CODE SECURITY ASSESSMENT

SWAPX

Overview

Project Summary

- Name: SwapX - contract v3
- Platform: EVM-compatible chains
- Language: Solidity
- Repository:
    - https://github.com/hi-swapx/contract-v3
- Audit Range: See Appendix - 1

Project Dashboard

Application Summary

Name	SwapX- contract v3
Version	v1
Type	Solidity
Dates	Apr 07 2025
Logs	Apr 07 2025

Contact

E-mail: support@salusec.io

Risk Level Description

High Risk	The issue puts a large number of users' sensitive information at risk, or is reasonably likely to lead to catastrophic impact for clients' reputations or serious financial implications for clients and users.
Medium Risk	The issue puts a subset of users' sensitive information at risk, would be detrimental to the client's reputation if exploited, or is reasonably likely to lead to a moderate financial impact.
Low Risk	The risk is relatively small and could not be exploited on a recurring basis, or is a risk that the client has indicated is low impact in view of the client's business circumstances.
Informational	The issue does not pose an immediate risk, but is relevant to security best practices or defense in depth.

SALUS

Content

SALUS

Introduction

1.1 About SALUS

At Salus Security, we are in the business of trust.

We are dedicated to tackling the toughest security challenges facing the industry today. By building foundational trust in technology and infrastructure through security, we help clients to lead their respective industries and unlock their full Web3 potential.

Our team of security experts employ industry-leading proof-of-concept (PoC) methodology for demonstrating smart contract vulnerabilities, coupled with advanced red teaming capabilities and a stereoscopic vulnerability detection service, to deliver comprehensive security assessments that allow clients to stay ahead of the curve.

In addition to smart contract audits and red teaming, our Rapid Detection Service for smart contracts aims to make security accessible to all. This high calibre, yet cost-efficient, security tool has been designed to support a wide range of business needs including investment due diligence, security and code quality assessments, and code optimisation.

We are reachable on Telegram (https://t.me/salusec), Twitter (https://twitter.com/salus_sec), or Email (support@salusec.io).

1.2 Audit Breakdown

The objective was to evaluate the repository for security-related issues, code quality, and adherence to specifications and best practices. Possible issues we looked for included (but are not limited to):
- Risky external calls
- Integer overflow/underflow
- Transaction-ordering dependence
- Timestamp dependence
- Access control
- Call stack limits and mishandled exceptions
- Number rounding errors
- Centralization of power
- Logical oversights and denial of service
- Business logic specification
- Code clones, functionality duplication

1.3 Disclaimer

This attestation is provided solely to confirm that the subject codebase is an unmodified fork of the referenced source repository at the time of review. It does not constitute a security audit and does not make any guarantees regarding the security, functionality, or suitability of the code. No warranty is given that the code is free from vulnerabilities, bugs, or other potential issues.

SALUS

Release Notes

Based on our review, the development of xone contract-v2 is entirely based on Uniswap V2, with no modifications made to the core logic. As a result, the security of the code also relies on that of Uniswap V2. We encourage the team to regularly monitor the status of third-party dependencies to mitigate potential impacts in case they fail or become unreliable.

Module Path	Description (optional)	Original Source Link
contracts/v3-core	Core logic of the swap	Uniswap V3 Core v1.0.0
contracts/v3-periphery	Peripheral/helper contracts	Uniswap V3 Periphery v1.0.1

SALUS

Appendix

Appendix 1 - Files in Scope

This audit covered the files in commit 14a2798.