
- setSwapAndLiquifyEnabled
- rescueBNBFromContract
- transferAnyBEP20Tokens

Very Low / Discussion / Best practices:

(1) external instead of public:
If any function is not called from inside the smart contract, then it is better to declare it as external instead of public. As it saves some gas as well.
https://ethereum.stackexchange.com/questions/19380/external-vs-public-best-practices

Centralization

This smart contract has some functions which can be executed by Admin (Owner) only. If the admin wallet private key would be compromised, then it would create trouble. Following are Admin functions:

- excludeFromReward: Owner can check if the account is excluded or not.
- setRouterAddress: Owner can set router address.
- includeInReward: Owner can check includeInReward.
- includeInFee: Owner can check includeInFee.
- setTaxFeePercent: Owner can set Tax Fee Percent.
- setLiquidityFeePercent: Owner can set Liquidity Fee Percent.
- setMaxTxPercent: Owner can set Max Tx Percent.
- setSwapAndLiquifyEnabled: Owner can set Swap And Liquify Enabled.
- rescueBNBFromContract: Owner can allow rescue BNB sent by mistake directly to the contract.
- transferAnyBEP20Tokens: Function to allow admin to claim *other* BEP20 tokens sent to this contract (by mistake).The Owner cannot transfer out Catecoin from this smart contract.
- setWalletBanStatus: Owner can set wallet address and ban status.

Conclusion

We were given a contract code. And we have used all possible tests based on given objects as files. We observed some issues in the smart contracts and those are fixed/acknowledged in the smart contracts. **So it is good to go for the production.**

Since possible test cases can be unlimited for such smart contracts protocol, we provide no such guarantee of future outcomes. We have used all the latest static tools and manual observations to cover maximum possible test cases to scan everything.

Smart contracts within the scope were manually reviewed and analyzed with static analysis tools. Smart Contract's high level description of functionality was presented in As-is overview section of the report.

Audit report contains all found security vulnerabilities and other issues in the reviewed code.

Security state of the reviewed contract, based on standard audit procedure scope, is **"Secured".**

Our Methodology

We like to work with a transparent process and make our reviews a collaborative effort. The goals of our security audits are to improve the quality of systems we review and aim for sufficient remediation to help protect users. The following is the methodology we use in our security audit process.

Manual Code Review:

In manually reviewing all of the code, we look for any potential issues with code logic, error handling, protocol and header parsing, cryptographic errors, and random number generators. We also watch for areas where more defensive programming could reduce the risk of future mistakes and speed up future audits. Although our primary focus is on the in-scope code, we examine dependency code and behavior when it is relevant to a particular line of investigation.

Vulnerability Analysis:

Our audit techniques included manual code analysis, user interface interaction, and whitebox penetration testing. We look at the project's web site to get a high level understanding of what functionality the software under review provides. We then meet with the developers to gain an appreciation of their vision of the software. We install and use the relevant software, exploring the user interactions and roles. While we do this, we brainstorm threat models and attack surfaces. We read design documentation, review other audit results, search for similar projects, examine source code dependencies, skim open issue tickets, and generally investigate details other than the implementation.

Documenting Results:

We follow a conservative, transparent process for analyzing potential security vulnerabilities and seeing them through successful remediation. Whenever a potential issue is discovered, we immediately create an Issue entry for it in this document, even though we have not yet verified the feasibility and impact of the issue. This process is conservative because we document our suspicions early even if they are later shown to not represent exploitable vulnerabilities. We generally follow a process of first documenting the suspicion with unresolved questions, then confirming the issue through code analysis, live experimentation, or automated tests. Code analysis is the most tentative, and we strive to provide test code, log captures, or screenshots demonstrating our confirmation. After this we analyze the feasibility of an attack in a live system.

Suggested Solutions:

We search for immediate mitigations that live deployments can take, and finally we suggest the requirements for remediation engineering for future releases. The mitigation and remediation recommendations should be scrutinized by the developers and deployment engineers, and successful mitigation and remediation is an ongoing collaborative process after we deliver our report, and before the details are made public.

Disclaimers

EtherAuthority.io Disclaimer

EtherAuthority team has analyzed this smart contract in accordance with the best industry practices at the date of this report, in relation to: cybersecurity vulnerabilities and issues in smart contract source code, the details of which are disclosed in this report, (Source Code); the Source Code compilation, deployment and functionality (performing the intended functions).

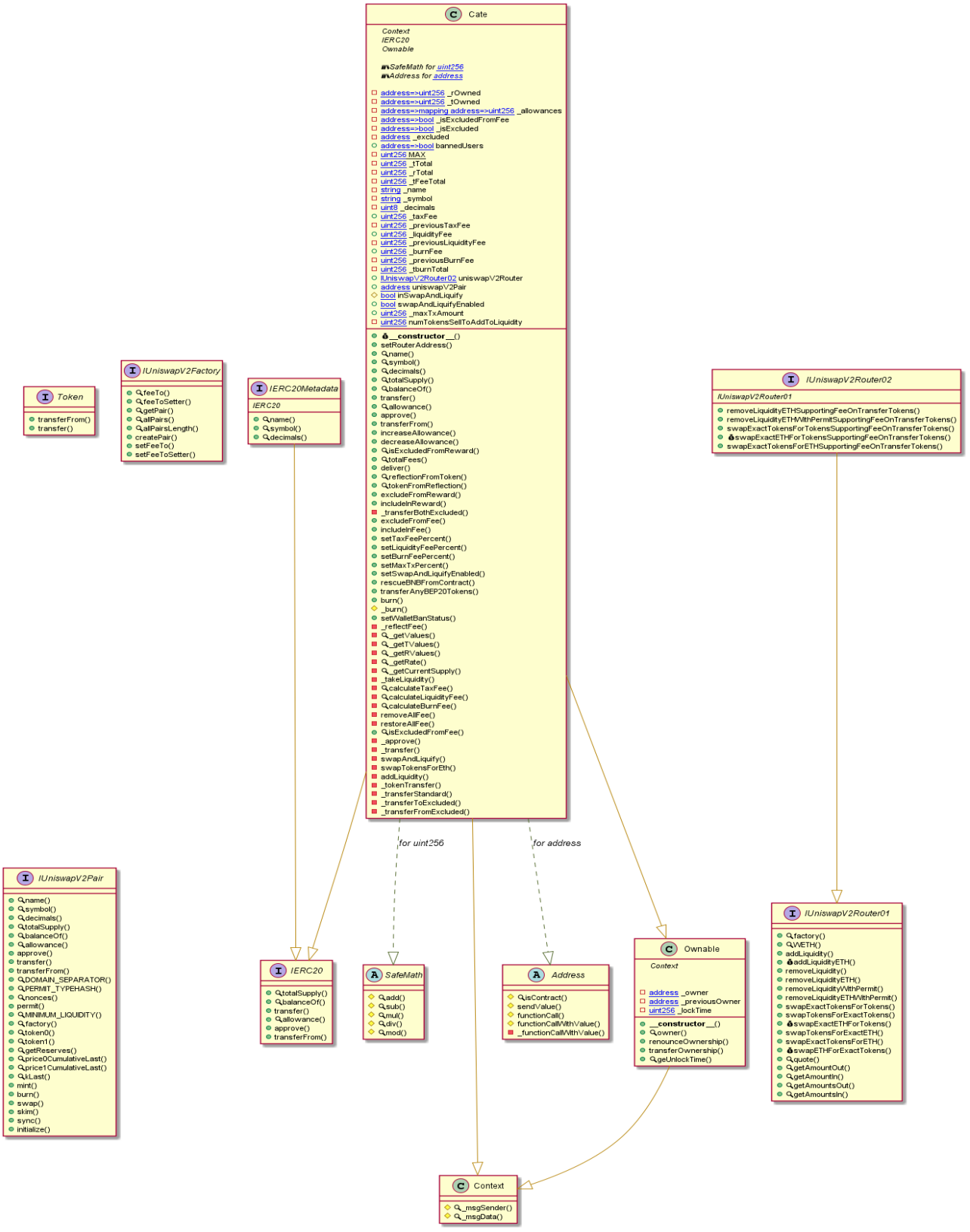
Due to the fact that the total number of test cases are unlimited, the audit makes no statements or warranties on security of the code. It also cannot be considered as a sufficient assessment regarding the utility and safety of the code, bugfree status or any other statements of the contract. While we have done our best in conducting the analysis and producing this report, it is important to note that you should not rely on this report only. We also suggest conducting a bug bounty program to confirm the high level of security of this smart contract.

Technical Disclaimer

Smart contracts are deployed and executed on the blockchain platform. The platform, its programming language, and other software related to the smart contract can have their own vulnerabilities that can lead to hacks. Thus, the audit can’t guarantee explicit security of the audited smart contracts.

Appendix

Code Flow Diagram - Cate Token



Slither Results Log

Slither log >> Cate.sol

```
INFO:Detectors:
Cate.rescueBNBFromContract() (Cate.sol#1198-1201) sends eth to arbitrary user
	Dangerous calls:
	- _owner.transfer(address(this).balance) (Cate.sol#1200)
Cate.addLiquidity(uint256,uint256) (Cate.sol#1478-1491) sends eth to arbitrary user
	Dangerous calls:
	- uniswapV2Router.addLiquidityETH{value:
ethAmount}(address(this),tokenAmount,0,0,owner(),block.timestamp) (Cate.sol#1483-1490)
Reference:
https://github.com/crytic/slither/wiki/Detector-Documentation#functions-that-send-ether-to-arbitrary-destinatio
ns
INFO:Detectors:
Reentrancy in Cate._transfer(address,address,uint256) (Cate.sol#1385-1435):
	External calls:
	- swapAndLiquify(contractTokenBalance) (Cate.sol#1422)
		- uniswapV2Router.addLiquidityETH{value:
ethAmount}(address(this),tokenAmount,0,0,owner(),block.timestamp) (Cate.sol#1483-1490)
		-
uniswapV2Router.swapExactTokensForETHSupportingFeeOnTransferTokens(tokenAmount,0,path,address(t
his),block.timestamp) (Cate.sol#1469-1475)
	External calls sending eth:
	- swapAndLiquify(contractTokenBalance) (Cate.sol#1422)
		- uniswapV2Router.addLiquidityETH{value:
ethAmount}(address(this),tokenAmount,0,0,owner(),block.timestamp) (Cate.sol#1483-1490)
	State variables written after the call(s):
	- _tokenTransfer(from,to,amount,takeFee) (Cate.sol#1434)
		- _rOwned[account] = _rOwned[account].sub(amount,ERC20: burn amount exceeds balance)
(Cate.sol#1219)
		- _rOwned[address(this)] = _rOwned[address(this)].add(rLiquidity) (Cate.sol#1328)
		- _rOwned[sender] = _rOwned[sender].sub(rAmount) (Cate.sol#1553)
		- _rOwned[sender] = _rOwned[sender].sub(rAmount) (Cate.sol#1530)
		- _rOwned[sender] = _rOwned[sender].sub(rAmount) (Cate.sol#1155)
		- _rOwned[recipient] = _rOwned[recipient].add(rTransferAmount) (Cate.sol#1531)
		- _rOwned[sender] = _rOwned[sender].sub(rAmount) (Cate.sol#1578)
		- _rOwned[recipient] = _rOwned[recipient].add(rTransferAmount) (Cate.sol#1579)
		- _rOwned[recipient] = _rOwned[recipient].add(rTransferAmount) (Cate.sol#1555)
		- _rOwned[recipient] = _rOwned[recipient].add(rTransferAmount) (Cate.sol#1157)
	- _tokenTransfer(from,to,amount,takeFee) (Cate.sol#1434)
		- _rTotal = _rTotal.sub(rFee) (Cate.sol#1238)
	- _tokenTransfer(from,to,amount,takeFee) (Cate.sol#1434)
		- _tOwned[address(this)] = _tOwned[address(this)].add(tLiquidity) (Cate.sol#1330)
		- _tOwned[sender] = _tOwned[sender].sub(tAmount) (Cate.sol#1154)
		- _tOwned[sender] = _tOwned[sender].sub(tAmount) (Cate.sol#1577)
		- _tOwned[recipient] = _tOwned[recipient].add(tTransferAmount) (Cate.sol#1554)
		- _tOwned[recipient] = _tOwned[recipient].add(tTransferAmount) (Cate.sol#1156)
	- _tokenTransfer(from,to,amount,takeFee) (Cate.sol#1434)
		- _tTotal = _tTotal.sub(amount) (Cate.sol#1220)
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#reentrancy-vulnerabilities
INFO:Detectors:
Cate.transferAnyBEP20Tokens(address,address,uint256) (Cate.sol#1205-1208) ignores return value by
Token(_tokenAddr).transfer(_to,_amount) (Cate.sol#1207)
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#unchecked-transfer
INFO:Detectors:
Ownable._lockTime (Cate.sol#464) is never initialized. It is used in:
	- Ownable.geUnlockTime() (Cate.sol#520-522)
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#uninitialized-state-variables
INFO:Detectors:
```

Cate.addLiquidity(uint256,uint256) (Cate.sol#1478-1491) ignores return value by uniswapV2Router.addLiquidityETH{value: ethAmount}(address(this),tokenAmount,0,0,owner(),block.timestamp) (Cate.sol#1483-1490)
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#unused-return
INFO:Detectors:
Cate.allowance(address,address).owner (Cate.sol#1007) shadows:
- Ownable.owner() (Cate.sol#483-485) (function)
Cate.rescueBNBFromContract()._owner (Cate.sol#1199) shadows:
- Ownable._owner (Cate.sol#462) (state variable)
Cate._approve(address,address,uint256).owner (Cate.sol#1374) shadows:
- Ownable.owner() (Cate.sol#483-485) (function)
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#local-variable-shadowing
INFO:Detectors:
Reentrancy in Cate._transfer(address,address,uint256) (Cate.sol#1385-1435):
External calls:
- swapAndLiquify(contractTokenBalance) (Cate.sol#1422)
- uniswapV2Router.addLiquidityETH{value: ethAmount}(address(this),tokenAmount,0,0,owner(),block.timestamp) (Cate.sol#1483-1490)
- uniswapV2Router.swapExactTokensForETHSupportingFeeOnTransferTokens(tokenAmount,0,path,address(this),block.timestamp) (Cate.sol#1469-1475)
External calls sending eth:
- swapAndLiquify(contractTokenBalance) (Cate.sol#1422)
- uniswapV2Router.addLiquidityETH{value: ethAmount}(address(this),tokenAmount,0,0,owner(),block.timestamp) (Cate.sol#1483-1490)
State variables written after the call(s):
- _tokenTransfer(from,to,amount,takeFee) (Cate.sol#1434)
- _burnFee = _previousBurnFee (Cate.sol#1366)
- _burnFee = 0 (Cate.sol#1360)
- _tokenTransfer(from,to,amount,takeFee) (Cate.sol#1434)
- _liquidityFee = _previousLiquidityFee (Cate.sol#1365)
- _liquidityFee = 0 (Cate.sol#1359)
- _tokenTransfer(from,to,amount,takeFee) (Cate.sol#1434)
- _previousBurnFee = _burnFee (Cate.sol#1356)
- _tokenTransfer(from,to,amount,takeFee) (Cate.sol#1434)
- _previousLiquidityFee = _liquidityFee (Cate.sol#1355)
- _tokenTransfer(from,to,amount,takeFee) (Cate.sol#1434)
- _previousTaxFee = _taxFee (Cate.sol#1354)
- _tokenTransfer(from,to,amount,takeFee) (Cate.sol#1434)
- _tFeeTotal = _tFeeTotal.add(tFee) (Cate.sol#1239)
- _tokenTransfer(from,to,amount,takeFee) (Cate.sol#1434)
- _taxFee = _previousTaxFee (Cate.sol#1364)
- _taxFee = 0 (Cate.sol#1358)
- _tokenTransfer(from,to,amount,takeFee) (Cate.sol#1434)
- _tburnTotal = _tburnTotal.add(amount) (Cate.sol#1221)
Reentrancy in Cate.constructor() (Cate.sol#954-968):
External calls:
- setRouterAddress(0x05fF2B0DB69458A0750badebc4f9e13aDd608C7F) (Cate.sol#957)
- uniswapV2Pair = IUniswapV2Factory(_uniswapV2Router.factory()).createPair(address(this),_uniswapV2Router.WETH()) (Cate.sol#973)
State variables written after the call(s):
- _isExcludedFromFee[owner()] = true (Cate.sol#962)
- _isExcludedFromFee[address(this)] = true (Cate.sol#963)
- _isExcludedFromFee[address(0x000000000000000000000000000000000000dEaD)] = true (Cate.sol#964)
Reentrancy in Cate.setRouterAddress(address) (Cate.sol#970-975):
External calls:
- uniswapV2Pair = IUniswapV2Factory(_uniswapV2Router.factory()).createPair(address(this),_uniswapV2Router.WETH()) (Cate.sol#973)
State variables written after the call(s):
- uniswapV2Router = _uniswapV2Router (Cate.sol#974)
Reentrancy in Cate.swapAndLiquify(uint256) (Cate.sol#1437-1458):
External calls:

- swapTokensForEth(half) (Cate.sol#1449)
- uniswapV2Router.swapExactTokensForETHSupportingFeeOnTransferTokens(tokenAmount,0,path,address(this),block.timestamp) (Cate.sol#1469-1475)
- addLiquidity(otherHalf,newBalance) (Cate.sol#1455)
- uniswapV2Router.addLiquidityETH{value: ethAmount}(address(this),tokenAmount,0,0,owner(),block.timestamp) (Cate.sol#1483-1490)

External calls sending eth:
- addLiquidity(otherHalf,newBalance) (Cate.sol#1455)
- uniswapV2Router.addLiquidityETH{value: ethAmount}(address(this),tokenAmount,0,0,owner(),block.timestamp) (Cate.sol#1483-1490)

State variables written after the call(s):
- addLiquidity(otherHalf,newBalance) (Cate.sol#1455)
- _allowances[owner][spender] = amount (Cate.sol#1381)

Reentrancy in Cate.transferFrom(address,address,uint256) (Cate.sol#1025-1040):

External calls:
- _transfer(sender,recipient,amount) (Cate.sol#1030)
- uniswapV2Router.addLiquidityETH{value: ethAmount}(address(this),tokenAmount,0,0,owner(),block.timestamp) (Cate.sol#1483-1490)
- uniswapV2Router.swapExactTokensForETHSupportingFeeOnTransferTokens(tokenAmount,0,path,address(this),block.timestamp) (Cate.sol#1469-1475)

External calls sending eth:
- _transfer(sender,recipient,amount) (Cate.sol#1030)
- uniswapV2Router.addLiquidityETH{value: ethAmount}(address(this),tokenAmount,0,0,owner(),block.timestamp) (Cate.sol#1483-1490)

State variables written after the call(s):
- _approve(sender,_msgSender(),_allowances[sender][_msgSender()].sub(amount,ERC20: transfer amount exceeds allowance)) (Cate.sol#1031-1038)
- _allowances[owner][spender] = amount (Cate.sol#1381)

Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#reentrancy-vulnerabilities-2

INFO:Detectors:

Reentrancy in Cate._transfer(address,address,uint256) (Cate.sol#1385-1435):

External calls:
- swapAndLiquify(contractTokenBalance) (Cate.sol#1422)
- uniswapV2Router.addLiquidityETH{value: ethAmount}(address(this),tokenAmount,0,0,owner(),block.timestamp) (Cate.sol#1483-1490)
- uniswapV2Router.swapExactTokensForETHSupportingFeeOnTransferTokens(tokenAmount,0,path,address(this),block.timestamp) (Cate.sol#1469-1475)

External calls sending eth:
- swapAndLiquify(contractTokenBalance) (Cate.sol#1422)
- uniswapV2Router.addLiquidityETH{value: ethAmount}(address(this),tokenAmount,0,0,owner(),block.timestamp) (Cate.sol#1483-1490)

Event emitted after the call(s):
- Transfer(sender,recipient,tTransferAmount) (Cate.sol#1583)
- _tokenTransfer(from,to,amount,takeFee) (Cate.sol#1434)
- Transfer(sender,recipient,tTransferAmount) (Cate.sol#1537)
- _tokenTransfer(from,to,amount,takeFee) (Cate.sol#1434)
- Transfer(sender,recipient,tTransferAmount) (Cate.sol#1161)
- _tokenTransfer(from,to,amount,takeFee) (Cate.sol#1434)
- Transfer(sender,recipient,tTransferAmount) (Cate.sol#1561)
- _tokenTransfer(from,to,amount,takeFee) (Cate.sol#1434)

Reentrancy in Cate.constructor() (Cate.sol#954-968):

External calls:
- setRouterAddress(0x05fF2B0DB69458A0750badebc4f9e13aDd608C7F) (Cate.sol#957)
- uniswapV2Pair = IUniswapV2Factory(_uniswapV2Router.factory()).createPair(address(this),_uniswapV2Router.WETH()) (Cate.sol#973)

Event emitted after the call(s):
- Transfer(address(0),_msgSender(),_tTotal) (Cate.sol#967)

Reentrancy in Cate.swapAndLiquify(uint256) (Cate.sol#1437-1458):

External calls:
- swapTokensForEth(half) (Cate.sol#1449)

-
uniswapV2Router.swapExactTokensForETHSupportingFeeOnTransferTokens(tokenAmount,0,path,address(this),block.timestamp) (Cate.sol#1469-1475)
- addLiquidity(otherHalf,newBalance) (Cate.sol#1455)
- uniswapV2Router.addLiquidityETH{value:
ethAmount}(address(this),tokenAmount,0,0,owner(),block.timestamp) (Cate.sol#1483-1490)
External calls sending eth:
- addLiquidity(otherHalf,newBalance) (Cate.sol#1455)
- uniswapV2Router.addLiquidityETH{value:
ethAmount}(address(this),tokenAmount,0,0,owner(),block.timestamp) (Cate.sol#1483-1490)
Event emitted after the call(s):
- Approval(owner,spender,amount) (Cate.sol#1382)
- addLiquidity(otherHalf,newBalance) (Cate.sol#1455)
- SwapAndLiquify(half,newBalance,otherHalf) (Cate.sol#1457)
Reentrancy in Cate.transferFrom(address,address,uint256) (Cate.sol#1025-1040):
External calls:
- _transfer(sender,recipient,amount) (Cate.sol#1030)
- uniswapV2Router.addLiquidityETH{value:
ethAmount}(address(this),tokenAmount,0,0,owner(),block.timestamp) (Cate.sol#1483-1490)
-
uniswapV2Router.swapExactTokensForETHSupportingFeeOnTransferTokens(tokenAmount,0,path,address(this),block.timestamp) (Cate.sol#1469-1475)
External calls sending eth:
- _transfer(sender,recipient,amount) (Cate.sol#1030)
- uniswapV2Router.addLiquidityETH{value:
ethAmount}(address(this),tokenAmount,0,0,owner(),block.timestamp) (Cate.sol#1483-1490)
Event emitted after the call(s):
- Approval(owner,spender,amount) (Cate.sol#1382)
- _approve(sender,_msgSender(),_allowances[sender][_msgSender()].sub(amount,ERC20:
transfer amount exceeds allowance)) (Cate.sol#1031-1038)
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#reentrancy-vulnerabilities-3
INFO:Detectors:
Cate.setWalletBanStatus(address,bool) (Cate.sol#1227-1235) uses timestamp for comparisons
Dangerous comparisons:
- require(bool,string)(1618531200 + 259200 > block.timestamp,Owner cannot longer ban wallets)
(Cate.sol#1229)
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#block-timestamp
INFO:Detectors:
Address.isContract(address) (Cate.sol#292-304) uses assembly
- INLINE ASM (Cate.sol#300-302)
Address._functionCallWithValue(address,bytes,uint256,string) (Cate.sol#419-446) uses assembly
- INLINE ASM (Cate.sol#438-441)
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#assembly-usage
INFO:Detectors:
Cate._transfer(address,address,uint256) (Cate.sol#1385-1435) compares to a boolean constant:
-require(bool,string)(bannedUsers[to] == false,Recipient is banned) (Cate.sol#1394)
Cate._transfer(address,address,uint256) (Cate.sol#1385-1435) compares to a boolean constant:
-require(bool,string)(bannedUsers[from] == false,Sender is banned) (Cate.sol#1393)
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#boolean-equality
INFO:Detectors:
Address._functionCallWithValue(address,bytes,uint256,string) (Cate.sol#419-446) is never used and should be removed
Address.functionCall(address,bytes) (Cate.sol#354-359) is never used and should be removed
Address.functionCall(address,bytes,string) (Cate.sol#367-373) is never used and should be removed
Address.functionCallWithValue(address,bytes,uint256) (Cate.sol#386-398) is never used and should be removed
Address.functionCallWithValue(address,bytes,uint256,string) (Cate.sol#406-417) is never used and should be removed
Address.isContract(address) (Cate.sol#292-304) is never used and should be removed
Address.sendValue(address,uint256) (Cate.sol#322-334) is never used and should be removed
Context._msgData() (Cate.sol#265-268) is never used and should be removed
SafeMath.mod(uint256,uint256) (Cate.sol#234-236) is never used and should be removed
SafeMath.mod(uint256,uint256,string) (Cate.sol#250-257) is never used and should be removed
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#dead-code
INFO:Detectors:

Cate._rTotal (Cate.sol#912) is set pre-construction with a non-constant function or state variable:
- (MAX - (MAX % _tTotal))
Cate._previousTaxFee (Cate.sol#920) is set pre-construction with a non-constant function or state variable:
- _taxFee
Cate._previousLiquidityFee (Cate.sol#923) is set pre-construction with a non-constant function or state variable:
- _liquidityFee
Cate._previousBurnFee (Cate.sol#926) is set pre-construction with a non-constant function or state variable:
- _liquidityFee
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#function-initializing-state-variables
INFO:Detectors:
Pragma version0.8.0 (Cate.sol#3) necessitates a version too recent to be trusted. Consider deploying with 0.6.12/0.7.6
solc-0.8.0 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) (Cate.sol#322-334):
- (success) = recipient.call{value: amount}() (Cate.sol#329)
Low level call in Address._functionCallWithValue(address,bytes,uint256,string) (Cate.sol#419-446):
- (success,returndata) = target.call{value: weiValue}(data) (Cate.sol#428-429)
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#low-level-calls
INFO:Detectors:
Cate (Cate.sol#895-1586) should inherit from IERC20Metadata (Cate.sol#874-889)
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#missing-inheritance
INFO:Detectors:
Function IUniswapV2Pair.DOMAIN_SEPARATOR() (Cate.sol#588) is not in mixedCase
Function IUniswapV2Pair.PERMIT_TYPEHASH() (Cate.sol#590) is not in mixedCase
Function IUniswapV2Pair.MINIMUM_LIQUIDITY() (Cate.sol#621) is not in mixedCase
Function IUniswapV2Router01.WETH() (Cate.sol#669) is not in mixedCase
Parameter Cate.setSwapAndLiquifyEnabled(bool)._enabled (Cate.sol#1189) is not in mixedCase
Parameter Cate.transferAnyBEP20Tokens(address,address,uint256)._tokenAddr (Cate.sol#1205) is not in mixedCase
Parameter Cate.transferAnyBEP20Tokens(address,address,uint256)._to (Cate.sol#1205) is not in mixedCase
Parameter Cate.transferAnyBEP20Tokens(address,address,uint256)._amount (Cate.sol#1205) is not in mixedCase
Parameter Cate.calculateTaxFee(uint256)._amount (Cate.sol#1333) is not in mixedCase
Parameter Cate.calculateLiquidityFee(uint256)._amount (Cate.sol#1337) is not in mixedCase
Parameter Cate.calculateBurnFee(uint256)._amount (Cate.sol#1345) is not in mixedCase
Variable Cate._taxFee (Cate.sol#919) is not in mixedCase
Variable Cate._liquidityFee (Cate.sol#922) is not in mixedCase
Variable Cate._burnFee (Cate.sol#925) is not in mixedCase
Variable Cate._maxTxAmount (Cate.sol#936) is not in mixedCase
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#conformance-to-solidity-naming-conventions
INFO:Detectors:
Redundant expression "this (Cate.sol#266)" inContext (Cate.sol#260-269)
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#redundant-statements
INFO:Detectors:
Variable IUniswapV2Router01.addLiquidity(address,address,uint256,uint256,uint256,uint256,address,uint256).amountADesired (Cate.sol#674) is too similar to IUniswapV2Router01.addLiquidity(address,address,uint256,uint256,uint256,uint256,address,uint256).amountBDesired (Cate.sol#675)
Variable Cate._transferBothExcluded(address,address,uint256).rTransferAmount (Cate.sol#1148) is too similar to Cate._getValues(uint256).tTransferAmount (Cate.sol#1254)
Variable Cate._transferBothExcluded(address,address,uint256).rTransferAmount (Cate.sol#1148) is too similar to Cate._transferFromExcluded(address,address,uint256).tTransferAmount (Cate.sol#1573)
Variable Cate._getValues(uint256).rTransferAmount (Cate.sol#1256) is too similar to Cate._getValues(uint256).tTransferAmount (Cate.sol#1254)
Variable Cate._getValues(uint256).rTransferAmount (Cate.sol#1256) is too similar to Cate._transferFromExcluded(address,address,uint256).tTransferAmount (Cate.sol#1573)
Variable Cate._transferBothExcluded(address,address,uint256).rTransferAmount (Cate.sol#1148) is too similar to Cate._transferBothExcluded(address,address,uint256).tTransferAmount (Cate.sol#1150)

Variable Cate._getRValues(uint256,uint256,uint256,uint256).rTransferAmount (Cate.sol#1300) is too similar to Cate._getTValues(uint256).tTransferAmount (Cate.sol#1279)
Variable Cate._transferBothExcluded(address,address,uint256).rTransferAmount (Cate.sol#1148) is too similar to Cate._getTValues(uint256).tTransferAmount (Cate.sol#1279)
Variable Cate._getValues(uint256).rTransferAmount (Cate.sol#1256) is too similar to Cate._transferBothExcluded(address,address,uint256).tTransferAmount (Cate.sol#1150)
Variable Cate._transferToExcluded(address,address,uint256).rTransferAmount (Cate.sol#1547) is too similar to Cate._transferFromExcluded(address,address,uint256).tTransferAmount (Cate.sol#1573)
Variable Cate._getRValues(uint256,uint256,uint256,uint256).rTransferAmount (Cate.sol#1300) is too similar to Cate._getValues(uint256).tTransferAmount (Cate.sol#1254)
Variable Cate._getValues(uint256).rTransferAmount (Cate.sol#1256) is too similar to Cate._transferStandard(address,address,uint256).tTransferAmount (Cate.sol#1526)
Variable Cate._getRValues(uint256,uint256,uint256,uint256).rTransferAmount (Cate.sol#1300) is too similar to Cate._transferFromExcluded(address,address,uint256).tTransferAmount (Cate.sol#1573)
Variable Cate._transferFromExcluded(address,address,uint256).rTransferAmount (Cate.sol#1571) is too similar to Cate._transferFromExcluded(address,address,uint256).tTransferAmount (Cate.sol#1573)
Variable Cate._transferStandard(address,address,uint256).rTransferAmount (Cate.sol#1524) is too similar to Cate._transferStandard(address,address,uint256).tTransferAmount (Cate.sol#1526)
Variable Cate._getValues(uint256).rTransferAmount (Cate.sol#1256) is too similar to Cate._transferToExcluded(address,address,uint256).tTransferAmount (Cate.sol#1549)
Variable Cate._getRValues(uint256,uint256,uint256,uint256).rTransferAmount (Cate.sol#1300) is too similar to Cate._transferToExcluded(address,address,uint256).tTransferAmount (Cate.sol#1549)
Variable Cate._transferFromExcluded(address,address,uint256).rTransferAmount (Cate.sol#1571) is too similar to Cate._transferToExcluded(address,address,uint256).tTransferAmount (Cate.sol#1549)
Variable Cate._transferToExcluded(address,address,uint256).rTransferAmount (Cate.sol#1547) is too similar to Cate._transferStandard(address,address,uint256).tTransferAmount (Cate.sol#1526)
Variable Cate._transferBothExcluded(address,address,uint256).rTransferAmount (Cate.sol#1148) is too similar to Cate._transferToExcluded(address,address,uint256).tTransferAmount (Cate.sol#1549)
Variable Cate._getRValues(uint256,uint256,uint256,uint256).rTransferAmount (Cate.sol#1300) is too similar to Cate._transferStandard(address,address,uint256).tTransferAmount (Cate.sol#1526)
Variable Cate._transferFromExcluded(address,address,uint256).rTransferAmount (Cate.sol#1571) is too similar to Cate._transferStandard(address,address,uint256).tTransferAmount (Cate.sol#1526)
Variable Cate._transferToExcluded(address,address,uint256).rTransferAmount (Cate.sol#1547) is too similar to Cate._transferToExcluded(address,address,uint256).tTransferAmount (Cate.sol#1549)
Variable Cate._transferBothExcluded(address,address,uint256).rTransferAmount (Cate.sol#1148) is too similar to Cate._transferStandard(address,address,uint256).tTransferAmount (Cate.sol#1526)
Variable Cate._getValues(uint256).rTransferAmount (Cate.sol#1256) is too similar to Cate._getTValues(uint256).tTransferAmount (Cate.sol#1279)
Variable Cate._getRValues(uint256,uint256,uint256,uint256).rTransferAmount (Cate.sol#1300) is too similar to Cate._transferBothExcluded(address,address,uint256).tTransferAmount (Cate.sol#1150)
Variable Cate._transferFromExcluded(address,address,uint256).rTransferAmount (Cate.sol#1571) is too similar to Cate._transferBothExcluded(address,address,uint256).tTransferAmount (Cate.sol#1150)
Variable Cate.reflectionFromToken(uint256,bool).rTransferAmount (Cate.sol#1101) is too similar to Cate._transferBothExcluded(address,address,uint256).tTransferAmount (Cate.sol#1150)
Variable Cate._transferToExcluded(address,address,uint256).rTransferAmount (Cate.sol#1547) is too similar to Cate._transferBothExcluded(address,address,uint256).tTransferAmount (Cate.sol#1150)
Variable Cate._transferFromExcluded(address,address,uint256).rTransferAmount (Cate.sol#1571) is too similar to Cate._getTValues(uint256).tTransferAmount (Cate.sol#1279)
Variable Cate.reflectionFromToken(uint256,bool).rTransferAmount (Cate.sol#1101) is too similar to Cate._getTValues(uint256).tTransferAmount (Cate.sol#1279)
Variable Cate._transferStandard(address,address,uint256).rTransferAmount (Cate.sol#1524) is too similar to Cate._transferBothExcluded(address,address,uint256).tTransferAmount (Cate.sol#1150)
Variable Cate._transferToExcluded(address,address,uint256).rTransferAmount (Cate.sol#1547) is too similar to Cate._getValues(uint256).tTransferAmount (Cate.sol#1254)
Variable Cate._transferToExcluded(address,address,uint256).rTransferAmount (Cate.sol#1547) is too similar to Cate._getTValues(uint256).tTransferAmount (Cate.sol#1279)
Variable Cate.reflectionFromToken(uint256,bool).rTransferAmount (Cate.sol#1101) is too similar to Cate._getValues(uint256).tTransferAmount (Cate.sol#1254)
Variable Cate._transferStandard(address,address,uint256).rTransferAmount (Cate.sol#1524) is too similar to Cate._getValues(uint256).tTransferAmount (Cate.sol#1254)
Variable Cate._transferStandard(address,address,uint256).rTransferAmount (Cate.sol#1524) is too similar to Cate._getTValues(uint256).tTransferAmount (Cate.sol#1279)
Variable Cate.reflectionFromToken(uint256,bool).rTransferAmount (Cate.sol#1101) is too similar to Cate._transferFromExcluded(address,address,uint256).tTransferAmount (Cate.sol#1573)

Variable Cate._transferStandard(address,address,uint256).rTransferAmount (Cate.sol#1524) is too similar to Cate._transferToExcluded(address,address,uint256).tTransferAmount (Cate.sol#1549)
Variable Cate.reflectionFromToken(uint256,bool).rTransferAmount (Cate.sol#1101) is too similar to Cate._transferToExcluded(address,address,uint256).tTransferAmount (Cate.sol#1549)
Variable Cate._transferFromExcluded(address,address,uint256).rTransferAmount (Cate.sol#1571) is too similar to Cate._getValues(uint256).tTransferAmount (Cate.sol#1254)
Variable Cate._transferStandard(address,address,uint256).rTransferAmount (Cate.sol#1524) is too similar to Cate._transferFromExcluded(address,address,uint256).tTransferAmount (Cate.sol#1573)
Variable Cate.reflectionFromToken(uint256,bool).rTransferAmount (Cate.sol#1101) is too similar to Cate._transferStandard(address,address,uint256).tTransferAmount (Cate.sol#1526)
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#variable-names-are-too-similar
INFO:Detectors:
Cate.constructor() (Cate.sol#954-968) uses literals with too many digits:
- _isExcludedFromFee[address(0x000000000000000000000000000000000000dEaD)] = true (Cate.sol#964)
Cate.slitherConstructorVariables() (Cate.sol#895-1586) uses literals with too many digits:
- _tTotal = 100000000 * 10 ** 6 * 10 ** 9 (Cate.sol#911)
Cate.slitherConstructorVariables() (Cate.sol#895-1586) uses literals with too many digits:
- _maxTxAmount = 100000000 * 10 ** 3 * 10 ** 9 (Cate.sol#936)
Cate.slitherConstructorVariables() (Cate.sol#895-1586) uses literals with too many digits:
- numTokensSellToAddToLiquidity = 2500000 * 10 ** 3 * 10 ** 9 (Cate.sol#937)
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#too-many-digits
INFO:Detectors:
Ownable._previousOwner (Cate.sol#463) is never used in Cate (Cate.sol#895-1586)
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#unused-state-variables
INFO:Detectors:
Cate._decimals (Cate.sol#917) should be constant
Cate._name (Cate.sol#915) should be constant
Cate._symbol (Cate.sol#916) should be constant
Cate.numTokensSellToAddToLiquidity (Cate.sol#937) should be constant
Ownable._lockTime (Cate.sol#464) should be constant
Ownable._previousOwner (Cate.sol#463) should be constant
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#state-variables-that-could-be-declared-constant
INFO:Detectors:
renounceOwnership() should be declared external:
- Ownable.renounceOwnership() (Cate.sol#502-505)
transferOwnership(address) should be declared external:
- Ownable.transferOwnership(address) (Cate.sol#511-518)
geUnlockTime() should be declared external:
- Ownable.geUnlockTime() (Cate.sol#520-522)
name() should be declared external:
- Cate.name() (Cate.sol#977-979)
symbol() should be declared external:
- Cate.symbol() (Cate.sol#981-983)
decimals() should be declared external:
- Cate.decimals() (Cate.sol#985-987)
totalSupply() should be declared external:
- Cate.totalSupply() (Cate.sol#989-991)
transfer(address,uint256) should be declared external:
- Cate.transfer(address,uint256) (Cate.sol#998-1005)
allowance(address,address) should be declared external:
- Cate.allowance(address,address) (Cate.sol#1007-1014)
approve(address,uint256) should be declared external:
- Cate.approve(address,uint256) (Cate.sol#1016-1023)
transferFrom(address,address,uint256) should be declared external:
- Cate.transferFrom(address,address,uint256) (Cate.sol#1025-1040)
increaseAllowance(address,uint256) should be declared external:
- Cate.increaseAllowance(address,uint256) (Cate.sol#1042-1053)
decreaseAllowance(address,uint256) should be declared external:
- Cate.decreaseAllowance(address,uint256) (Cate.sol#1055-1069)
isExcludedFromReward(address) should be declared external:
- Cate.isExcludedFromReward(address) (Cate.sol#1071-1073)
totalFees() should be declared external:
- Cate.totalFees() (Cate.sol#1075-1077)

deliver(uint256) should be declared external:
	- Cate.deliver(uint256) (Cate.sol#1079-1089)
reflectionFromToken(uint256,bool) should be declared external:
	- Cate.reflectionFromToken(uint256,bool) (Cate.sol#1091-1104)
excludeFromReward(address) should be declared external:
	- Cate.excludeFromReward(address) (Cate.sol#1119-1126)
excludeFromFee(address) should be declared external:
	- Cate.excludeFromFee(address) (Cate.sol#1164-1166)
includeInFee(address) should be declared external:
	- Cate.includeInFee(address) (Cate.sol#1168-1170)
setSwapAndLiquifyEnabled(bool) should be declared external:
	- Cate.setSwapAndLiquifyEnabled(bool) (Cate.sol#1189-1192)
transferAnyBEP20Tokens(address,address,uint256) should be declared external:
	- Cate.transferAnyBEP20Tokens(address,address,uint256) (Cate.sol#1205-1208)
isExcludedFromFee(address) should be declared external:
	- Cate.isExcludedFromFee(address) (Cate.sol#1369-1371)
Reference:
https://github.com/crytic/slither/wiki/Detector-Documentation#public-function-that-could-be-declared-external
INFO:Slither:Cate.sol analyzed (12 contracts with 75 detectors), 135 result(s) found
INFO:Slither:Use https://crytic.io/ to get access to additional detectors and Github integration

Email: audit@EtherAuthority.io