COINMERCENARY / SMART CONTRACT AUDIT

Qcity Token

13 SEPTEMBER 2018 / TABLE OF CONTENTS

INTRODUCTION

CoinMercenary provides comprehensive, independent smart contract auditing.

We help stakeholders confirm the quality and security of their smart contracts using our comprehensive and standardized audit process. Each audit is unbiased and verified by multiple reputable auditors.

The scope of this audit was to analyze and document the Qcity token contract.

This audit provides practical assurance of the logic and implementation of the contract.

AUDIT METHODOLOGY

CoinMercenary audits consist of four categories of analysis.

Design Patterns

We first inspect the overall structure of the smart contract, including both manual and automated analysis.

The design pattern analysis checks appropriate test coverage, utilizes a linter to ensure consistent style and composition, and code comments are reviewed. Overall architecture and safe usage of third party smart contracts are checked to ensure the contract is structured in a way that will not result in future issues.

Static Analysis

The static analysis portion of our audit is performed using a series of automated tools, purposefully designed to test the security of the contract. These tools include:

- **Manticore** - Dynamic binary analysis tool with EVM support.
- **Mythril** - Reversing and bug hunting framework for the Ethereum blockchain.
- **Oyente** - Analyzes Solidity code to find common vulnerabilities.
- **Solgraph** - DOT graph creation for visualizing function control flow of a Solidity contract to highlight potential security vulnerabilities.

Data flow and control flow are also analyzed to identify vulnerabilities.

Manual Analysis

Performing a hands on review of the smart contract to identify common vulnerabilities is the most intensive portion of our audit. Checks for race conditions, transaction-ordering dependence, timestamp dependence, and denial of service attacks are part of our standardized process.

Network Behavior

In addition to our design pattern check, we also specifically look at network behavior. We model how the smart contract will operate once in production,

then determine the answers to questions such as: how much gas will be used, are there any optimizations, how will the contract interact?

Contracts Reviewed

On September 14, 2018 using git hash 73832adbcf59f9be54e6e1c8c1295c1a9f159507 the following contract files and their respective SHA256 fingerprints were reviewed:

Filename	SHA256 Fingerprint
QcityToken.sol	3b7dd6175e682ed6d0fa0e1dd08acba1f34620554b1301b4849df15776d2ff87
EIP20Interface.sol	8b9884e23709d7d3cf86df0c07ff4cd59533dff51edece184d0cb14de1f0dfd1

Remediation Audit #1

On September 15, 2018 using git hash e7826fc1952863083f8f0ed52790ffbc770c72cb the following contract files and their respective SHA256 fingerprints were reviewed:

Filename	SHA256 Fingerprint
QcityToken.sol	cb0cb66691a8cdfbdb767b4d665dccd97b05dedde0e6c10443f294462e636314
EIP20Interface.sol	8b9884e23709d7d3cf86df0c07ff4cd59533dff51edece184d0cb14de1f0dfd1

Remediation Audit #2

On September 25, 2018 using git hash 1b93a4ed1db286cf91e572064f8f508507c3fb29 the following contract files and their respective SHA256 fingerprints were reviewed:

Filename	SHA256 Fingerprint
QcityToken.sol	87d030d1b618a5333ee5f8cce5cea29b520ef1aba35a9db3a46ea0ba0866559b
EIP20Interface.sol	8b9884e23709d7d3cf86df0c07ff4cd59533dff51edece184d0cb14de1f0dfd1

AUDIT SUMMARY

The contracts have been found to be free of security issues.

Analysis Results

	Initial Audit	Remediation Audit
Design Patterns	Passed	Passed
Static Analysis	Passed	Passed
Manual Analysis	Passed	Passed
Token Allocation	Updates Recommended	Passed
Network Behavior	Passed	Passed

Test Results

- No unit test coverage available.

Token Allocation Results

- Symbol: Dynamically configured for deployment.
- Decimal: Dynamically configured for deployment.
- Total Supply: Dynamically configured for deployment.

Explicit Vulnerability Check Results

Known Vulnerability	Results
Parity Multisig Bug 2	Not vulnerable
Callstack Depth Attack	Not vulnerable
Transaction-Ordering Dependence	Not vulnerable
Timestamp Dependency	Not vulnerable
Re-Entrancy Vulnerability	Not vulnerable
Proxy and Buffer Overflow	Not vulnerable

ISSUES DISCOVERED

Issues below are listed from most critical to least critical. Severity is determined by an assessment of the risk of exploitation or otherwise unsafe behavior.

Severity Levels

- **Informational** - No impact on the contract.
- **Low** - Minimal impact on operational ability.
- **Medium** - Affects the ability of the contract to operate.
- **High** - Affects the ability of the contract to work as designed in a significant way.
- **Critical** - Funds may be allocated incorrectly, lost or otherwise result in a significant loss.

Issues

QC-1 / Informational: Transfer event is not emitted during initial assignment of token balance

Present in QcityToken.sol, line 27

Explanation

Several third party services such as Etherscan use the Transfer event to maintain an external record of transfers. When assigning the initial tokens in the constructor of the token contract, a Transfer event must be emitted to ensure proper tracking of token allocation when viewed using these third party services.

Example:

```
    emit Transfer(address(0), msg.sender, totalSupply);
```

Resolution

Resolved in e7826fc1952863083f8f0ed52790ffbc770c72cb.

QC-2 / Low: Use latest Solidity compiler version

Present in all contract files

Explanation

Update all contract files to use the latest version of Solidity compiler in order to ensure the latest performance enhancements, features and bug fixes are available.

Resolution

Resolved in e7826fc1952863083f8f0ed52790ffbc770c72cb.

QC-3 / Informational: Use SafeMath for subtraction and addition

Present in all contract files

Explanation

Update all contract files to use SafeMath in order to ensure security functionality is in place for integer over-and-under flows.

Resolution

Resolved in 20a8c897033eb57d3d9cc6f71714f8b70ed919c9.

CONCLUSION

The reviewed smart contracts are free of security issues and well crafted.

We look forward to seeing the success of Qcity and appreciate the opportunity to be a part of their story.