



Smart Contract Security Audit Report

GearBox Oracles Update

1. Contents

1.	Contents	2
2.	General Information	3
2.1.	Introduction	3
2.2.	Scope of Work	3
2.3.	Threat Model.....	3
2.4.	Weakness Scoring	4
2.5.	Disclaimer.....	4
3.	Summary.....	5
4.	General Recommendations	5
4.1.	Security Process Improvement	5
5.	Appendix.....	6
5.1.	About us	6

2. General Information

This report contains information about the results of the security audit of the GearBox (hereafter referred to as “Customer”) smart contracts, conducted by [Decurity](#) in the period from 2025-10-21 to 2025-10-22.

2.1. Introduction

Tasks solved during the work are:

- Review the protocol design and the usage of 3rd party dependencies,
- Audit the contracts implementation,
- Develop the recommendations and suggestions to improve the security of the contracts.

2.2. Scope of Work

The audit scope included the contracts in the following repository: [Gearbox-protocol/oracles-v3](#).
The review was done for the commit [64a386](#).

The following contracts have been tested:

- contracts/oracles/pendle/PendleTWAPPTPriceFeed.sol
- contracts/oracles/curve/CurveTWAPPriceFeed.sol

2.3. Threat Model

The assessment presumes actions of an intruder who might have capabilities of any role (an external user, token owner, token service owner, a contract). The centralization risks have not been considered upon the request of the Customer.

The main possible threat actors are:

- User,
- Protocol owner,
- Liquidity Token owner/contract.

2.4. Weakness Scoring

An expert evaluation scores the findings in this report, an impact of each vulnerability is calculated based on its ease of exploitation (based on the industry practice and our experience) and severity (for the considered threats).

2.5. Disclaimer

Due to the intrinsic nature of the software and vulnerabilities and the changing threat landscape, it cannot be generally guaranteed that a certain security property of a program holds.

Therefore, this report is provided “as is” and is not a guarantee that the analyzed system does not contain any other security weaknesses or vulnerabilities. Furthermore, this report is not an endorsement of the Customer’s project, nor is it an investment advice.

That being said, Decurity exercises best effort to perform their contractual obligations and follow the industry methodologies to discover as many weaknesses as possible and maximize the audit coverage using the limited resources.

3. Summary

As a result of this work, we have not discovered any security issues.

The team has given the explanation for the underlying code.

4. General Recommendations

This section contains general recommendations on how to improve overall security level.

The Findings section contains technical recommendations for each discovered issue.

4.1. Security Process Improvement

The following is a brief long-term action plan to mitigate further weaknesses and bring the product security to a higher level:

- Keep the whitepaper and documentation updated to make it consistent with the implementation and the intended use cases of the system,
- Perform regular audits for all the new contracts and updates,
- Ensure the secure off-chain storage and processing of the credentials (e.g. the privileged private keys),
- Launch a public bug bounty campaign for the contracts.

5. Appendix

5.1. About us

The [Decurity](#) team consists of experienced hackers who have been doing application security assessments and penetration testing for over a decade.

During the recent years, we've gained expertise in the blockchain field and have conducted numerous audits for both centralized and decentralized projects: exchanges, protocols, and blockchain nodes.

Our efforts have helped to protect hundreds of millions of dollars and make web3 a safer place.