BLOCKAPEX

SMART CONTRACT SECURITY

V 1.0

DATE: 19th APR, 2024

PREPARED FOR: ELECTROSWAP DEX

About BlockApex

Founded in early 2021, is a security-first blockchain consulting firm. We offer services in a wide range of areas including Audits for Smart Contracts, Blockchain Protocols, Tokenomics along with Invariant development (i.e., test-suite) and Decentralized Application Penetration Testing. With a dedicated team of over 40+ experts dispersed globally, BlockApex has contributed to enhancing the security of essential software components utilized by many users worldwide, including vital systems and technologies.

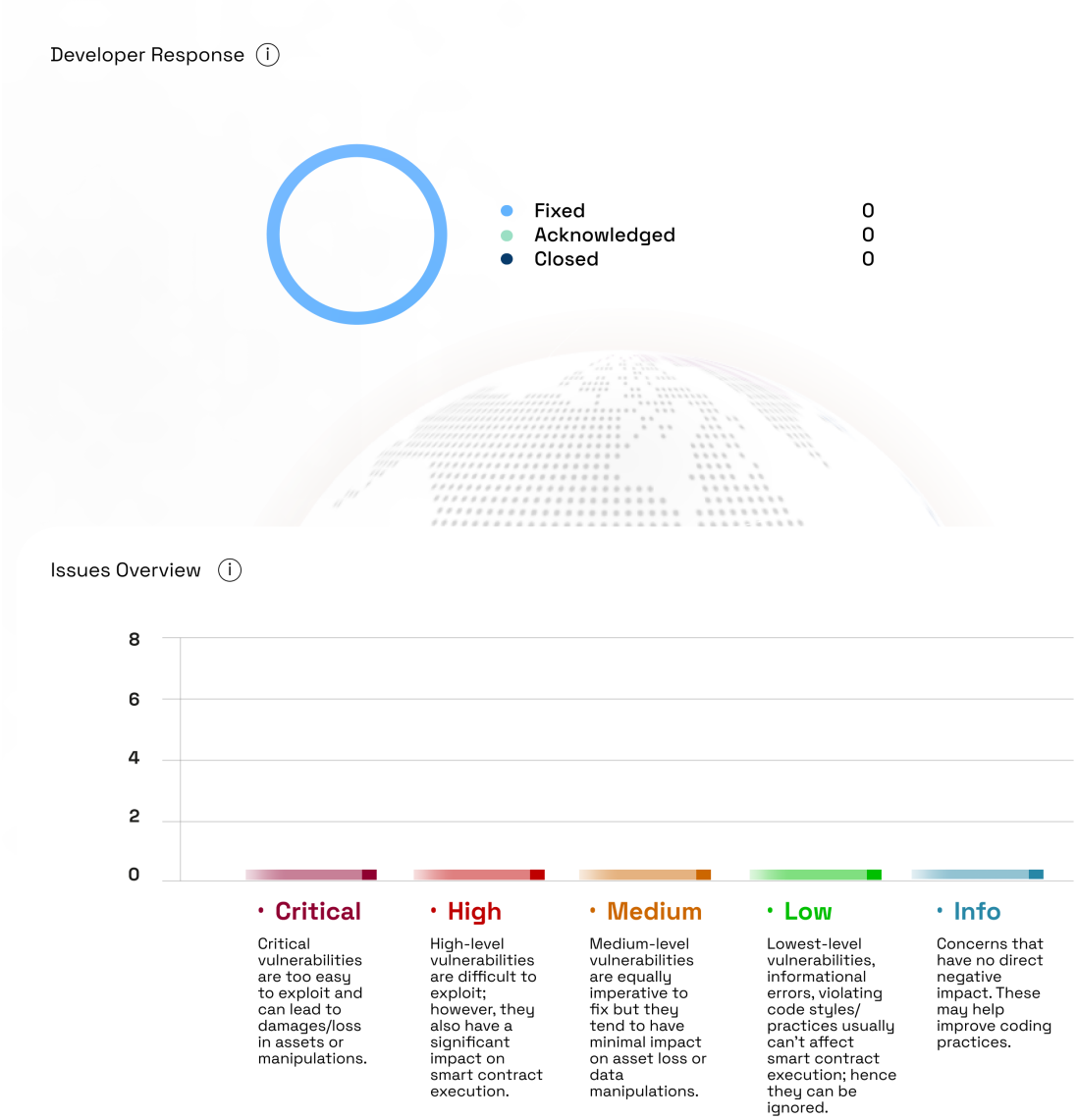
BlockApex has a focus on blockchain security, maintaining an expertise hub to navigate this dynamic field. We actively contribute to security research and openly share our findings with the community. Our work is available for review at our public repository, showcasing audit reports and insights into our innovative practices.

To stay informed about BlockApex's latest developments, breakthroughs, and services, we invite you to follow us on Twitter and explore our GitHub. For direct inquiries, partnership opportunities, or to learn more about how BlockApex can assist your organization in achieving its security objectives, please visit our Contact page at our website , or reach out to us via email at hello@blockapex.io.

Contents

1 Executive Summary

BlockApex conducted a comparitive audit for the UniswapV2Factory.sol and UniswapV2Router02.sol smart contracts under the UniswapV2 directory for the ElectroSwapV2 Protocol. This equivalency review employed a manual checking approach to determine any changes of major or minor category focusing exclusively on a line-by-line examination of the contract's code to identify potential vulnerabilities and coding best practices deviations that may have derived from introducing changes from the renowned version of the UniswapV2 Implementation.



1.1 Scope

1.1.1 In Scope

The audit focuses on the UniswapV2Factory and Router smart contracts. UniswapV2 is a decentralized automated market maker protocol that allows anyone to swap token A for token B.

- The UniswapV2Factory smart contract is a factory pattern designed singleton that deploys UniswapV2Pair contracts that implement the actual AMM protocol where Liquidity Providers provide liquidity to earn fees and traders swap their funds for a required token within a UniswapV2Pair.
- The UniswapV2Router02 smart contract is the main entry point for the Uniswap UI and other web and decentralized applications working on top of Uniswap. Router makes it easier to create pairs, add and remove liquidity, calculate prices for all possible swap variations and perform actual swaps. Router works with all pairs deployed via the Factory contract.

Contracts in Scope:

All Files under the folder: contracts/UniswapV2/**.sol

Commit Hash: 1a2fd21688492df599593754ac80f57cf6273f8b

UniswapV2Factory Deployed Link: https://blockexplorer.electroneum.com/address/0x203D550ed6fA9dAB8A4190720CF9F65138abd15B/contracts#address-tabs

UniswapV2Router02 Deployed Link: https://blockexplorer.electroneum.com/address/0x072D4706f9A383D5608BD14B09b41683cb95fFd7/contracts#address-tabs

1.1.2 Out of Scope

All features or functionalities not delineated within the “In Scope” section of this document shall be deemed outside the review of this audit. This exclusion particularly applies to the backend operations of the ElectroSwapLockerV2 contracts associated with the platform & any other external libraries

1.2 Methodology

The audit of the ElectroSwap smart contract was conducted over the course of 5 days, utilizing a straightforward, manual code review complimented with comparitive review approach by one auditor. The methodology began with a reconnaissance phase to compare the UniswapV2 original repository. Following this, the auditor engaged in a detailed, line-by-line examination of the code. This manual review process focused on comparing the repository code and implementation files in order to identify any logical flaws and security vulnerabilities in newly introduced differences, if any, while ensuring adherence to Solidity best practices, security design patterns, and coding standards for clarity and efficiency.

1.3 Status Descriptions

Acknowledged: The issue has been recognized and is under review. It indicates that the relevant team is aware of the problem and is actively considering the next steps or solutions.

Fixed: The issue has been addressed and resolved. Necessary actions or corrections have been implemented to eliminate the vulnerability or problem.

Closed: This status signifies that the issue has been thoroughly evaluated and acknowledged by the development team. While no immediate action is being taken.

2 Findings and Risk Analysis

2.1 Critical Issues

- No Issues Found

2.2 High Issues

- No Issues Found

2.3 Medium Issues

- No Issues Found

2.4 Low Issues

- No Issues Found

2.5 Info Issues

- No Issues Found

Disclaimer:

The smart contracts provided by the client with the purpose of security review have been thoroughly analyzed in compliance with the industrial best practices till date w.r.t. Smart Contract Weakness Classification (SWC) and Cybersecurity Vulnerabilities in smart contract code, the details of which are enclosed in this report.

This report is not an endorsement or indictment of the project or team, and they do not in any way guarantee the security of the particular object in context. This report is not considered, and should not be interpreted as an influence, on the potential economics of the token (if any), its sale, or any other aspect of the project that contributes to the protocol's public marketing.

Crypto assets/ tokens are the results of the emerging blockchain technology in the domain of decentralized finance and they carry with them high levels of technical risk and uncertainty. No report provides any warranty or representation to any third-party in any respect, including regarding the bug-free nature of code, the business model or proprietors of any such business model, and the legal compliance of any such business. No third party should rely on the reports in any way, including to make any decisions to buy or sell any token, product, service, or asset. Specifically, for the avoidance of doubt, this report does not constitute investment advice, is not intended to be relied upon as investment advice, is not an endorsement of this project or team, and is not a guarantee as to the absolute security of the project. Smart contracts are deployed and executed on a blockchain. The platform, its programming language, and other software related to the smart contract can have vulnerabilities that can lead to hacks. The scope of our review is limited to a review of the programmable code and only the programmable code, we note, as being within the scope of our review within this report. The smart contract programming language itself remains under development and is subject to unknown risks and flaws. The review does not extend to the compiler layer or any other areas beyond the programming language's compiler scope that could present security risks.

This security review cannot be considered a sufficient assessment regarding the utility and safety of the code, bug-free status, or any other statements of the contract. While BlockApex has done their best in conducting the analysis and producing this report, it is important to note that one should not rely on this report only - we recommend proceeding with several independent code security reviews and a public bug bounty program to ensure the security of smart contracts.