its__msn itsmsn

ITISH

AUDIT COMPANY

Audit Details

Audited project

CALLISTO TOKEN

Deployer address

0x07e71a6A4eAe5087f0f847cE7EA87D64CA7ecBB2

Client contacts:

CALLISTO TOKEN Team

Blockchain

Binance Smart Chain

Project website:

Not Provided By CALLISTO TOKEN Team

Disclaimer

This is a limited report on our findings based on our analysis, in accordance with good industry practice as at the date of this report, in relation to cybersecurity vulnerabilities and issues in the framework and algorithms based on smart contracts, the details of which are set out in this report. In order to get a full view of our analysis, it is crucial for you to read the full report. While we have done our best in conducting our analysis and producing this report, it is important to note that you should not rely on this report and cannot claim against us on the basis of what it says or doesn't say, or how we produced it, and it is important for you to conduct your own independent investigations before making any decisions. We go into more detail on this in the below disclaimer below – please make sure to read it in full.

DISCLAIMER: By reading this report or any part of it, you agree to the terms of this disclaimer. If you do not agree to the terms, then please immediately cease reading this report, and delete and destroy any and all copies of this report downloaded and/or printed by you. This report is provided for information purposes only and on a non-reliance basis, and does not constitute investment advice. No one shall have any right to rely on the report or its contents, and Itish and its affiliates (including holding companies, shareholders, subsidiaries, employees, directors, officers and other representatives) (Itish) owe no duty of care towards you or any other person, nor does Itish make any warranty or representation to any person on the accuracy or completeness of the report. The report is provided "as is", without any conditions, warranties or other terms of any kind except as set out in this disclaimer, and Itish hereby excludes all representations, warranties, conditions and other terms (including, without limitation, the warranties implied by law of satisfactory quality, fitness for purpose and the use of reasonable care and skill) which, but for this clause, might have effect in relation to the report. Except and only to the extent that it is prohibited by law, Itish hereby excludes all liability and responsibility, and neither you nor any other person shall have any claim against Itish, for any amount or kind of loss or damage that may result to you or any other person (including without limitation, any direct, indirect, special, punitive, consequential or pure economic loss or damages, or any loss of income, profits, goodwill, data, contracts, use of money, or business interruption, and whether in delict, tort (including without limitation negligence), contract, breach of statutory duty, misrepresentation (whether innocent or negligent) or otherwise under any claim of any nature whatsoever in any jurisdiction) in any way arising from or connected with this report and the use, inability to use or the results of use of this report, and any reliance on this report.

The analysis of the security is purely based on the smart contracts alone. No applications or operations were reviewed for security. No product code has been reviewed.

Background

Itish was commissioned by CALLISTO TOKEN to perform an audit of smart contracts:
https://bscscan.com/token/0x07e71a6A4eAe5087f0f847cE7EA87D64CA7ecBB2

The purpose of the audit was to achieve the following:

- Ensure that the smart contract functions as intended.
- Identify potential security issues with the smart contract.

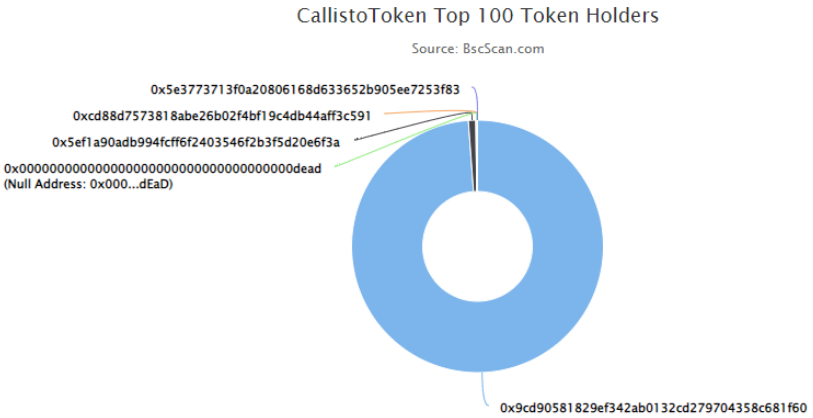
The information in this report should be used to understand the risk exposure of the smart contract, and as a guide to improve the security posture of the smart contract by remediating the issues that were identified.

Contracts Details

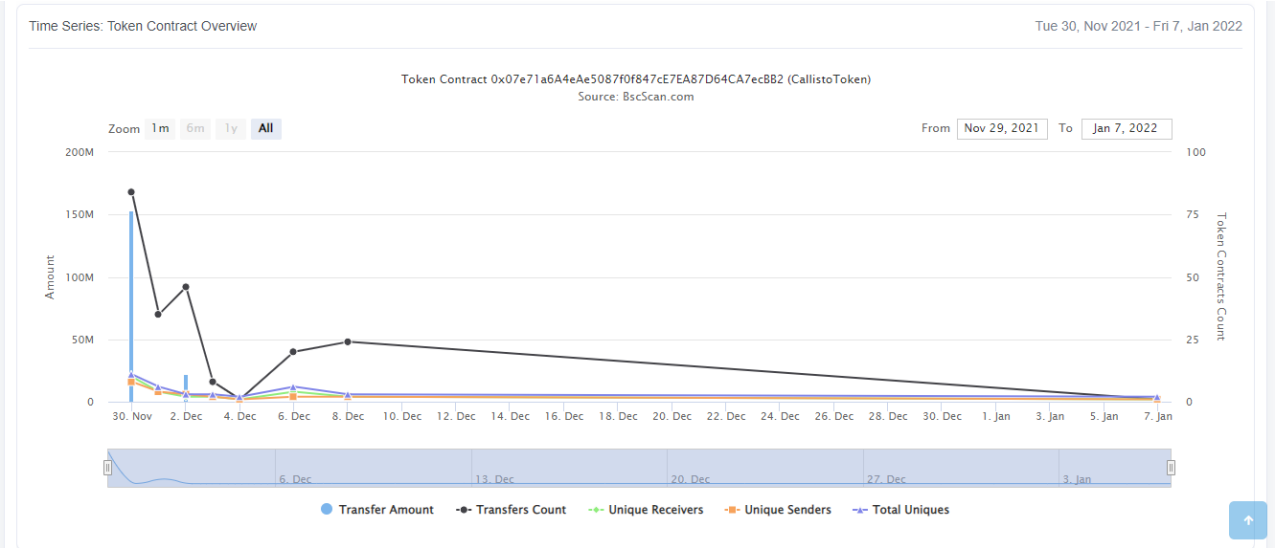
Token contract details for 16.06.2021

Contract name	CALLISTO TOKEN
Contract address	0x07e71a6A4eAe5087f0f847cE7EA87D64CA7ecBB2
Total supply	52,695,972.01
Token ticker	YCT
Decimal CALLISTO	18
Token holders	8
Transactions count	219
Top 100 holders dominance	100.00%
Liquidity fee	0.17
Tax fee	0
Total fees	0.25
Token Creator	0x9cd90581829ef342ab0132cd279704358c681f60

CALLISTO TOKEN Distribution



CALLISTO TOKEN Contract Interaction Details



CALLISTO TOKEN Top 10 Token Holders

Rank	Address	Quantity	Percentage	Analytics
1	0x9cd90581829ef342ab0132cd279704358c681f60	52,091,857.783481071495978501	98.8536%	
2	0x5ef1a90adb994fcff6f2403546f2b3f5d20e6f3a	494,629.33574963455985131	0.9386%	
3	Null Address: 0x000...dEaD	109,482	0.2078%	
4	0xcd88d7573818abe26b02f4bf19c4db44aff3c591	1.663610183639398998	0.0000%	
5	0x5e3773713f0a20806168d633652b905ee7253f83	0.709145023995027412	0.0000%	
6	0x6d96254e563907d0b73a5cbaadeea761a20cd8cb	0.522642655205199938	0.0000%	
7	PancakeSwap V2: YCT 13	0.003809316574913395	0.0000%	
8	PancakeSwap V2: YCT-BUSD 4	0.000398993150320019	0.0000%	

Contract Functions Details

```
+ [Int] IBEP20
  - [Ext] balanceOf
  - [Ext] totalSupply
  - [Ext] decimals
  - [Ext] symbol
  - [Ext] name
  - [Ext] getOwner
  - [Ext] transfer #
  - [Ext] allowance
  - [Ext] approve #
  - [Ext] transferFrom #

+ [Lib] SafeMath
  - [Int] add
  - [Int] sub
  - [Int] sub
  - [Int] mul
  - [Int] div
  - [Int] div
  - [Int] mod
  - [Int] mod

+  Context
  - [Int] _msgSender
  - [Int] _msgData

+ [Lib] Address
  - [Int] isContract
  - [Int] sendValue #
  - [Int] functionCall #
  - [Int] functionCall #
  - [Int] functionCallWithValue #
  - [Int] functionCallWithValue #
  - [Prv] _functionCallWithValue #

+  Ownable (Context)
  - [Int] <Constructor> #
  - [Pub] owner
  - [Pub] renounceOwnership #
    - modifiers: onlyOwner
  - [Pub] transferOwnership #
    - modifiers: onlyOwner
  - [Pub] geUnlockTime
  - [Pub] lock #
    - modifiers: onlyOwner
  - [Pub] unlock #
```

```
+  CALLISTOToken (Context, IBEP20, Ownable)
  - [Pub] <Constructor> #
  - [Pub] name
  - [Pub] symbol
  - [Pub] decimCALLISTO
  - [Pub] totCALLISTOupply
  - [Pub] balanceOf
  - [Pub] transfer #
  - [Pub] allowance
  - [Pub] approve #
  - [Pub] transferFrom #
  - [Pub] increaseAllowance #
  - [Pub] decreaseAllowance #
  - [Pub] isExcludedFromReward
  - [Pub] totalFees
  - [Pub] deliver #
  - [Pub] reflectionFromToken
  - [Pub] tokenFromReflection
  - [Pub] excludeFromReward #
    - modifiers: onlyOwner
  - [Ext] includeInReward #
    - modifiers: onlyOwner
  - [Prv] _transferBothExcluded #
  - [Pub] excludeFromFee #
    - modifiers: onlyOwner
    -
  [Pub] includeInFee #
    - modifiers: onlyOwner
  - [Ext] setTaxFeePercent #
    - modifiers: onlyOwner
  - [Ext] setLiquidityFeePercent #
    - modifiers: onlyOwner
  - [Ext] setMaxTxPercent #
    - modifiers: onlyOwner
  - [Pub] setSwapAndLiquifyEnabled #
    - modifiers: onlyOwner

($) = payable function
(#)   = non-constant function
    -
```

Issues Checking Status

	Issue description	Checking status
1.	Compiler errors.	Passed
2.	Compiler Compatibilities	Failed
3.	Possible delays in data delivery.	Passed
4.	Oracle calls.	Moderate
5.	Front running.	Passed
6.	Timestamp dependence.	Passed
7.	Integer Overflow and Underflow.	Passed
8.	DoS with Revert.	Passed
9.	DoS with block gas limit.	Moderate
10.	Methods execution permissions.	Passed
11.	Economy model of the contract.	Passed
12.	The impact of the exchange rate on the logic.	Severe
13.	Private user data leaks.	Passed
14.	Malicious Event log.	Passed
15.	Scoping and Declarations.	Passed
16.	Uninitialized storage pointers.	Passed
17.	Arithmetic accuracy.	Passed
18.	Design Logic.	Moderate
19.	Cross-function race conditions.	Passed
20.	Safe Open Zeppelin contracts implementation and usage.	Failed
21.	Fallback function security.	Passed

Security Issues

Overview | Detailed Result

0	1	1	1	0
Crit	High	Med	Low	Infor

3.00
Score

SCAN STATISTICS

Status	Completed
Score	3.00
Issue Count	3
Duration	0
Lines of code	1

High Severity Issues

One high severity issues found.

0	1	1	1	0
Crit	High	Med	Low	Infor

- SIGNATURE MALLEABILITY — 1 file
  - contract.sol
- BLOCK VALUES AS A PROXY FOR T... — 1 file
- OUTDATED COMPILER VERSION — 1 file

contract.sol — Create issue

```
1175    function safe32(uint n, string memory errorMessage) internal pure returns
1176        require(n < 2**32, errorMessage);
1177        return uint32(n);
1178    }
1179
1180    function getChainId() internal pure returns (uint) {
1181        uint256 chainId;
1182        assembly { chainId := chainid() }
1183        return chainId;
1184    }
1185 }
```

Vulnerability Description | Remediation

SIGNATURE MALLEABILITY

The function `ecrecover` allows you to convert a valid signature into a different valid signature without requiring knowledge of the private key. It is usually not a problem unless you use signatures to identify items or require them to be uniquely recognizable.

Therefore, depending on the function of the code, this may lead to discrepancies and faulty logic.

REMEDIATION METHOD :

It is recommended to use OpenZeppelin's ECDSA library that has a wrapper around `ecrecover` that mitigates this issue. The data signer can be recovered using `ECDSA.recover`, and its address can be compared to verify the signature.

Medium Severity Issues

One medium severity issues found.

0	1	1	1	0
Crit	High	Med	Low	Infor

- SIGNATURE MALLEABILITY — 1 file
- BLOCK VALUES AS A PROXY FOR T... — 1 file
  - contract.sol
- OUTDATED COMPILER VERSION — 1 file

contract.sol — Create issue

```
1175    function safe32(uint n, string memory errorMessage) internal pure returns
1176        require(n < 2**32, errorMessage);
1177        return uint32(n);
1178    }
1179
1180    function getChainId() internal pure returns (uint) {
1181        uint256 chainId;
1182        assembly { chainId := chainid() }
1183        return chainId;
1184    }
1185 }
```

Vulnerability Description | Remediation

BLOCK VALUES AS A PROXY FOR TIME

Contracts often need access to time values to perform certain types of functionality. Values such as `block.timestamp` and `block.number` can be used to determine the current time or the time delta. However, they are not recommended for most use cases.

For `block.number`, as Ethereum block times are generally around 14 seconds, the delta between blocks can be predicted. The block times, on the other hand, do not remain constant and are subject to change for a number of reasons, e.g., fork reorganizations and the difficulty bomb.

Due to variable block times, `block.number` should not be relied on for precise calculations of time.

REMEDIATION METHOD :

Smart contracts should be written with the idea that block values are not precise, and their use can have unexpected results. Alternatively, oracles can be used.

Low Severity Issues

One Low severity issues found.

0	1	1	1	0
Crit	High	Med	Low	Infor

- SIGNATURE MALLEABILITY — 1 file
- BLOCK VALUES AS A PROXY FOR T... — 1 file
- OUTDATED COMPILER VERSION — 1 file

contract.sol

contract.sol — Create issue

```
1175    function safe32(uint n, string memory errorMessage) internal pure returns
1176        require(n < 2**32, errorMessage);
1177        return uint32(n);
1178    }
1179
1180    function getChainId() internal pure returns (uint) {
1181        uint256 chainId;
1182        assembly { chainId := chainid() }
1183        return chainId;
1184    }
1185 }
```

Vulnerability Description | Remediation

OUTDATED COMPILER VERSION

Using an outdated compiler version can be problematic especially if there are publicly disclosed bugs and issues that affect the current compiler version.

It should also be noted that the Solidity version 0.5.0 introduced some breaking changes.

REMEDIATION METHOD :

It is recommended to use a recent version of the Solidity compiler, preferably something above 0.8.4+ that patches most of the vulnerabilities introduced in older compiler versions.

Conclusion

Smart contracts contain High severity issues! Liquidity pair contract's security is not checked due to out of scope.

Liquidity locking details NOT provided by the team.

Itish note:

Please check the disclaimer above and note, the audit makes no statements or warranties on business model, investment attractiveness or code sustainability. The report is provided for the only contract mentioned in the report and does not include any other potential contracts deployed by Owner.