Audit Report for Idle Finance Audit Competition

Introduction to Hats.finance

Hats.finance builds autonomous security infrastructure for integration with major DeFi protocols to secure users' assets. It aims to be the decentralized choice for Web3 security, offering proactive security mechanisms like decentralized audit competitions and bug bounties. The protocol facilitates audit competitions to quickly secure smart contracts by having auditors compete, thereby reducing auditing costs and accelerating submissions. This aligns with their mission of fostering a robust, secure, and scalable Web3 ecosystem through decentralized security solutions.

Idle DAO

Idle DAO is a decentralized collective that has created products for unlocking the power of decentralized finance.

The product to be audited, Yield Tranches (YT), enables users to deposit assets into a DeFi protocol with two risk-adjusted investment profiles. The audit aims to cover the latest changes in the contract, particularly focusing on the distribution of losses between the two tranches on-chain.

Competition Details:

Competition type: This was the first Hats.finance private audit competition and it had 6 individual auditors participating.

Participation Level: The competition had a partipication that lower than usual on hats.finance.

Duration: The competition ran for a duration of 12 days, providing a time-bound framework for participants to submit their findings.

Scope

1. **IdleCDO.sol:** Main file with all the logic for tranches management and for eventual loss management.
2. **IdleCDOInstadappLiteVariant.sol:** A variant of IdleCDO.sol with additional logic to handle Instadapp Lite integration for iETHv2 (which has withdrawal fees).

Total solidity lines of code in scope: 700

The commit hash to be audited is 2ae25e.. A fork of Idle Labs:idle-tranches repo 2ae25e..

Previous Audits

Previous audit reports

Pool size

- **Pool for Lows:** $900
- **Pool for Medium / High:** $17k
- **Cap for High:** 10k

- **Cap for Medium:** 5k

Issues Found

Issue #1:

Submitted by: @bahurum
Submission Hash: 0x081ee604f554cd0218c57f1a72cf73135b1724d6a35e8136cb5296b4150f1144
Issue Link
Severity: Low
Bounty Awarded: $1500

Description: The function `_checkStkIDLEBal()` intends to limit user deposits in a tranche. However, it's possible for a user to bypass this check by transferring tranche tokens to another account, thus enabling them to deposit more than their `stkIDLE` balance should allow.

Attack Scenario:

1. User deposits the maximum allowed amount with EOA #1, obtaining X tranche tokens.
2. User transfers these tokens to EOA #2.
3. User deposits again with EOA #1, obtaining another set of X tranche tokens.
4. Repeat steps 2 and 3.

Recommendation: It's recommended to introduce an internal mapping that stores the tranche balances of each user, ensuring that if a user transfers tranche tokens out, they will need to stake additional IDLE to mint additional tranche tokens. This change should be reflected in the `_checkStkIDLEBal()`, `_mintShares()`, and `_withdraw()` functions.

Issue #2 (out of scope):

Submitted by: Arnie

Issue Link

Bounty Awarded: $500

Although this issue was out of the scope of the audit competition, a small bounty was awarded in recognition of the dedication shown by the auditor.

Payout Details

The following payouts were made to the auditors for their contributions:

- **bahurum:** Awarded $1,500 for identifying a low-severity issue. Issue Link
- **Arnie:** Awarded $500 for an out-of-scope issue but recognized for overall dedication. Issue Link

The total payout for this competition was $2,000.

Disclaimer:

This report does not guarantee that the smart contracts examined are free from any security issues. It is always advisable to seek multiple opinions and conduct thorough testing before deploying critical smart contracts on the blockchain.

The audit competition for Idle Finance was focused on ensuring the robustness and security of the system, particularly the logic embedded in the in-scope files. The low-severity issue identified by @bahurum sheds light on a potential vulnerability that could allow users to bypass deposit limitations. By addressing this finding, Idle Finance can further enhance the security and reliability of its Yield Tranches product.