certora

Security Assessment Report

aave

Risk Steward

April-2025

Prepared for:
Aave DAO

Code developed by:
BORED
GHOSTS
DEVELOPING

Table of content

Project Summary

Project Scope

Project Name	Repository (link)	Latest Commit Hash	Platform
Aave Risk Steward	Github Repository	c4f6bac	EVM

Project Overview

This document describes the verification of **Aave Risk Steward** code using manual code review. The work was undertaken from **April 15** to **April 17, 2025**.

The following contracts are considered in scope for this review:

- `src/contracts/RiskSteward.sol`
- `src/interfaces/IRiskSteward.sol`

The team performed a manual audit of all the solidity contracts. During the audit, Certora didn't find any significant issues in the code.

Protocol Overview

The **Risk Steward** is a privileged contract that enables authorized parties to safely update critical protocol risk parameters (supply/borrow caps, reserve LTV, price caps…) within predefined boundaries. It implements timelocks between updates and maximum change limits to prevent repetitive parameter adjustment that could destabilize the protocol.

This update aims to integrate Pendle PT price adapter and Aave's efficiency mode (e-Mode), allowing administrators to safely modify relevant parameters of these features.

Findings Summary

The table below summarizes the findings of the review, including type and severity details.

Severity	Discovered	Confirmed	Fixed
Critical	-	-	-
High	-	-	-
Medium	-	-	-
Low	-	-	-
Informational	-	-	-
Total	-	-	-

Severity Matrix

Impact	High	Medium	High	Critical
	Medium	Low	Medium	High
	Low	Low	Low	Medium
		Low	Medium	High
		Likelihood		

Detailed Findings

Audit Goals

1. The contract aims to update the discount rate of the `PendlePriceAdapter` contract. The interface used to interact with it should be compatible.
2. In order to validate the update parameters, the contract now retrieves the effective parameters by interacting with the Aave `Pool`. In the past, this information was read from the Aave `PoolDataProvider`. Thus, the correctness of the information obtained from the pool should remain the same as before.
3. Before allowing any changes in the system, the new parameters should be validated according to the time locks and maximum boundaries.
4. Changes in the contract's structure types have been introduced for better readability and comprehension. The contract should interact with these types accordingly to extract the relevant information from them.

Coverage and Conclusions

1. The interface used to update the discount rate of a Pendle PT token is correct and compatible with the adapter's ABI.
2. The contract reads information from the Aave `Pool` by using externally available interfaces, parses and interprets the results using the `Pool's` libraries. The information obtained from the pool remains consistent with the previous version.
3. Updating an e-Mode or a Pendle price adapter configuration systematically undergoes a verification process that only allows the changes to take effect if enough time has elapsed since the last update and if the delta is below the maximum percentage allowed.
4. The contract is compatible with the new structure types and reads the correct values.

Disclaimer

Even though we hope this information is helpful, we provide no warranty of any kind, explicit or implied. The contents of this report should not be construed as a complete guarantee that the contract is secure in all dimensions. In no event shall Certora or any of its employees be liable for any claim, damages, or other liability, whether in an action of contract, tort, or otherwise, arising from, out of, or in connection with the results reported here.

About Certora

Certora is a Web3 security company that provides industry-leading formal verification tools and smart contract audits. Certora's flagship security product, Certora Prover, is a unique SaaS product that automatically locates even the most rare & hard-to-find bugs on your smart contracts or mathematically proves their absence. The Certora Prover plugs into your standard deployment pipeline. It is helpful for smart contract developers and security researchers during auditing and bug bounties.

Certora also provides services such as auditing, formal verification projects, and incident response.