ADI DLT FOUNDATION

SMART CONTRACTS REVIEW REPORT

zokyo

September 27th 2024 | v. 1.0

Table of Contents

CONFIDENTIALITY NOTICE:

This report contains sensitive information about the security of the ADI DLT Foundation. It is intended for the sole use of ADI DLT Foundation and should not be distributed or shared without express written permission.

SCOPE

- https://github.com/adi-foundation/zksync-era commit hash:
  6f42d3b0febfbf81bae9c349c93ef8de6a792529
- https://github.com/adi-foundation/zksync-era-contracts commit hash:
  446d391d34bdb48255d5f8fef8a8248925fc98b9
- https://github.com/adi-foundation/zksync-era-compiler-solidity commit hash:
  92d1433bb7c2f9ea3094852786ed1e3eb92aead7
- https://github.com/adi-foundation/zksync-era-hardhat commit hash:
  1a847195a4eeee9598d930e29fa58791fc240e36
- https://github.com/adi-foundation/zksync-era-explorer commit hash:
  d951ad07711b36cf52eb4d5099e33ff8bcc04705
- https://github.com/adi-foundation/zksync-era-portal commit hash:
  485d8791fd7003f1bf7b65b9c7c6515c95511ebd

Executive Summary

Zokyo conducted a comprehensive ADI DLT Foundation security audit from September 9, 2024, to September 27, 2024. The audit aimed to identify potential vulnerabilities and weaknesses within the codebase and overall security posture.

The list of the original repositories (respectively):
- https://github.com/matter-labs/zksync-era
- https://github.com/matter-labs/era-contracts
- https://github.com/matter-labs/era-compiler-solidity
- https://github.com/matter-labs/hardhat-zksync
- https://github.com/matter-labs/block-explorer
- https://github.com/matter-labs/dapp-portal

The list of previous audits being reviewed:
- Layer 1 Smart Contracts by OpenZeppelin, from 2022-09-05 to 2022-09-30. - Layer 1 Diff Audit (Upgrade Audit) by OpenZeppelin, from 2022-11-21 to 2022-11-25.
- Layer 1 Diff Audit (Upgrade Audit), by OpenZeppelin, from 2023-02-06 to 2023-02-17.
- Layer 1 Public Contest by Code4rena, from 2022-10-28 to 2022-11-09. - Layer 1 Smart Contracts by Secure3, from 2022-10-22 to 2022-11-06. - WETH Bridge Audit by OpenZeppelin, from 2023-03-27 to 2023-03-31. - Bridge and .transfer & .send by OpenZeppelin, from 2023-04-24 to 2023-05-01. - GnosisSafeZk Assessment by OpenZeppelin, from 2023-05-22 to 2023-05-26. - Upgrade System by OpenZeppelin, from 2023-06-26 to 2023-06-30. - Layer 1 Messenger Upgrade by OpenZeppelin, from 2023-08-30 to 2023-09-14. - Diff and Governance Audit by OpenZeppelin, from 2023-12-04 to 2023-12-22. - Layer 2 Bootloader by OpenZeppelin, from 2022-11-28 to 2022-12-23. - Layer 2 Fee Model and Token Bridge by OpenZeppelin, from 2023-01-23 to 2023-02-17.
- Layer 2 System Contracts Public Contest by Code4rena, from 2023-03-10 to 2023-03-19.

- Layer 2 Block Refactor by OpenZeppelin, from 2023-07-25 to 2023-07-31. - Keccak256 Upgrade by OpenZeppelin, from 2023-10-23 to 2023-10-27. - Layer 1 & 2 Diff Audit by OpenZeppelin, from 2023-11-27 to 2023-12-05. - Short-Term Fee Model Changes by OpenZeppelin, from 2023-12-06 to 2023-12-13.
- ZK Proof System by Halborn, from 2023-01-09 to 2023-03-08.
- Smart Contract Security Assessment by Halborn, from July 12th, 2023 - July 20th, 2023.
- SNARK Wrapper by Spearbit, November 2023
- EIP-4844 Support by OpenZeppelin, February 2024

We are pleased to report that **no critical, high or medium-severity vulnerabilities were discovered during the audit. However, we identified low-severity issues and** opportunities for enhancing the security posture. This report presents our detailed findings and actionable recommendations to address these issues.

SCOPE AND METHODOLOGY

The scope of the audit included:

- **Comprehensive code review:** We thoroughly examined ADI DLT Foundation's codebase, focusing on the Rust, TypeScript, and Solidity components.
- **Previous audits analysis:** We’ve analyzed the audits previously assessed on the provided codebase by different security firms.
- **Thorough vulnerability mapping:** We conducted extensive vulnerability mapping, referencing industry best practices and known attack vectors specific to the systems, to identify potential areas of weakness.

Our methodology involved:

- **Static code analysis:** We used automated tools to scan the codebase for common vulnerabilities and coding errors.
- **Manual code review:** Our experienced security engineers manually reviewed the codebase to identify potential security flaws that automated tools could not detect.
- **Threat modeling:** We constructed threat models to identify potential attack scenarios specific to ADI DLT Foundation’s architecture and assess their likelihood and impact.
- **Penetration testing:** We attempted to exploit potential vulnerabilities to assess their severity and impact within the context of the environment.

DETAILED FINDINGS

Low-Severity Issues

1. Node version contains known vulnerabilities:

○ **Description:** The `node` docker image version `18,17.1-alpine` has been used. It is known to have multiple vulnerabilities within multiple included packages, such as libssl3, node, and busybox.

○ **Recommendation:** A minor upgrade to version `18.20.4-alpine` could help lower the vulnerabilities count from 29 to 3, while a major upgrade to version `22.9-alpine` will help eliminate all known vulnerabilities.

2. Improper Verification of Cryptographic Signature:

○ **CWE-347**

○ **CVE-2024-42459, CVE-2024-42460, CVE-2024-42461**

○ **Description:** package `@ethersproject/abi` uses the Elliptic package version 6.5.6 which is known to have critical vulnerabilities listed above

○ **Recommendation:** upgrade Elliptic package to version 6.5.7

Informational Issues And Recommendations

1. Being up to date with audited repositories.

While the original repositories are being regularly audited and the Bug Bounty program is running, it is a good idea to be updated with the latest security updates. Right now, we can see that the provided repositories are a bit out of date with the originals. Make sure to keep the code in sync with the upstream repository.

DISCLAIMER

This report is intended solely for ADI DLT Foundation's use and should not be distributed or shared without express written permission. The information contained in this report reflects our findings and recommendations based on the audit conducted from September 9, 2024, to September 27, 2024. While we have exercised due care and diligence in conducting this audit, we cannot guarantee that ADI DLT Foundation is entirely free from vulnerabilities. We recommend that the ADI DLT Foundation team continue to monitor and assess their security posture on an ongoing basis.

We are grateful for the opportunity to work with the ADI DLT Foundation team.

The statements made in this document should not be interpreted as an investment or legal advice, nor should its authors be held accountable for the decisions made based on them.

Zokyo Security recommends the ADI DLT Foundation team put in place a bug bounty program to encourage further analysis of the smart contract by third parties.

zokyo