YO Protocol
Security Audit

Report Version 0.1

October 23, 2025

Conducted by **Aether Labs**

Table of Contents

1 About Aether Labs

Aether Labs is an industry-leading smart contract security company. Having conducted over 100+ security assessments protecting over $3B in TVL, we deliver high-signal security reviews to emerging and established DeFi protocols.

2 Disclaimer

Audits are a time-, resource-, and expertise-bound effort where trained experts evaluate smart contracts using a combination of automated and manual techniques to identify as many vulnerabilities as possible. Audits can reveal the presence of vulnerabilities, but cannot guarantee their absence.

3 Risk classification

Severity	Impact: High	Impact: Medium	Impact: Low
Likelihood: High	High	High	Medium
Likelihood: Medium	High	Medium	Low
Likelihood: Low	Medium	Low	Low

3.1 Impact

- **High** - leads to a significant loss of assets in the protocol or significantly harms a group of users.
- **Medium** - involves a small loss of funds or affects a core functionality of the protocol.
- **Low** - encompasses any unexpected behavior that is non-critical.

3.2 Likelihood

- **High** - a direct attack vector; the cost is relatively low compared to the potential loss of funds.
- **Medium** - only a conditionally incentivized attack vector, with a moderate likelihood.
- **Low** - involves too many or unlikely assumptions; offers little to no incentive.

3.3 Actions required by severity level

- **High** - client **must** fix the issue.
- **Medium** - client **should** fix the issue.
- **Low** - client **could** fix the issue.

4 Executive summary

Overview

Project Name	YO Protocol
Repository	https://github.com/yoprotocol/core
Commit hash	4552188eef57a7f5ed30967b9feb9e20cfd11d03
Resolution	666c456585658ac957c565d14dcf0a1ac42ae6e8
Methods	Manual review & testing

Scope

src/YoSecondaryVault.sol

Issues Found

High risk	0
Medium risk	0
Low risk	0
Informational	6

5 Findings

5.1 Informational

5.1.1 Non-critical issues and suggestions

Severity: Informational

Description: The contracts contain one or more non-critical issues. In an effort to keep the report size reasonable, we enumerate these below:

1. No need to call _disableInitializers in constructor as it is already part of the parent contract's constructor.
2. decimals() could be inlined in _convertToShares and _convertToAssets.
3. Anyone can call initializeV2 eventually frontrunning the call upon deployment.
4. Unused imports and libraries: Address, IERC20, SafeERC20.
5. Consider overriding and reverting in onUnderlyingBalanceUpdate to reduce attack surface.
6. totalAssets() will return only the available vault assets which could be midleading to external readers.

Recommendation: Consider fixing the above non-critical issues and suggestions.

Resolution: Resolved 1-5.