Bug Bounty Program

Program Overview

Raydium's full bug bounty program with ImmuneFi can be found at the below link https://immunefi.com/bounty/raydium/ The bug bounty program covers Raydium's open-source Concentrated Liquidity Market Maker (CLMM) smart contracts and is focused on preventing thefts and freezing of funds. UI bugs do not qualify for the bug bounty program. If you have information on vulnerabilities or bugs, please go through the official channels on the ImmuneFi program site: https://immunefi.com/bounty/raydium/

Rewards

Rewards are distributed according to the impact of the vulnerability based on the Immunefi Vulnerability Severity Classification System V2.2 . Smart Contracts 1. 1. 2. Critical 3. USD 50,000 to USD 505,000 4. 2. 5. High 6. USD 40,000 7. 3. 8. Medium 9. USD 5,000 All bug reports must include a Proof of Concept (PoC) demonstrating how the vulnerability can be exploited to impact an asset-in-scope to be eligible for a reward. Critical and High severity bug reports should also include a suggestion for a fix. Explanations and statements are not accepted as PoC and code is required. Critical smart contract vulnerabilities are capped at 10% of economic damage, primarily taking into consideration funds at risk, but also PR and branding aspects, at the discretion of the team. However, there is a minimum reward of USD 50,000. The following vulnerabilities are not eligible for a reward: * For the CLMM program, vulnerabilities marked in the * Ottersec security review * are not eligible for a reward. For the Hybrid AMM program, vulnerabilities marked in the * Kudelski security review * , * Ottersec security review * , and *MadShield security * review are not eligible for a reward. * The CLMM contract emits trading fees and farming yield tokens to LPs. If tokens from the vault or fees were drained by an attacker, however, users would not be able to claim yield and transactions would fail. This is by design and not a vulnerability Payouts are handled by Raydium directly and are denominated in USD. However, payouts are done in RAY.

Programs in Scope

View details, developer documentation, and testing environments for each program: CLMM Bug Bounty Details Hybrid AMM Bug Bounty Details

Impacts in Scope

Only the following impacts are accepted within this bug bounty program. All other impacts are not considered in-scope, even if they affect something in the assets in scope tables.

Critical

* Direct theft of any user funds, whether at-rest or in-motion, other than unclaimed yield * Permanent freezing of funds * Vulnerabilities that could freeze user funds permanently or involve the draining or theft of funds without user transaction approval

High

* Theft of unclaimed yield * Permanent freezing of unclaimed yield * Temporary freezing of funds for any amount of time * Vulnerabilities that could freeze user funds temporarily or intentionally alter the value of user funds

Medium

* Smart contract unable to operate due to lack of token funds * Block stuffing for profit * Griefing (e.g. no profit motive for an attacker, but damage to the users or the protocol) * Theft of gas * Unbounded gas consumption

Out of Scope & Rules

The following vulnerabilities are excluded from the rewards for this bug bounty program: * Attacks that the reporter has already exploited themselves, leading to damage * Attacks requiring access to leaked keys/credentials * Attacks requiring access to privileged addresses (governance, strategist) Smart Contracts and Blockchain * Incorrect data supplied by third party oracles * * Not to exclude oracle manipulation/flash loan attacks * Basic economic governance attacks (e.g. 51% attack) * Lack of liquidity * Best practice critiques * Sybil attacks * Centralization risks The following activities are prohibited by this bug bounty program: * Any testing with mainnet or public testnet contracts; all testing should be done on private testnets * Any testing with pricing oracles or third party smart contracts * Attempting phishing or other social engineering attacks against our employees and/or customers * Any testing with third party systems and applications (e.g. browser extensions) as well as websites (e.g. SSO providers, advertising networks) * Any denial of service attacks * Automated testing of services that generates significant amounts of traffic * Public disclosure of an unpatched vulnerability in an embargoed bounty

Previous Access Controls Next CLMM Bug Bounty Details Last modified6mo ago