Ethena Security Review

Pashov Audit Group

Conducted by: sashik_eth, Dan Ogurtsov

February 20th 2024 - February 22nd 2024

Contents

1. About Pashov Audit Group

Pashov Audit Group consists of multiple teams of some of the best smart contract security researchers in the space. Having a combined reported security vulnerabilities count of over 1000, the group strives to create the absolute very best audit journey possible - although 100% security can never be guaranteed, we do guarantee the best efforts of our experienced researchers for your blockchain protocol. Check our previous work here or reach out on Twitter @pashovkrum.

2. Disclaimer

A smart contract security review can never verify the complete absence of vulnerabilities. This is a time, resource and expertise bound effort where we try to find as many vulnerabilities as possible. We can not guarantee 100% security after the review or even if the review will find any problems with your smart contracts. Subsequent security reviews, bug bounty programs and on-chain monitoring are strongly recommended.

3. Introduction

A time-boxed security review of the **ethena** repository was done by **Pashov Audit Group**, with a focus on the security aspects of the application's smart contracts implementation.

4. About Ethena

StakingRewardsDistributor is the contract from Ethena Finance - a synthetic dollar protocol built on Ethereum. The contract is a piece of the new staking rewards distribution system and the intermediary between the Off-chain service and the actual staking contract.

5. Risk Classification

Severity	Impact: High	Impact: Medium	Impact: Low
Likelihood: High	Critical	High	Medium
Likelihood: Medium	High	Medium	Low
Likelihood: Low	Medium	Low	Low

5.1. Impact

- High - leads to a significant material loss of assets in the protocol or significantly harms a group of users.
- Medium - only a small amount of funds can be lost (such as leakage of value) or a core functionality of the protocol is affected.
- Low - can lead to any kind of unexpected behavior with some of the protocol's functionalities that's not so critical.

5.2. Likelihood

- High - attack path is possible with reasonable assumptions that mimic on-chain conditions, and the cost of the attack is relatively low compared to the amount of funds that can be stolen or lost.
- Medium - only a conditionally incentivized attack vector, but still relatively likely.
- Low - has too many or too unlikely assumptions or requires a significant stake by the attacker with little or no incentive.

5.3. Action required for severity levels

- Critical - Must fix as soon as possible (if already deployed)
- High - Must fix (before deployment if not already deployed)
- Medium - Should fix
- Low - Could fix

6. Security Assessment Summary

***review commit hash* - 974992cbde8c5305578ba4edad357e64c25e14da**

***fixes review commit hash* - 995dcfed3424e628be9de763a562503594c08c51**

Scope

The following smart contracts were in scope of the audit:

- `StakingRewardsDistributor`

7. Executive Summary

Over the course of the security review, sashik_eth, Dan Ogurtsov engaged with Ethena to review Ethena. In this period of time a total of **1** issues were uncovered.

Protocol Summary

Protocol Name	Ethena
Repository	https://github.com/ethena-labs/ethena
Date	February 20th 2024 - February 22nd 2024
Protocol Type	Rewards Distribution contract

Findings Count

Severity	**Amount**
Low	1
Total Findings	**1**

Summary of Findings

ID	**Title**	**Severity**	**Status**
[L-01]	Renounce approvals from the previous mintContract	Low	Resolved

8. Findings

8.1. Low Findings

[L-01] Renounce approvals from the previous mintContract

`StakingRewardsDistributor` gives approvals for a list of `_assets` to `mint_contract`. `setMintingContract()` can set the new `mint_contract`. But previous asset approvals given to the previous `mintContract` are not revoked.

Consider implementing a function to renounce approvals from addresses.