Aligned Layer

Security Assessment

December 2024

FUZZING LABS

Contents

About FuzzingLabs

Founded in 2021 and headquartered in Paris, FuzzingLabs is a cybersecurity startup specializing in vulnerability research, fuzzing, and blockchain security. We combine cutting-edge research with hands-on expertise to secure some of the most critical components in the blockchain ecosystem.

At FuzzingLabs, we aim to uncover and mitigate vulnerabilities before they can be exploited. Over the past year, our tools and methodologies have identified hundreds of vulnerabilities in essential blockchain components, such as RPC libraries, cryptographic systems, compilers, and smart contracts. We collaborate with leading protocols and foundations to deliver open-source security tools, continuous audits, and comprehensive fuzzing services that help secure the future of blockchain technology.

If you're interested, we have a blog available at fuzzinglabs.com and an X account @FuzzingLabs. You can also contact us at contact@fuzzinglabs.com.

Executive Summary

Goals

The security audit was focused on a comprehensive review of the project's updates, with specific attention to the ERC-20 token and airdrop components. The following key areas were in scope:

1. **Smart Contract Analysis:**
    - Evaluate the security of the ERC-20 token contract for compliance with standards and resistance to common attack vectors.
    - Analyze the claim contract for logical integrity and secure token distribution.
    - Audit the airdrop deployment script to verify its correctness and safeguard against potential misuse.

This scope was tailored to ensure the security and integrity of the token and airdrop systems while prioritizing areas critical to their functionality and deployment readiness.

Project Summary

About Aligned Layer

Aligned Layer is a decentralized network designed to provide fast, efficient, and low-cost verification of zero-knowledge (ZK) and validity proofs on the Ethereum blockchain. It seeks to overcome the limitations of current blockchain verification systems, which are often slow and expensive due to the need for nodes to re-execute each transaction. By offloading the computation off-chain, Aligned Layer enables faster proof verification and significantly reduces costs.

The platform operates in two modes: **fast mode** and **aggregation mode**. In **fast mode**, a subset of Ethereum's validators (operators) verify proofs in parallel, posting the results to Ethereum only after reaching a two-thirds consensus. This approach allows Aligned Layer to achieve verification speeds of over 1,000 proofs per second, far outpacing Ethereum's native capabilities. In **aggregation mode**, the system further compresses proofs for even greater efficiency at scale.

Aligned Layer is particularly useful for applications requiring large-scale computations with the assurance that they are verified in a trustless manner. It supports various proof systems, making it versatile for developers working on ZK technology, including zk-rollups, identity protocols, and decentralized applications that demand high throughput and low latency.

The goal of Aligned Layer is to accelerate Ethereum's roadmap, supporting the adoption of verifiable computation and making ZK verification accessible and affordable to a wider range of developers.

On chain review for Aligned Layer Airdrop

Key Findings:

1. **Contract Initialization and State:**
    - Both the `AlignedToken` and `ClaimableAirdrop` contracts are correctly initialized, with accurate states and supply distribution.
    - The `ClaimMerkleRoot` is not set, and the `ClaimableAirdrop` contract is paused, making the airdrop unclaimable at this stage.
2. **Fuzzing Results:**
    - Extensive fuzzing of the `AlignedToken` and `ClaimableAirdrop` contracts (over 477M executions combined) revealed no issues.
3. **Supply Distribution:**
    - The `AlignedToken` supply is correctly allocated:
        - **Foundation Safe**: 7.4 billion ALIGN tokens.
        - **Token Distributor Safe**: 2.6 billion ALIGN tokens.
4. **Gnosis Safes:**
    - Gnosis Safes for the foundation and token distributor are well-configured with a threshold of 5 out of 8 owners.
5. **Online Scanner Results:**
    - Online scanners (`de.fi`, `tokensniffer.com`) flagged multiple false positives:
        - Missing liquidity pairs (to be created later).
        - Proxy contract and ownership renunciation issues (scanners are unreliable in these checks).
6. **Security:**
    - No vulnerabilities detected.

Recommendations:

- Prefund the 0x57C..7CF Gnosis Safe address with ETH to align with other safe owners.

Conclusion:

The contracts and safes are securely configured, and the token supply is appropriately distributed. While the online scanners raised false positives, these do not reflect any actual vulnerabilities. However, the airdrop is not yet

functional as the `ClaimMerkleRoot` is unset, and the `ClaimableAirdrop` contract remains paused.

Conclusion

The audit of the Aligned Layer Airdrop and ERC-20 token components demonstrates that the system is securely configured and adheres to best practices. Both the `AlignedToken` and `ClaimableAirdrop` contracts were thoroughly reviewed, with extensive fuzzing (over 477M executions) revealing no vulnerabilities. The contracts are correctly initialized, and the token supply is appropriately allocated across the foundation and token distributor safes.

The Gnosis Safes managing the token supply are well-configured, with a threshold of 5 out of 8 owners, ensuring strong access control. While online scanners flagged false positives, these do not reflect actual vulnerabilities.

However, the airdrop is currently non-functional as the `ClaimMerkleRoot` is unset, and the `ClaimableAirdrop` contract remains paused. It is recommended to address these issues and prefund the Gnosis Safe at 0x57C..7CF with ETH for consistency with other safes.

Overall, the audit confirms the robustness and readiness of the token and airdrop components, with minor adjustments required to ensure complete functionality and deployment readiness.

Disclaimer

This report is provided under the terms of the agreement between FuzzingLabs and the client. It is intended solely for the client's use and may not be shared or referenced without FuzzingLabs' prior written consent. The findings in this report are based on a point-in-time assessment and do not guarantee the absence of vulnerabilities or security flaws. FuzzingLabs cannot ensure future security as systems and threats evolve. We recommend continuous monitoring, independent assessments, and a bug bounty program.

This report is not financial, legal, or investment advice, and should not be used for decision-making regarding project involvement or investment. FuzzingLabs aims to help reduce risks, but we do not provide any guarantees regarding the complete security of the technology assessed.