certora

Security Assessment Report

aave

SVROracleSteward

March-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
SVROracleSteward	Github Repository	119bfea	EVM

Project Overview

This document describes the verification of **SVROracleSteward** code using manual code review. The work was undertaken from **March 6** to **March 10, 2025**.

The following contracts are considered in scope for this review:

- `src/risk/SvrOracleSteward.sol`
- `src/risk/interfaces/ISvrOracleSteward.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 **SVROracleSteward** is a utility contract designed to facilitate the replacement of Aave's traditional oracle feeds to SVR oracle feeds while maintaining the ability to swap back in extreme situations. These experimental SVR feeds can be enabled through governance proposals while the ability to disable them and swap back to traditional feeds is given to a trusted Guardian which does not require any validation from governance.

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. Aave's oracle feeds are typically modified through governance proposals. The implementation of the steward must not conflict with the latter.

2. The Guardian role should have the least amount of privileges possible over the protocol. Its only ability should be to disable an SVR feed in case of emergency.

3. There must be no situation where a deviating SVR oracle feed cannot be replaced with a healthy one.

4. When disabling an SVR feed, the replacing oracle should always be the traditional one.

Coverage and Conclusions

1. The steward contract caches the oracle currently being used in storage when an SVR feed is enabled. If governance modifies Aave's oracle feed later on through proposals, the steward is prevented from falling back to the cached oracle which could be outdated. Governance has priority over the oracle to use.

2. Every external function is protected with access control. The Guardian only has the ability to disable an SVR feed using `disableSvrOracle()` marked as `onlyGuardian`, effectively switching back to the traditional and trusted oracle stored in cache.

3. The steward is, at all time, able to fall back to the traditional cached oracle feed in case of emergency as long as the feed has not been modified through governance proposals. If the oracle currently in use is not the SVR oracle (e.g. Aave oracle was changed through a proposal), the transaction will revert, preventing the Aave feed from being replaced with a potentially outdated feed.

4. The implementation allows replacing the effective oracle with the one stored in cache only if the feed activated is an SVR. A requirement has been implemented for this purpose.

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.