Royco Dawn

Competition

February 3, 2026

Contents

1 Introduction

1.1 About Cantina

Cantina is a security services marketplace that connects top security researchers and solutions with clients. Learn more at cantina.xyz

1.2 Disclaimer

A competition provides a broad evaluation of the security posture of the code at a particular moment based on the information available at the time of the review. While competitions endeavor to identify and disclose all potential security issues, they cannot guarantee that every vulnerability will be detected or that the code will be entirely secure against all possible attacks. The assessment is conducted based on the specific commit and version of the code provided. Any subsequent modifications to the code may introduce new vulnerabilities, therefore, any changes made to the code would require an additional security review. Please be advised that competitions are not a replacement for continuous security measures such as penetration testing, vulnerability scanning, and regular code reviews.

1.3 Risk assessment

Severity level	Impact: High	Impact: Medium	Impact: Low
Likelihood: high	Critical	High	Medium
Likelihood: medium	High	Medium	Low
Likelihood: low	Medium	Low	Low

1.3.1 Severity Classification

The severity of security issues found during the security review is categorized based on the above matrix. High severity findings represent the most critical issues that must be addressed immediately, as they either have high impact and high likelihood of occurrence, or medium impact with high likelihood.

Medium severity findings represent issues that, while not immediately critical, still pose significant risks and should be addressed promptly. These typically involve scenarios with medium impact and medium likelihood, or high impact with low likelihood.

Low severity findings represent issues that, while not posing immediate threats, could potentially cause problems in specific scenarios. These typically involve medium impact with low likelihood, or low impact with medium likelihood.

Lastly, some findings might represent improvements that don't directly impact security but could enhance the codebase's quality, readability, or efficiency (Gas and Informational findings).

2 Security Review Summary

From Jan 20th to Jan 27th Cantina hosted a competition based on Royco Dawn.

This competition was judged entirely by the Royco team; no external judge validated the findings presented in this report.

As defined by Royco, this competition considered only high-severity submissions, limited to:

- Funds sent to non-whitelisted addresses or to addresses not specified by whitelisted addresses.
- Funds permanently locked or unrecoverable.

There were no valid findings submitted that fulfilled the requirements stated above.

2.1 Scope

The security review had the following components in scope for Royco Dawn on commit hash d5f9360c:

```
src
├── accountant
│   └── RoycoAccountant.sol
├── auth
│   ├── RoycoAuth.sol
│   └── RoycoRoles.sol
├── base
│   └── RoycoBase.sol
├── interfaces
│   ├── external
│   │   ├── aave
│   │   │   ├── IPool.sol
│   │   │   ├── IPoolAddressesProvider.sol
│   │   │   └── IPoolDataProvider.sol
│   │   ├── chainlink
│   │   │   └── AggregatorV3Interface.sol
│   │   └── reUSD
│   │       └── IInsuranceCapitalLayer.sol
│   ├── IRoycoAccountant.sol
│   ├── IRoycoAuth.sol
│   ├── IRoycoFactory.sol
│   ├── IYDM.sol
│   ├── kernel
│   │   ├── IAsyncJTDepositKernel.sol
│   │   ├── IAsyncSTDepositKernel.sol
│   │   ├── IAsyncSTRedemptionKernel.sol
│   │   └── IRoycoKernel.sol
│   └── tranche
│       ├── IRoycoAsyncCancellableVault.sol
│       ├── IRoycoAsyncVault.sol
│       └── IRoycoVaultTranche.sol
├── kernels
│   ├── base
│   │   ├── junior
│   │   │   ├── AaveV3_JT_Kernel.sol
│   │   │   ├── ERC4626_JT_Kernel.sol
│   │   │   └── YieldBearingERC20_JT_Kernel.sol
│   │   ├── quoter
│   │   │   ├── base
│   │   │   │   ├── IdenticalAssetsAdminOracleQuoter.sol
│   │   │   │   ├── IdenticalAssetsChainlinkOracleQuoter.sol
│   │   │   │   ├── IdenticalAssetsOracleQuoter.sol
│   │   │   │   └── IdenticalERC4626SharesOracleQuoter.sol
```

```
│   │   │   ├── IdenticalAssetsChainlinkToAdminOracleQuoter.sol
│   │   │   ├── IdenticalERC4626SharesAdminOracleQuoter.sol
│   │   │   └── InKindAssetsQuoter.sol
│   │   ├── recipe
│   │   │   ├── ERC4626_ST_ERC4626_JT_Kernel.sol
│   │   │   └──
↪  YieldBearingERC20_ST_YieldBearingERC20_JT_IdenticalAssetsOracleQuoter_Kernel.sol
│   │   ├── RoycoKernel.sol
│   │   └── senior
│   │       ├── ERC4626_ST_Kernel.sol
│   │       └── YieldBearingERC20_ST_Kernel.sol
│   ├── ERC4626_ST_AaveV3_JT_InKindAssets_Kernel.sol
│   ├── ERC4626_ST_ERC4626_JT_InKindAssets_Kernel.sol
│   ├── ReUSD_ST_ReUSD_JT_Kernel.sol
│   ├── YieldBearingERC20_ST_YieldBearingERC20_JT_IdenticalAssetsChainlinkToAdminOracleQ┘
↪  uoter_Kernel.sol
│   └── YieldBearingERC4626_ST_YieldBearingERC4626_JT_IdenticalERC4626SharesAdminOracleQ┘
↪  uoter_Kernel.sol
├── libraries
│   ├── Constants.sol
│   ├── kernels
│   │   ├── ERC4626KernelStorageLib.sol
│   │   └── YieldBearingERC20KernelStorageLib.sol
│   ├── RoycoKernelStorageLib.sol
│   ├── RoycoTrancheStorageLib.sol
│   ├── Types.sol
│   ├── Units.sol
│   └── UtilsLib.sol
├── RoycoFactory.sol
├── tranches
│   ├── base
│   │   └── RoycoVaultTranche.sol
│   ├── RoycoJuniorTranche.sol
│   └── RoycoSeniorTranche.sol
└── ydm
    ├── AdaptiveCurveYDM.sol
    └── StaticCurveYDM.sol
```