hexens x ROYCO

Whitelist Review Report for Royco

January 2026

Table of Contents

1. About Hexens

Hexens is a pioneering cybersecurity firm dedicated to establishing robust security standards for Web3 infrastructure, driving secure mass adoption through innovative protection technology and frameworks. As an industry elite experts in blockchain security, we deliver comprehensive audit solutions across specialized domains, including infrastructure security, Zero Knowledge Proof, novel cryptography, DeFi protocols, and NFTs.

Our methodology combines industry-standard security practices combined with unique methodology of two teams per audit, continuously advancing the field of Web3 security. This innovative approach has earned us recognition from industry leaders.

Since our founding in 2021, we have built an exceptional portfolio of enterprise clients, including major blockchain ecosystems and Web3 platforms.

2. Executive Summary

This report covers a supplementary whitelist review of the Royco Dawn protocol. During this review, we analyzed the code and looked for any cases where monetary assets would go through any non-whitelisted addresses.

From our review, we found that:

- Every user-facing function has been restricted using a whitelist approach that can only be managed by Royco;
- Every admin-facing function has been gated by access control and is only accessible by Royco;
- Assets are deployed into 3rd party protocols that were explicitly set by Royco during Tranche creation, which we find to be equal to manual whitelisting.

By specifically reviewing the flow of assets, we found that:

- Assets only flow from whitelisted depositors directly to whitelisted protocols and vice versa.
- Protocol fees on assets are only sent to the specific fee recipient of Royco.

Our review did not identify any issues in the whitelisting approach of Royco Dawn protocol.

3. Security Review Details

- **Review Led by**

Kasper Zwijsen, Head of Audits

- **Scope**

The analyzed resources are located on:

🔗 https://github.com/roycoprotocol/royco-dawn/tree/9eb345e56b01467b9b114035f574381de75341ca

- **Changelog**

26th January 2026	Review start
30th January 2026	Final report

4. Severity Structure

The vulnerability severity is calculated based on two components:

1. Impact of the vulnerability
2. Probability of the vulnerability

Impact	Probability			
	Rare	Unlikely	Likely	Very likely
Low	Low	Low	Medium	Medium
Medium	Low	Medium	Medium	High
High	Medium	Medium	High	Critical
Critical	Medium	High	Critical	Critical

- **Severity Characteristics**

Smart contract vulnerabilities can range in severity and impact, and it's important to understand their level of severity in order to prioritize their resolution. Here are the different types of severity levels of smart contract vulnerabilities:

Critical

Vulnerabilities that are highly likely to be exploited and can lead to catastrophic outcomes, such as total loss of protocol funds, unauthorized governance control, or permanent disruption of contract functionality.

High

Vulnerabilities that are likely to be exploited and can cause significant financial losses or severe operational disruptions, such as partial fund theft or temporary asset freezing.

Medium

Vulnerabilities that may be exploited under specific conditions and result in moderate harm, such as operational disruptions or limited financial impact without direct profit to the attacker.

Low

Vulnerabilities with low exploitation likelihood or minimal impact, affecting usability or efficiency but posing no significant security risk.

Informational

Issues that do not pose an immediate security risk but are relevant to best practices, code quality, or potential optimizations.

Issue Symbolic Codes

Each identified and validated issue is assigned a unique symbolic code during the security research stage.

Due to the structure of the vulnerability reporting flow, some rejected issues may be missing.

5. Findings Summary

Severity	Number of findings
🟥 Critical	0
🟥 High	0
🟧 Medium	0
🟩 Low	0
🟦 Informational	0
Total:	**0**

6. Weaknesses

During a supplementary whitelist review, our auditing team didn’t identify any issues.

hexens x ROYCO