Ethena Timelock Audit Report

Prepared by KupiaSec

Version 1.0

Auditors

KupiaSec

May 26th, 2025

Contents

1 About KupiaSec

KupiaSec is a team of Web3 security experts that operates with transparency and a meritocratic spirit.

KupiaSec executes the modified **MPA** model for the Private Audits, a.k.a. **Solo Audit by a Lead + Internal Competition + Mitigation Review**.

- Solo Audit by a Lead

  KupiaSec assigns a senior auditor as a Lead Auditor based on the protocol category. The Lead Auditor is responsible for the first phase and will be the main point of contact for the client. The Lead Auditor shares the analysis and findings with the team.

- Internal Competition

  KupiaSec assigns more than 3 assist auditors to conduct the second phase. The auditors compete to find the most issues and the best solutions. This phase ensures the protocol goes through a rigorous review process by "many eyes" in a competitive environment.

- Mitigation Review

  After the protocol team has fixed the issues, KupiaSec conducts a final review to ensure all the issues are resolved.

2 Disclaimer

The KupiaSec team makes every effort to find as many vulnerabilities in the code as possible in the given time but holds no responsibility for the findings in this document. A security audit by the team does not endorse the underlying business or product. The audit was time-boxed and the review of the code was solely on the security aspects of the solidity implementation of the contracts.

3 Risk Classification

	Impact: High	**Impact: Medium**	**Impact: Low**
Likelihood: High	Critical	High	Medium
Likelihood: Medium	High	Medium	Low
Likelihood: Low	Medium	Low	Low

4 Protocol Summary

The EthenaTimelockController is a custom timelock contract extending OpenZeppelin's TimelockController. It is designed for application-level modules and provides advanced features for managing delayed execution of operations.

5 Audit Scope

timelock-contract\src\EthenaTimelockController.sol

Summary of Commits

Project Name	Ethena Timelock
Repository	timelock-contract
Initial Commit	6441a5c10786...
Mitigation Commit	c0da4e947c86...

6 Executive Summary

KupiaSec executed a modified Multi-Phase Audit model, a.k.a. **Solo Audit by a Lead + Internal Competition + Mitigation Review**.

Auditor conducted the audit as the Lead Auditor.

Execution Timeline

Phase-1: Audit by a Lead	May 24th, 2025 - May 25th, 2025
Phase-2: Internal Competition	May 24th, 2025 - May 25th, 2025
Initial Report Delivery	May 26th, 2025
Phase-3: Mitigation Review	May 26th, 2025 - May 26th, 2025
Final Report Delivery	May 26th, 2025

Issues Found

Critical Risk	0
High Risk	0
Medium Risk	0
Low Risk	0
Informational	2
Gas Optimizations	0
Total Issues	2

Summary of Findings

[I-1] Whitelist logic limitation	Acknowledged
[I-2] Risk of double execution	Acknowledged

7 Findings

7.1 Informational

7.1.1 Whitelist logic limitation

Description: The current whitelist logic only verifies the target address and function selector, without checking the calldata or value. This can lead to unexpected behaviors.

- Execution with arbitrary ETH values.
- ERC20 tokens (e.g., USDT) being transferred to any address with any amount, if `(USDT, transfer)` is whitelisted.

Ethena: Acknowledged. We understand this risk and have updated our documentation in this pull request.

KupiaSec: Acknowledged.

7.1.2 Risk of double execution

Description: A whitelisted operation could be executed twice.

- An operation is scheduled for execution 1 day later.
- During the delay, the operation is whitelisted.
- The `executeWhitelisted()` function is called by `WHITELISTED_EXECUTOR_ROLE`.
- Since the scheduled operation isn't canceled, it executes again using `execute()`. This risk increases if anyone can execute operations.

Ethena: Acknowledged. We understand this risk and have updated our documentation in this pull request.

KupiaSec: Acknowledged.