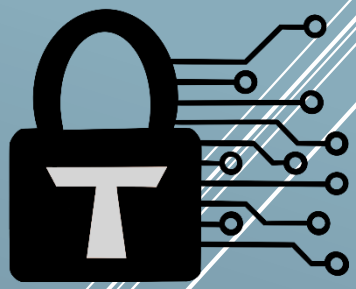
Trust Security



Smart Contract Audit

The Graph – PR #1242/#1243

17/11/2025

Executive summary

Properties:

Category	Indexing
Auditor	Trust

Findings:

Severity	Total	Fixed	Acknowledged
High	0	-	-
Medium	0	-	-
Low	0	-	-

Signature

Digitally signed by Trust
Date: 2025.11.17 16:02:35 +02'00'

Document properties

Versioning

Version	Date	Description
0.1	07/11/25	Client report
0.2	17/11/25	Updated scope

Contact

Trust

trust@trust-security.xyz

Introduction

Trust Security has conducted an audit at the customer's request. The audit is focused on uncovering security issues and additional bugs contained in the code defined in scope. Some additional recommendations have also been given when appropriate.

Scope

All changed non-interface files in the PRs are included in the scope.

For PR #1243/1255, the following assumptions are made:

- The **rewardsEligibilityOracle** shall not be set to a non-zero value.
- The **issuanceAllocator** shall not be set to a non-zero value.

Under such assumptions, in-scope are any functionality changes from the current implementation.

Repository details

- **Repository URL:** https://github.com/graphprotocol/contracts
- **PR #1242 commit hash:** d863720f3f03678a68a403f5c319a40a911b7a53
- **PR #1243 commit hash:** ec0c984132fe665f917a8ae149e19839d6a79b6f
- **PR #1255 commit hash (rebase)**: 8c08f3a63b4f0f766501b8dead917729fed5f82e

About Trust Security

Trust Security has been established by top-end blockchain security researcher Trust, in order to provide high quality auditing services. Since its inception it has safeguarded over 30 clients through private services and over 30 additional projects through bug bounty submissions.

About the Auditors

Trust has established a dominating presence in the smart contract security ecosystem since 2022. He is a resident on the Immunefi, Sherlock and C4 leaderboards and is now focused in auditing and managing audit teams under Trust Security. When taking time off auditing & bug hunting, he enjoys sharing knowledge and experience with aspiring auditors through X or the Trust Security blog.

Disclaimer

Smart contracts are an experimental technology with many known and unknown risks. Trust Security assumes no responsibility for any misbehavior, bugs or exploits affecting the audited code or any part of the deployment phase.

Furthermore, it is known to all parties that changes to the audited code, including fixes of issues highlighted in this report, may introduce new issues and require further auditing.

Methodology

In general, the primary methodology used is manual auditing. The entire in-scope code has been deeply looked at and considered from different adversarial perspectives. Any additional dependencies on external code have also been reviewed.

Qualitative analysis

Metric	Rating	Comments
Code complexity	**Excellent**	Project kept code as simple as possible, reducing attack risks
Documentation	**Excellent**	Project is very well documented.
Best practices	**Excellent**	Project consistently adheres to industry standards.
Centralization risks	**N/A**	No changes have been made to centralization aspects.

Findings

Recommendations

TRST-R-1 Consider setting key addresses in the initializer

The PR introduces the **rewardsEligibilityOracle** and **issueanceAllocator** state variables which control the issuance of rewards. As the code is mainly intended for an upgrade, it is not necessarily to set them immediately on the upgrade deployment. However, in case the RewardManager should ever be freshly deployed, it is logical to be able to set them among any other variables during construction, so that rewards can be accrued as designed from the first block post-deployment.

TRST-R-2 BaseUpgradeable limits the issuance of new roles

The BaseUpgradeable defines the GOVERNOR, PAUSER and OPERATOR roles, which are all controlled by the GOVERNOR. If deriving contracts would need to introduce new roles for operation, they would have to appoint a DEFAULT_ADMIN_ROLE during their own initialization. In case the above is intended, it is recommended to only document the behavior for any child contracts. Otherwise, consider receiving an optional address from parent contracts to set the DEFAULT_ADMIN_ROLE.