



# Security Assessment Report



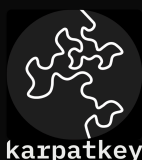
## Pool Exposure Steward

February-2025

*Prepared for:*

**Aave DAO**

*Code developed by:*



## Table of content

<b>Project Summary</b>	<b>3</b>
Project Scope	3
Project Overview	3
Protocol Overview	3
Coverage	4
Findings Summary	4
Severity Matrix	5
<b>Detailed Findings</b>	<b>6</b>
Informational Issues	6
I-01 Gas Efficiency Enhancement in withdrawFromV3	6
<b>Disclaimer</b>	<b>7</b>
<b>About Certora</b>	<b>7</b>

# Project Summary

## Project Scope

Project Name	Repository (link)	Latest Commit Hash	Platform
Finance Steward	<a href="#">GitHub Repository</a>	<a href="#">0865323</a>	EVM/Solidity 0.8

## Project Overview

This document describes the security considerations for **PoolExposureSteward**, including all findings and recommendations reported and discussed with the developing team. The work was undertaken on **February 16th, 2025**.

The following contract list is included in our scope:

- PoolExposureSteward.sol

## Protocol Overview

The **PoolExposureSteward** serves as a specialized financial steward for managing assets between Aave V2 and V3 pools. It enables deposits, withdrawals, and migrations by interacting with the Collector contract while ensuring that only pre-approved pools can be used. Additionally, it enforces strict role-based access with owner and guardian permissions and provides emergency rescue functions. It saves the need for frequent governance proposals of fund management without compromising security or decentralization.

## Coverage

1. The system's mechanisms were examined to ensure their integrity during our manual audit. Specific details regarding some of the checks performed and our thought processes are outlined below:
  - a. **Approved Pool Validation:**

- i. Before executing any pool-specific operation, the contract validates that the provided pool address is pre-approved using `_validateV3Pool(...)` or `_validateV2Pool(...)`, ensuring interactions only occur with recognized pools.
- b. **Safe Migration Logic:**
  - i. The migration functions (`_migrateV2toV3(...)` and `_migrateBetweenV3(...)`) securely handle funds by withdrawing assets from one pool and depositing the exact withdrawn amount into another, maintaining integrity during transfers.
- c. **Delegated Fund Handling by the Collector.**
- d. **Emergency Rescue Mechanisms.**
- e. **Access Control:**
  - i. Functions that manage deposits, withdrawals, and migrations require `onlyOwnerOrGuardian`, ensuring only authorized roles execute critical operations.

## Findings Summary

The table below summarizes the review's findings, including details on type and severity.

Severity	Discovered	Confirmed	Fixed
Critical	-	-	-
High	-	-	-
Medium	-	-	-
Low	-	-	-
Informational	1	1	-
<b>Total</b>	<b>1</b>	<b>1</b>	

# Severity Matrix

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

# Detailed Findings

ID	Title	Severity	Status
I-01	Gas Efficiency Enhancement in withdrawFromV3	Informational	acknowledged

## Informational Issues

I-01 Gas Efficiency Enhancement in withdrawFromV3	
Severity: <b>Informational</b>	Impact: <b>None</b>

### Description:

The function `withdrawFromV3(...)` retrieves the full reserve data using `getReserveData(input.underlying)` and only utilizes the `aTokenAddress` from the returned structure. A more gas-efficient approach would be to call the newly added (from 3.3) dedicated function `getReserveAToken(input.underlying)`, which directly returns the `aTokenAddress` without fetching the additional unnecessary data.

# Disclaimer

The Certora Prover takes a contract and a specification as input and formally proves that the contract satisfies the specification in all scenarios. Notably, the guarantees of the Certora Prover are scoped to the provided specification and the Certora Prover does not check any cases not covered by the specification.

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.