OPTIMUM
BLOCKCHAIN SECURITY

Yearn Finance

Smart contract
Security Assessment

Angle Protocol Strategy

July, 2022

Table Of Contents

Disclaimer

This report does not provide any security warranty, investment advice, endorsement, or disapproval of any particular project or team. This report does not provide a warranty that the code in scope is completely free of vulnerabilities, bugs, or potential exploits. This report does not assess the financial risk of any asset. No third party should rely on this report to make any decisions to buy or sell any asset or product.

Delivering secured code is a continuous challenge that requires multiple steps. It is strongly recommended to use best code practices, write a full test suite, conduct an internal audit, and launch a bug bounty program as a complement to this report.

It is the sole responsibility of the project team to ensure that the code in scope is functioning as intended and that the recommendations presented in this report are carefully tested before deployment.

Overview Page

Summary

Project name	Yearn Finance
URL	https://yearn.finance/
Code	https://github.com/Mattdwest/angle_protocol
Commit hash	60d2051420c2e9743b8d67c62570529d991d1a98
Mitigations commit hash	
Language	Solidity

Contracts Assessed

Contract name	SHA-1
/contracts/Strategy.sol	8d0f8e1a5376c739a5365241c0ee59cc32f4140f

Findings Summary

Severity	Found	Resolved	Partially resolved	Acknowledged
High	0	0	0	0
Medium	0	0	0	0
Low	1	0	0	0
Informational	0	0	0	0
Total	1	0	0	0

Classification of issues

Severity	
High	Vulnerabilities that may directly result in loss of funds, and thus require an urgent fix.
Medium	Issues that may not be directly exploitable, or with a limited impact, are still required to be fixed.
Low	Subjective issues with a negligible impact.
Informational	Subjective issues or observations with negligible or no impact.

Findings

Issue #01	**ERC20 approvals of type(uint256).max**
Severity	**Low**
Location	*Strategy.sol* - Lines 89-90
Description	Approving the maximum value of uint256 is a known practice to save gas. However, this pattern was proven to increase the impact of an attack many times in the past, in case the approved contract gets hacked.
Recommendation	Consider approving the exact amount that's needed to be transferred, or alternatively, add an external function that allows the revocation of approvals.
Resolution	

Trust Assumptions

Angle Protocol smart contracts	
Description	*Angle Protocol* contracts are trusted in many ways, including but not only: • Deposits and withdrawals can be paused.


OPTIMUM
BLOCKCHAIN SECURITY