CircuitDAO Invite-Only Program

Summary Report
May 2025

Content Index

Immunefi

Overview

Immunefi Invite-Only Programs (IOPs) are invite-only, time-limited events that connect handpicked security researchers to project code.

From April 9 to April 24, 2025, the CircuitDAO protocol offered $2,000 USD in guaranteed rewards to each of the two selected security researchers, along with up to $6,000 USD in rewards for vulnerabilities and insights.

Immunefi's Discord server hosted a channel for enhanced, two-way communication between whitehats and the **CircuitDAO** team, improving feedback and response times. Managed Triaging was also activated for the duration of this event, streamlining the resolution process for incoming bug reports.

During this event, 1 critical, 1 high and 1 medium reports were found on the target contracts.

The **CircuitDAO** team rewarded $2,000 in guaranteed rewards to two selected security researchers, along with an additional $6,000 for their 3 submissions.

CircuitDAO Introduction

Circuit is a DeFi protocol built on the Chia blockchain.

Specifically, Circuit is a collateralized debt position (CDP) protocol that allows users to borrow Bytecash (BYC), a USD stablecoin issued by the protocol, against XCH, the native token of Chia.

For more information about CircuiDAo, please visit https://docs.circuitdao.com/.

Scope Of Assets

The target assets in scope for this IOP were Smart Contracts

The total nSLOC was 6,750.

Summary

Duration:
2 weeks

Boost Date:
9 Apr - 24 Apr 2025

Rewards Pool:
Up to $10,000

nSLOC:
6,750

Submitted reports:
6

Security researchers:
2

Valid vulnerabilities:
3

Insight reports:
0

Immunefi

Total Whitehat Participation

2

Total Researchers

2

Paid Researchers

Leaderboard

Position	Reward	Username	Valids	Insights
1	**$8,000**	perseverance	3	0
2	**$2,000**	blocksmith0	0	0

Top 3 Reports

Attackers can exploit Lack of Validation in BYC Coin Issuance Process to Issue arbitrary amount of BYC Coin

Report number: 43705

Submitted by: @perseverance

Target: https://github.com/immunefi-team/CircuitDAO-IoP/tree/main/circuit_puzzles

Impacts:

- Protocol insolvency
- Permanent significant depeg of stablecoin (BYC), e.g. by forcing undercollateralization

Program Action: Confirmed as critical severity.

Report Excerpt:

The BYC coin issuance process in the Circuit DAO protocol allows users to borrow BYC coins while providing collateral. However, there is a critical vulnerability in the validation process that could allow attackers to exploit Lack of Validation of `amount` in `byc_issuing_coin_info` BYC Coin Issuance Process to Issue arbitrary amount of BYC Coin. This attack can also depeg BYC because BYC will be under collaterized.

Announcer Owner Can Inflate Announcers Registry Entries via Mutate and Register Loop to Claim Most of Rewards

Report number: 44355

Submitted by: @perseverance

Target: https://github.com/immunefi-team/CircuitDAO-IoP/tree/main/circuit_puzzles

Impacts:

- Theft of unclaimed yield

Program Action: Confirmed as high severity.

Report Excerpt:

The announcer owner can repeatedly use the `announcer_mutate` operation to change their `atom_announcer` coin's `INNER_PUZZLE_HASH` and then re-register the announcer using the `announcer_register` operation with the new hash in the `announcer_registry`. Because the registry uses the mutable `inner_puzzle_hash` as the unique identifier instead of the immutable `LAUNCHER_ID`, the owner can create multiple distinct entries in the registry, all ultimately controlled by them. This inflates the apparent number of unique announcers, causing the reward distribution mechanism (`MINT` operation in the registry) to allocate them a disproportionately large share of the CRT rewards, effectively draining rewards intended for other legitimate participants.

Atom Announcer Owner Can Nulify Financial Penalty by Self-Penalizing

Report number: 44324

Submitted by: @perseverance

Target: https://github.com/immunefi-team/CircuitDAO-IoP/tree/main/circuit_puzzles

Impacts:

- Griefing (e.g. no profit motive for an attacker, but damage to the users or the protocol)
- Protocol insolvency

Program Action: Confirmed as medium severity.

Report Excerpt:

The `announcer_penalize.clsp` puzzle allows the keeper (means anyone), including the announcer coin's owner, to trigger a penalty if the conditions are met. While the penalty correctly reduces the `DEPOSIT` amount stored in the announcer coin's state, the keeper triggering the penalty (the "keeper") can claim the slashed amount. If the owner self-penalizes, they can direct this slashed amount back to themselves, effectively nullifying the intended financial disincentive of the penalty mechanism for the announcer.

So the attacker can potentially exploit this to behave badly. This can potentially affect protocol's health.

Immunefi

End of Report