IQ Token Security Analysis

by Pessimistic

This report is public

June 16, 2023

Abstract

In this report, we consider the security of smart contracts of IQ Token project. Our task is to find and describe security issues in the smart contracts of the platform.

Disclaimer

The audit does not give any warranties on the security of the code. A single audit cannot be considered enough. We always recommend proceeding with several independent audits and a public bug bounty program to ensure the security of smart contracts. Besides, a security audit is not investment advice.

Summary

In this report, we considered the security of IQ Token smart contracts. We performed our audit according to the procedure described below.

The initial audit did not reveal any issues.

Later, the developers updated the codebase. The recheck also did not show any issues.

General recommendations

We have no recommendations for the project.

Project overview

Project description

For the audit, we were provided with IQ Token project on a private GitHub repository, commit 2ba44d524ee6c085adacecd811e09080e84d8fb1.

The project has README.md file with a short description of the project.

The project compiles successfully and has a test.

The total LOC of audited sources is three lines.

Token details

Name:	IQ Protocol Token
Symbol:	IQT
Decimals:	18
Total Supply:	1 000 000 000

Codebase update

After some time, the developers updated the codebase. For the recheck, we were provided with commit 1ff445748c59009da64f760d69e436dd9ea7399f.

In this commit, the developers updated the solidity version, project dependencies and inheritance, and the hardhat configuration. These changes do not affect the code operation logic. The recheck did not reveal any issues.

The project contains a single test that passes successfully.

Procedure

In our audit, we consider the following crucial features of the code:

1. Whether the code is secure.
2. Whether the code corresponds to the documentation (including whitepaper).
3. Whether the code meets best practices.

We perform our audit according to the following procedure:

- Automated analysis
    - We scan project's code base with automated tool Slither.
    - We manually verify (reject or confirm) all the issues found by tools.
- Manual audit
    - We manually analyze code base for security vulnerabilities.
    - We assess overall project structure and quality.
- Report
    - We reflect all the gathered information in the report.

Manual analysis

The contracts were completely manually analyzed, their logic was checked. Besides, the results of the automated analysis were manually verified. All the confirmed issues are described below.

Critical issues

Critical issues seriously endanger project security. They can lead to loss of funds or other catastrophic consequences. The contracts should not be deployed before these issues are fixed.

The audit showed no critical issues.

Medium severity issues

Medium issues can influence project operation in the current implementation. Bugs, loss of potential income, and other non-critical failures fall into this category, as well as potential problems related to incorrect system management. We highly recommend addressing them.

The audit showed no issues of medium severity.

Low severity issues

Low severity issues do not directly affect project operation. However, they might lead to various problems in future versions of the code. We recommend fixing them or explaining why the team has chosen a particular option.

The audit showed no issues of low severity.

This analysis was performed by Pessimistic:

Pavel Kondratenkov, Senior Security Engineer
Yhtyyar Sahatov, Security Engineer
Irina Vikhareva, Project Manager
Alexander Seleznev, Founder

June 16, 2023