verichains

SECURITY AUDIT OF

SENSEIFI STAKING POOL SMART CONTRACT

SenSei Fi

Public Report

May 31, 2023

Verichains Lab

info@verichains.io

https://www.verichains.io

Driving Technology > Forward

ABBREVIATIONS

Name	Description
Sei	A decentralized blockchain built to enable scalable, user-friendly apps for the world.
DAO	A digital Decentralized Autonomous Organization and a form of investor-directed venture capital fund.

EXECUTIVE SUMMARY

This Security Audit Report was prepared by Verichains Lab on May 31, 2023. We would like to thank the SenseiFi for trusting Verichains Lab in auditing smart contracts. Delivering high-quality audits is always our top priority.

This audit focused on identifying security flaws in code and the design of the SenseiFi Staking Pool Smart Contract. 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 smart contracts code.

TABLE OF CONTENTS

1. MANAGEMENT SUMMARY

1.1. About SenseiFi

SenseiFi Leading gamified Defi on Sei network with the spiciest rewards.

1.2. Audit scope

This audit focused on identifying security flaws in code and the design of the SenseiFi Staking Smart Contract. It was conducted on commit `c6271f461d8d1ffc00a6e2738768d81ecfceb0cb` from git repository link: *httpshttps://github.com/senseifi/staking-rewards-nll/tree/main/smart_contracts/contracts/senseifi_staking_pool*.

1.3. Audit methodology

Our security audit process for Sei smart contract includes two steps:

- Smart contract codes are scanned/tested for commonly known and more specific vulnerabilities using our in-house smart contract security analysis tool.
- Manual audit of the codes for security issues. The contracts are manually analyzed to look for any potential problems.

Following is the list of commonly known vulnerabilities that were considered during the audit of the Sei smart contract:

- Arithmetic Overflow and Underflow
- Ownership checks
- Numerical precision errors
- Logic Flaws

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 contract functioning; creates a critical risk to the contract; required to be fixed immediately.
HIGH	A vulnerability that could affect the desired outcome of executing the contract with high impact; needs to be fixed with high priority.

SEVERITY LEVEL	DESCRIPTION
MEDIUM	A vulnerability that could affect the desired outcome of executing the contract 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 smart contract. 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

The SenseiFi Staking Smart Pool Contract was written in `Rust` programming language.

The staking pool contract is a smart contract that incentivizes users to hold and lock up their tokens for a certain period of time. In return, they receive rewards in the form of both primary and secondary tokens, which are distributed based on the reward rate that is set by the admin user.

To set the reward rate, the admin user can use the set_reward_rate function, which will allow them to specify how much of each token will be distributed as rewards. Additionally, anyone can add rewards to the contract through the supply_rewards function.

2.2. Findings

During the audit process, the audit team found no issue in the given version of SenseiFi Staking Pool Smart Contract.

3. VERSION HISTORY

Version	Date	Status/Change	Created by
1.0	*May 31, 2023*	Public Report	Verichains Lab

Table 2. Report versions history