SECURITY AUDIT OF

POOL REGISTER SMART CONTRACT

Public Report

Nov 21, 2023

Verichains Lab

info@verichains.io

https://www.verichains.io

Driving Technology > Forward

ABBREVIATIONS

Name	Description
Ethereum	An open source platform based on blockchain technology to create and distribute smart contracts and decentralized applications.
Ether (ETH)	A cryptocurrency whose blockchain is generated by the Ethereum platform. Ether is used for payment of transactions and computing services in the Ethereum network.
Smart contract	A computer protocol intended to digitally facilitate, verify or enforce the negotiation or performance of a contract.
Solidity	A contract-oriented, high-level language for implementing smart contracts for the Ethereum platform.
Solc	A compiler for Solidity.
ERC20	ERC20 (BEP20 in Binance Smart Chain or *x*RP20 in other chains) tokens are blockchain-based assets that have value and can be sent and received. The primary difference with the primary coin is that instead of running on their own blockchain, ERC20 tokens are issued on a network that supports smart contracts such as Ethereum or Binance Smart Chain.
BSC	Binance Smart Chain or BSC is an innovative solution for introducing interoperability and programmability on Binance Chain.

EXECUTIVE SUMMARY

This Security Audit Report was prepared by Verichains Lab on Nov 21, 2023. We would like to thank the Segment Finance 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 Pool Register 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 project source code.

TABLE OF CONTENTS

1. MANAGEMENT SUMMARY

1.1. About Pool Register Smart Contract

Segment Finance is a decentralized lending and borrowing plattform built on BNB Chains. The protocol operates in a peer-to-peer manner, eliminating the need for intermediaries such as banks or traditional financial institutions.

Segment Finance aims to be the prime lending platform on BNB Chains by offering highest competitive incentives for money markets and having the deepest liquidity.

At its launch, Segment Finance will support a selection of high-liquidity money markets, featuring incentives that dynamically adapt in response to market conditions:

- BNB
- BTCB
- ETH
- USDT
- USDC
- CAKE

The Pool Register Contract is a vital component of the Segment Finance system.

1.2. Audit scope

This audit focused on identifying security flaws in code and the design of the Pool Register Smart Contract.

It was conducted on commit `9e446feefe09f456083d5a9996254a1009336353` from git repository *https://github.com/Segment-Finance/protocol*.

Our audit scope encompasses only two files: `PoolRegistry.sol` and `PoolRegistryInterface.sol` located in the `packages/isolated/contracts/Pool/` path.

1.3. Audit methodology

Our security audit process for smart contract includes two steps:

- Smart contract codes are scanned/tested for commonly known and more specific vulnerabilities using public and RK87, 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 smart contract:

- Integer Overflow and Underflow
- Timestamp Dependence
- Race Conditions
- Transaction-Ordering Dependence
- DoS with (Unexpected) revert
- DoS with Block Gas Limit
- Gas Usage, Gas Limit and Loops
- Redundant fallback function
- Unsafe type Inference
- Reentrancy
- Explicit visibility of functions state variables (external, internal, private and public)
- 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.
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

Segment Finance acknowledges that the security services provided by Verichains, are conducted to the best of their professional abilities but cannot guarantee 100% coverage of all security vulnerabilities. Segment Finance understands and accepts that despite rigorous auditing, certain vulnerabilities may remain undetected. Therefore, Segment Finance agrees that Verichains shall not be held responsible or liable, and shall not be charged for any hacking incidents that occur due to security vulnerabilities not identified during the audit process.

1.5. Acceptance Minute

This final report served by Verichains to the Segment Finance will be considered an Acceptance Minute. Within 7 days, if no any further responses or reports is received from the Segment Finance, the final report will be considered fully accepted by the Segment Finance without the signature.

2. AUDIT RESULT

2.1. Overview

Pool Register contract is built based on isolated-pool of Venus Protocol which is an open source project. This project is a fork from the original repository of Venus Protocol *https://github.com/VenusProtocol/isolated-pools/* based on the commit `6dd144e080806290b22ca2e7c8d32a23c4188998` with some minor modifications. These changes can be summarized below:

- Transition from `Upgradeable` libraries to Standard libraries.
- Renaming all variables prefixed with `vToken` to `seToken` and `Venus` to `Segment`.

These changes do not make any serious impact on the security design of the Pool Register, which is directly based on Pool Register of Venus Protocol. Nonetheless, it's important to note that the audit team disclaims any responsibility for any errors related to `seToken` and `comptroller` as it falls outside the scope of the audit.

2.2. Findings

During the audit process, the audit team found no vulnerability in the given version of Pool Register Smart Contract.

3. VERSION HISTORY

Version	Date	Status/Change	Created by
1.0	*Nov 21, 2023*	Public Report	Verichains Lab

Table 2. Report versions history