SALUS SECURITY

Mar 2024

CODE SECURITY ASSESSMENT

INK FINANCE

Overview

Project Summary

- Name: Ink Finance - QuillToken
- Platform: Avalanche
- Language: Solidity
- Address: 0xf3E5914cA1F678E0A3a38031B5514682e3450919
- Audit Range: See Appendix - 1

Project Dashboard

Application Summary

Name	Ink Finance - QuillToken
Version	v1
Type	Solidity
Dates	Mar 26 2024
Logs	Mar 26 2024

Vulnerability Summary

Total High-Severity issues	0
Total Medium-Severity issues	0
Total Low-Severity issues	1
Total informational issues	1
Total	2

Contact

E-mail: support@salusec.io

Risk Level Description

High Risk	The issue puts a large number of users' sensitive information at risk, or is reasonably likely to lead to catastrophic impact for clients' reputations or serious financial implications for clients and users.
Medium Risk	The issue puts a subset of users' sensitive information at risk, would be detrimental to the client's reputation if exploited, or is reasonably likely to lead to a moderate financial impact.
Low Risk	The risk is relatively small and could not be exploited on a recurring basis, or is a risk that the client has indicated is low impact in view of the client's business circumstances.
Informational	The issue does not pose an immediate risk, but is relevant to security best practices or defense in depth.

Content

Introduction

1.1 About SALUS

At Salus Security, we are in the business of trust.

We are dedicated to tackling the toughest security challenges facing the industry today. By building foundational trust in technology and infrastructure through security, we help clients to lead their respective industries and unlock their full Web3 potential.

Our team of security experts employ industry-leading proof-of-concept (PoC) methodology for demonstrating smart contract vulnerabilities, coupled with advanced red teaming capabilities and a stereoscopic vulnerability detection service, to deliver comprehensive security assessments that allow clients to stay ahead of the curve.

In addition to smart contract audits and red teaming, our Rapid Detection Service for smart contracts aims to make security accessible to all. This high calibre, yet cost-efficient, security tool has been designed to support a wide range of business needs including investment due diligence, security and code quality assessments, and code optimisation.

We are reachable on Telegram (https://t.me/salusec), Twitter (https://twitter.com/salus_sec), or Email (support@salusec.io).

1.2 Audit Breakdown

The objective was to evaluate the repository for security-related issues, code quality, and adherence to specifications and best practices. Possible issues we looked for included (but are not limited to):

- Risky external calls
- Integer overflow/underflow
- Transaction-ordering dependence
- Timestamp dependence
- Access control
- Call stack limits and mishandled exceptions
- Number rounding errors
- Centralization of power
- Logical oversights and denial of service
- Business logic specification
- Code clones, functionality duplication

1.3 Disclaimer

Note that this security audit is not designed to replace functional tests required before any software release and does not give any warranties on finding all possible security issues with the given smart contract(s) or blockchain software, i.e., the evaluation result does not guarantee the nonexistence of any further findings of security issues.

1.4 About QuillToken

- Address: 0xf3E5914cA1F678E0A3a38031B5514682e3450919
- Name: InkFinance
- Symbol: QUILL
- Decimals: 18
- Total Supply: 100 million
- Blockchain: Avalanche
- Who can burn the token: Users who own tokens can burn their tokens at any time.

Findings

2.1 Summary of Findings

ID	Title	Severity	Category	Status
1	Centralization risk with initial token distribution	Low	Centralization	Pending
2	Use of floating pragma	Informational	Configuration	Pending

2.2 Notable Findings

Significant flaws that impact system confidentiality, integrity, or availability are listed below.

1. Centralization risk with initial token distribution	
Severity: Low	Category: Centralization
Target: - QuillToken.sol	

Description

When the contract is deployed, 100% of $QUILL is sent to an EOA account. This address then has full control over the token distribution, so any compromise of its private key could have a drastic effect on the project. For example, attackers could dump the price of $QUILL on the DEX if they gain access to the private key.

Recommendation

It is recommended to transfer tokens to a multi-sig account and promote transparency by providing a breakdown of the intended initial token distribution in a public location.

2.3 Informational Findings

2. Use of floating pragma	
Severity: Informational	Category: Configuration
Target: - QuillToken.sol	

Description

```
pragma solidity >=0.7.0 <0.9.0;
```

The QuillToken uses a floating compiler version >=0.7.0 <0.9.0.

Using a floating pragma >=0.7.0 <0.9.0 statement is discouraged, as code may compile to different bytecodes with different compiler versions. Use a locked pragma statement to get a deterministic bytecode. Also use the latest Solidity version to get all the compiler features, bug fixes and optimizations.

Recommendation

It is recommended to use a locked Solidity version throughout the project. It is also recommended to use the most stable and up-to-date version.

Appendix

Appendix 1 - Files in Scope

This audit covered the following file from address 0xf3E5914cA1F678E0A3a38031B5514682e3450919:

File	SHA-1 hash
QuillToken.sol	11e479b6c2b3066d1602cc38ad8cd52ff32e7080