verichains

SECURITY AUDIT OF

RENEC

Public Report

Dec 07, 2022

Verichains Lab

info@verichains.io

https://www.verichains.io

Driving Technology > Forward

EXECUTIVE SUMMARY

This Security Audit Report prepared by Verichains Lab on Dec 07, 2022. We would like to thank Remitano for trusting Verichains Lab, delivering high-quality audits is always our top priority.

This audit focused on identifying security flaws in code and the design of the inflation module of the Renec Network. The scope of the audit is limited to the source code files provided to Verichains. Verichains Lab completed the assessment using manual, static, and dynamic analysis techniques.

During the audit process, the audit team had identified no vulnerable issue in the project source code.

TABLE OF CONTENTS

1. MANAGEMENT SUMMARY

1.1. About Renec Network

Renec Network is designed with extendable awareness from beginning. The network is designed so that it is possible to add new capabilities and leverage the latest exciting technology in the blockchain space to the network without the need to introduce a new token.

Renec Network is not a single blockchain, rather it is a set of blockchains designed to be interchangeable from the beginning. The initial network will be a simple value transfer one, similar to bitcoin, litecoin but with faster block time and more efficient consensus protocol. Then they will add a token decentralized exchange to the network, and then the decentralized fiat-token escrow, and last, a full ledge smart contract platform. As the Renec team discover new technologies in the blockchain space, they will add it to the Renec Network, so with the RENEC token, investor should have the ability to transact quickly, exchange cheaply, escrow reliably, and performing sophisticated smart contracts.

Scalability

Each blockchain will have a specific scalability capacity. With the initial blockchain, we don't expect it to be huge. But since the network is designed to be extensible from the beginning, they will be adding multiple new blockchain technologies to the network, allowing it to achieve the level of scalability second to none.

Cross-chain communication

In order for RENEC token to be utilized on different technologies, every blockchain in the Renec Network will need to implement cross-chain communication capability, allowing a specific amount of token to be locked on a blockchain and simultaneously unlocked on the other blockchain.

1.2. Audit scope

In this particular project, a timebox approach was used to define the consulting effort. This means that **Verichains Lab** allotted a prearranged amount of time to identify and document vulnerabilities. Because of this, there is no guarantee that the project has discovered all possible vulnerabilities and risks.

Furthermore, the security check is only an immediate evaluation of the situation at the time the check was performed. An evaluation of future security levels or possible future risks or vulnerabilities may not be derived from it.

This audit focused on identifying security flaws in code and the design of the Renec Network.

It was conducted on commit `dd356cd95ff664464d5f8410b08cad22352c4d8a` from Git repository *https://github.com/remitano/renec*.

1.3. Audit methodology

Our security audit process includes four steps:

- Mechanism Design is reviewed to look for any potential problems.
- Source codes are scanned/tested for commonly known and more specific vulnerabilities using public and our in-house security analysis tool.
- Manual audit of the codes for security issues. The source code is manually analyzed to look for any potential problems.
- Set up a testing environment to debug/analyze found issues and verifies our attack PoCs.

For vulnerabilities, we categorize the findings into categories as listed in table below, depending on their severity level:

SEVERITY LEVEL	DESCRIPTION
CRITICAL	A vulnerability that can disrupt the functioning; creates a critical risk to the application; required to be fixed immediately.
HIGH	A vulnerability that could affect the desired outcome of executing the application with high impact; needs to be fixed with high priority.
MEDIUM	A vulnerability that could affect the desired outcome of executing the application with medium impact in a specific scenario; needs to be fixed.
LOW	An issue that does not have a significant impact, can be considered as less important.

Table 1. Severity levels

1.4. Disclaimer

Please note that security auditing cannot uncover all existing vulnerabilities, and even an audit in which no vulnerabilities are found is not a guarantee for a 100% secure application. However, auditing allows discovering vulnerabilities that were unobserved, overlooked during development and areas where additional security measures are necessary.

2. AUDIT RESULT

2.1. Overview

Renec network is built based on the Solana blockchain which is an open source project implementing a new, high-performance, permissionless blockchain. This project is a fork from the original repository of Solana *https://github.com/solana-labs/solana* based on the commit `0c54340a4a4b71583595da6307213055efab80da` with some minor modifications. These changes can be summarized below:

- Update some parameters of the unlock schedule for genesis accounts.
- Update some parameters of the inflation schedule as below (based on Solana's inflation schedule):
  - Initial inflation rate: 4.5%
  - Dis-inflation rate: 0%
  - Long-term inflation rate: 4.5%

These changes do not make any serious impact on the security design of the Renec network, which is directly based on Solana. However, the audit team will not take any responsibility for the economic affects after changing parameters related to the unlock schedule as well as the inflationary model.

2.2. Findings

During the audit process, the audit team found no vulnerability in the given version of Renec Network.

3. VERSION HISTORY

Version	Date	Status/Change	Created by
1.0	*Dec 07, 2022*	Public Report	Verichains Lab

Table 2. Report versions history