SECURITY AUDIT OF

HOLDSTATION DEX ON ZKSYNC

Public Report

Jun 25, 2024

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.

EXECUTIVE SUMMARY

This Security Audit Report was prepared by Verichains Lab on Jun 25, 2024. We would like to thank the Holdstation 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 Holdstation DEX on ZKsync. 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 Holdstation DEX on ZKsync

Holdstation DEX on ZKsync is a cutting-edge decentralized exchange (DEX) based on the ZKsync blockchain, a fork of the Uniswap V3 protocol. It provides exceptional efficiency and flexibility, allowing users to focus liquidity in specific price ranges for maximized returns. With the power of ZKsync's zk-rollup technology, users benefit from high-speed, low-cost transactions.

1.2. Audit scope

This audit focused on identifying security flaws in the Holdstation DEX on ZKsync's difference code, which was cloned from the `UniswapV3` protocol. It was conducted contracts on Zksync deployed at the following addresses:

Contract	Address	Block Deploy	Verified
HoldstationRouter	0xD1f1bA4BF2aDe4F47472D0B73ba0f5DC30E225DF	31123301	Yes
NonfungiblePositionManager	0x7FE3975fb0f9A7F78b015806fB8a1E569b014C10	31199859	Yes
V3CoreFactory	0x1153D1d27A558471eF051c5D2D075d7D07B84A07	31199635	No

Table 1. Contract audited list

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 2. Severity levels

1.4. Disclaimer

Holdstation 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. Holdstation understands and accepts that despite rigorous auditing, certain vulnerabilities may remain undetected. Therefore, Holdstation 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 Holdstation will be considered an Acceptance Minute. Within 7 days, if no any further responses or reports is received from the Holdstation, the final report will be considered fully accepted by the Holdstation without the signature.

2. AUDIT RESULT

2.1. Overview

Holdstation DEX on ZKsync is a decentralized exchange (DEX) that runs on the ZKsync blockchain. It is a direct and unaltered clone of the Uniswap V3 protocol, preserving all of its innovative features and functionalities.

Key Features:

- **Concentrated Liquidity**: Liquidity providers (LPs) can allocate capital within specific price ranges, maximizing capital efficiency and returns.
- **Multiple Fee Tiers**: Offers different fee structures tailored to the volatility of trading pairs, ensuring appropriate compensation for LPs.
- **Non-Fungible Liquidity Positions**: Each liquidity position is represented as an NFT, allowing for unique and flexible liquidity management.
- **Advanced Oracle Functionality**: Incorporates robust price oracles for accurate and reliable price data essential for DeFi applications.
- **Gas Optimization**: Enhanced performance with optimized gas costs for various operations.

Holdstation DEX on ZKsync is a folk of Uniswap V3 protocol, with no modifications to the original codebase. This guarantees that users and liquidity providers will experience the same high standards of security, efficiency, and functionality that Uniswap V3 is renowned for, but on the scalable and cost-effective ZKsync blockchain.

2.2. Findings

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

3. VERSION HISTORY

Version	Date	Status/Change	Created by
1.0	*Jun 25, 2024*	Public Report	Verichains Lab

Table 3. Report versions history