OFFSIDE LABS

Presale 0.1.1

Smart Contract Security Assessment

November 2025

Prepared for:

Meteora

Prepared by:

Offside Labs

Sirius Xie

Contents

1 About Offside Labs

Offside Labs is a leading security research team, composed of top talented hackers from both academia and industry.

We possess a wide range of expertise in modern software systems, including, but not limited to, *browsers*, *operating systems*, *IoT devices*, and *hypervisors*. We are also at the forefront of innovative areas like *cryptocurrencies* and *blockchain technologies*. Among our notable accomplishments are remote jailbreaks of devices such as the **iPhone** and **PlayStation 4**, and addressing critical vulnerabilities in the **Tron Network**.

Our team actively engages with and contributes to the security community. Having won and also co-organized *DEFCON CTF*, the most famous CTF competition in the Web2 era, we also triumphed in the **Paradigm CTF 2023** within the Web3 space. In addition, our efforts in responsibly disclosing numerous vulnerabilities to leading tech companies, such as *Apple*, *Google*, and *Microsoft*, have protected digital assets valued at over **$300 million**.

In the transition towards Web3, Offside Labs has achieved remarkable success. We have earned over **$9 million** in bug bounties, and **three** of our innovative techniques were recognized among the **top 10 blockchain hacking techniques of 2022** by the Web3 security community.

https://offside.io/

https://github.com/offsidelabs

https://twitter.com/offside_labs

2 Executive Summary

Introduction

Offside Labs completed a security audit of *Meteora Presale* smart contracts, starting on November 8th, 2025, and concluding on November 11th, 2025.

Project Overview

The Presale program is designed to support new token launches with flexible and secure presale mechanisms. It allows creators to run presales in multiple formats, giving full control over how tokens are sold and how unsold tokens are handled.

In this release, the protocol updates the presale timeline, introduces an immediate-release timestamp, adds a configurable option to disable withdrawals in fixed-price mode, adds a “no early end” option in both fixed-price and FCFS modes, and tightens the registry-cap constraint when whitelist mode is set to permissioned.

Audit Scope

The assessment scope contains mainly the smart contracts of the presale program for the *Meteora Presale* project.

The audit is based on the following specific branches and commit hashes of the codebase repositories:

- Meteora Presale
  - Codebase: `https://github.com/MeteoraAg/presale`
  - PR-33
    - Commit Hash: 50862dad540c07ca5f41ffca25e0d5bd7cab8246
    - Codebase Link: `PR-33`

We listed the files we have audited below:

- Meteora Presale
  - programs/presale/src/constants.rs
  - programs/presale/src/instructions/initialize_presale/params.rs
  - programs/presale/src/instructions/initialize_presale/process_create_presale_vault.rs
  - programs/presale/src/instructions/process_claim.rs
  - programs/presale/src/instructions/process_close_escrow.rs
  - programs/presale/src/instructions/process_deposit.rs
  - programs/presale/src/instructions/process_initialize_extra_presale_params.rs
  - programs/presale/src/instructions/process_perform_unsold_base_token_action.rs
  - programs/presale/src/instructions/process_refresh_escrow.rs
  - programs/presale/src/instructions/process_withdraw.rs
  - programs/presale/src/lib.rs

- programs/presale/src/math/claim_math.rs
- programs/presale/src/presale_mode_handler/fcfs_presale.rs
- programs/presale/src/presale_mode_handler/fixed_price_presale.rs
- programs/presale/src/presale_mode_handler/mod.rs
- programs/presale/src/presale_mode_handler/prorata_presale.rs
- programs/presale/src/state/fixed_price_presale_params.rs
- programs/presale/src/state/presale.rs

Findings

The security audit revealed:

- 0 critical issue
- 0 high issue
- 0 medium issue
- 1 low issue
- 0 informational issue

Further details, including the nature of these issues and recommendations for their remediation, are detailed in the subsequent sections of this report.

3 Summary of Findings

ID	Title	Severity	Status
01	Missing validation in initialize_fixed_price_presale_args IX	Low	Fixed

4 Key Findings and Recommendations

4.1 Missing validation in initialize_fixed_price_presale_args IX

Severity: Low	Status: Fixed
Target: Smart Contract	Category: Data Validation

Description

In the `initialize_fixed_price_presale_args` IX, the `FixedPricePresaleExtraArgs` account is initialized from the IX parameter `InitializeFixedPricePresaleExtraArgs`. The program code defines a `InitializeFixedPricePresaleExtraArgs.validate` method to check the IX parameters, but the IX doesn't call it.

Impact

Without invoking `validate`, a user can pass malicious values (e.g., `q_price == 0`) and create a malformed Presale account.

Recommendation

It's recommended to call `InitializeFixedPricePresaleExtraArgs.validate` inside `handle_initialize_fixed_price_presale_args`.

Mitigation Review Log

Fixed in the commit ff88ced4270536db909603b2165993ad45219cb6.

5 Disclaimer

This audit report is provided for informational purposes only and is not intended to be used as investment advice. While we strive to thoroughly review and analyze the smart contracts in question, we must clarify that our services do not encompass an exhaustive security examination. Our audit aims to identify potential security vulnerabilities to the best of our ability, but it does not serve as a guarantee that the smart contracts are completely free from security risks.

We expressly disclaim any liability for any losses or damages arising from the use of this report or from any security breaches that may occur in the future. We also recommend that our clients engage in multiple independent audits and establish a public bug bounty program as additional measures to bolster the security of their smart contracts.

It is important to note that the scope of our audit is limited to the areas outlined within our engagement and does not include every possible risk or vulnerability. Continuous security practices, including regular audits and monitoring, are essential for maintaining the security of smart contracts over time.

Please note: we are not liable for any security issues stemming from developer errors or misconfigurations at the time of contract deployment; we do not assume responsibility for any centralized governance risks within the project; we are not accountable for any impact on the project's security or availability due to significant damage to the underlying blockchain infrastructure.

By using this report, the client acknowledges the inherent limitations of the audit process and agrees that our firm shall not be held liable for any incidents that may occur subsequent to our engagement.

This report is considered null and void if the report (or any portion thereof) is altered in any manner.

OFFSIDE LABS

https://offside.io/

https://github.com/offsidelabs

https://twitter.com/offside_labs