Monarch Lend

Smart Contract Security Assessment and Code Review

Jan 15th, 2025

By Shao-Ku Tien, Independent Researcher

Summary

Monarch Lend (monarchlend.xyz) is an easy-to-use interface for users to supply assets directly to markets on Morpho Protocol. It offers an efficient alternative for those confident in managing their own positions, allowing them to avoid intermediary vault management fees.

Monarch Lend engaged me for an audit of their smart contracts written in Solidity. The codebase was audited for 1 week, from Jan 2nd to Jan 6th, 2025. The scope of the audit was:

- `MonarchAgent.sol`, at commit 613f417
- `IMonarchAgent.sol` and `ErrorsLib.sol`, at commit e637ae8

Features of the above scope include:

- User authorisation for a specific address to become their "rebalancer" who can manage positions on their behalf.
- Rebalancer moving assets between different Morpho markets while respecting user-set caps.
- User setting, removing and updating authorisation.

The below is a list of issues found ranging from critical to informational:

Severity	Number of Findings
Critical	0
High	0
Medium	0
Low	0
Informational	2

Findings

Unable to call rebalance

Type: Informational
Files Affected: `MonarchAgent.sol`

On line 134 in `_approveMaxTo()`, the ERC20 allowance is strictly checked against `0`. In extreme but unlikely situations, if the allowance drops below the amount to be transferred later in `_supplyAndCheckCap()`, `rebalance()` will no longer succeed. Since this contract is not upgradeable, the issue cannot be resolved once it occurs.

Impact: The `rebalance()` will fail to execute in extreme but unlikely situations.
Suggestion: Add a second value check against the amount to be transferred in the `if` condition on line 134 to ensure sufficient allowance.

Naming Inconsistency

Type: Informational
Files Affected: `MonarchAgent.sol`

The mapping storage `rebalancers` is not an array, and a user can only have one rebalancer at a time. Therefore, it should be renamed to the singular `rebalancer` to align with the convention used for another mapping storage, `marketCap`.

Impact: This is only a naming suggestion and does not affect security.
Suggestion: Rename `rebalancers` to `rebalancer` to improve naming consistency.