Security Assessment

Final Report

EclpLPOracle

September 2025

Prepared for Balancer

certora Balancer

Table of content

certora Balancer

Project Summary

Project Scope

Project Name	Repository (link)	Latest Commit Hash	Platform
Balancer	balancer-v3	64ed31e	EVM

Project Overview

This document describes the verification of **EclpLPOracle contract** using manual code review.
The work was undertaken from **September 9** to **September 10, 2025**.

The scope is limited to the EclpLPOracle contract, as defined in:

`/pkg/oracles/contracts/EclpLPOracle.sol`

Protocol Overview

EclpLPOracle is a manipulation-resistant TVL oracle tailored for Gyro's Elliptic Constant Liquidity Pools (ECLP). It combines external market prices with the pool's geometric parameters and invariant to value the pool's LP tokens in a way that's robust against internal price distortions. When prices are below, within, or above the configured range, it switches to the appropriate geometric formula to ensure accurate, conservative valuation.

Under the hood, it integrates Chainlink feeds and Balancer's vault data, carefully handling mixed-precision math (38- to 18-decimals) from ECLP's derived parameters and transformations. The result is a stable, precise TVL signal suitable for downstream uses like risk controls, redemptions, and protocol accounting.

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

The EclpLPOracle contract was reviewed in detail. Its implementation was compared against the mathematical specification provided in the E-CLP Mathematics paper.
The TVL calculation correctly:

- derives the current price ratio,
- handles cases where the price lies outside the active range (α, β), and
- for in-range values, computes the appropriate transformed boundary vectors and applies the scalar product with the price vector, scaled by the invariant.

Precision handling and rounding behavior were also examined and found to be consistent with the intended design, ensuring safe integer arithmetic without affecting correctness.

The logic and calculations are consistent with the documented E-CLP design, and no issues were identified.

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.