QuillAudits

AUDIT REPORT

January, 2025

For

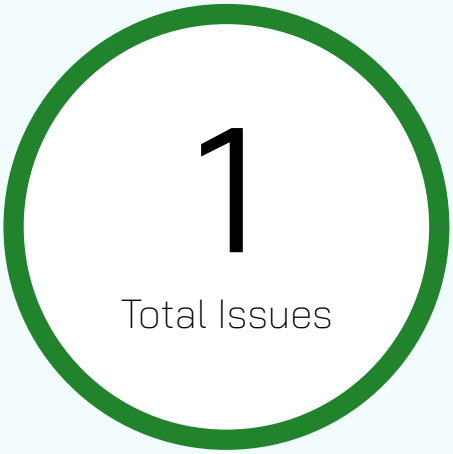
SONEX

Table of Content

Executive Summary

Project name	Sonex
Overview	SONEX is a decentralized exchange (DEX) designed to leverage the power of Soneium, offering users a fast, secure, and efficient way to trade digital assets. Built with cutting-edge blockchain technology, SoneX aims to deliver a seamless trading experience with a strong focus on innovation, collaboration, and user empowerment.
Audit Scope	The scope of this audit was to analyse theSonic Codebase for quality, security, and correctness.
Method	Manual Review, Functional Testing, Automated Testing, etc. All the raised flags were manually reviewed and re-tested to identify any false positives.
Blockchain	EVM
Source Code	https://github.com/sonex-dex/sonex-deploy-v3/tree/master
Review 1	16th January 2025 - 17th January 2025
Updated Code Received	NA
Review 2	NA
Fixed In	NA

Number of Issues per Severity



High	0 (0.00%)
Medium	0 (0.00%)
Low	1 (100.00%)
Informational	0 (0.00%)

Severity

Issues	High	Medium	Low	Informational
Open	0	0	0	0
Resolved	0	0	**1**	0
Acknowledged	0	0	0	0
Partially Resolved	0	0	0	0

Checked Vulnerabilities

- ☑ Re-entrancy
- ☑ Timestamp Dependence
- ☑ Gas Limit and Loops
- ☑ DoS with Block Gas Limit
- ☑ Transaction-Ordering Dependence
- ☑ Use of tx.origin
- ☑ Gasless Send
- ☑ Exception Disorder
- ☑ Byte Array
- ☑ Compiler Version Not Fixed
- ☑ Redundant Fallback Function
- ☑ Style Guide Violation
- ☑ Unchecked External Call
- ☑ Unchecked Math
- ☑ Access Management
- ☑ Implicit Visibility Level
- ☑ Centralization of Control
- ☑ Improper or Missing Events
- ☑ Logical Issues and Flaws
- ☑ Arithmetic Computations Correctness

Techniques and Methods

Throughout the audit of smart contracts, care was taken to ensure:

- The overall quality of code.
- Use of best practices.
- Code documentation and comments, match logic and expected behavior.
- Token distribution and calculations are as per the intended behavior mentioned in the whitepaper.
- Implementation of ERC standards.
- Efficient use of gas.
- Code is safe from re-entrancy and other vulnerabilities.

The following techniques, methods, and tools were used to review all the smart contracts.

Structural Analysis

In this step, we have analyzed the design patterns and structure of smart contracts. A thorough check was done to ensure the smart contract is structured in a way that will not result in future problems.

Static Analysis

A static Analysis of Smart Contracts was done to identify contract vulnerabilities. In this step, a series of automated tools are used to test the security of smart contracts.

Code Review / Manual Analysis

Manual Analysis or review of code was done to identify new vulnerabilities or verify the vulnerabilities found during the static analysis. Contracts were completely manually analyzed, their logic was checked and compared with the one described in the whitepaper. Besides, the results of the automated analysis were manually verified.

Gas Consumption

In this step, we have checked the behavior of smart contracts in production. Checks were done to know how much gas gets consumed and the possibilities of optimization of code to reduce gas consumption.

Tools And Platforms Used For Audit

Remix IDE, Foundry, Solhint, Mythril, Slither, Solidity statistical analysis.

Types of Severity

Every issue in this report has been assigned to a severity level. There are four levels of severity, and each of them has been explained below

High Severity Issues

A high severity issue or vulnerability means that your smart contract can be exploited. Issues on this level are critical to the smart contract's performance or functionality, and we recommend these issues be fixed before moving to a live environment.

Medium Severity Issues

The issues marked as medium severity usually arise because of errors and deficiencies in the smart contract code. Issues on this level could potentially bring problems, and they should still be fixed.

Low Severity Issues

Low-level severity issues can cause minor impact and are just warnings that can remain unfixed for now. It would be better to fix these issues at some point in the future.

Informational Issues

These are four severity issues that indicate an improvement request, a general question, a cosmetic or documentation error, or a request for information. There is low-to-no impact.

Types of Issues

Open

Security vulnerabilities identified that must be resolved and are currently unresolved.

Resolved

Security vulnerabilities identified that must be resolved and are currently unresolved.

Acknowledged

Vulnerabilities which have been acknowledged but are yet to be resolved.

Partially Resolved

Considerable efforts have been invested to reduce the risk/ impact of the security issue, but are not completely resolved.

Low Severity Issues

Remove Unused Contracts

Resolved

Path

https://github.com/sonex-dex/sonex-deploy-v3/tree/9db9cbf9656a4778c36e37092144df9dc422359e/contracts/swap-router-contracts

Description

In the Sonex V3 Repository, Swap Router Contracts are present which are not used in the protocol.

Recommendation

We Recommed to remove the unused code.

Automated Tests

No issues were found.

Closing Summary

In this report, we have considered the security of the Sonex Smart contracts. Sonex is fork of Uniswap V3 with no changes. Code is good and well tested. We performed our audit according to the procedure described above. No Issues found in the codebase except one low severity issues,which the sonex team has resolved.

Disclaimer

QuillAudits Smart contract security audit provides services to help identify and mitigate potential security risks in sonex smart contracts. However, it is important to understand that no security audit can guarantee complete protection against all possible security threats. QuillAudits audit reports are based on the information provided to us at the time of the audit, and we cannot guarantee the accuracy or completeness of this information. Additionally, the security landscape is constantly evolving, and new security threats may emerge after the audit has been completed.

Therefore, it is recommended that multiple audits and bug bounty programs be conducted to ensure the ongoing security of sonex smart contracts. One audit is not enough to guarantee complete protection against all possible security threats. It is important to implement proper risk management strategies and stay vigilant in monitoring your smart contracts for potential security risks.

QuillAudits cannot be held liable for any security breaches or losses that may occur subsequent to and despite using our audit services. It is the responsibility of the sonex to implement the recommendations provided in our audit reports and to take appropriate steps to mitigate potential security risks.

About QuillAudits

QuillAudits is a leading name in Web3 security, offering top-notch solutions to safeguard projects across DeFi, GameFi, NFT gaming, and all blockchain layers. With six years of expertise, we've secured over 1000 projects globally, averting over $30 billion in losses. Our specialists rigorously audit smart contracts and ensure DApp safety on major platforms like Ethereum, BSC, Arbitrum, Algorand, Tron, Polygon, Polkadot, Fantom, NEAR, Solana, and others, guaranteeing your project's security with cutting-edge practices.

6+ Years of Expertise	**1M+** Lines of Code Audited
$30B+ Secured in Digital Assets	**1K+** Projects Secured

Follow Our Journey

AUDIT REPORT

January, 2025

For

SONEX

QuillAudits

Canada, India, Singapore, UAE, UK

www.quillaudits.com audits@quillaudits.com