Pendle AVAX Integrations Security Audit

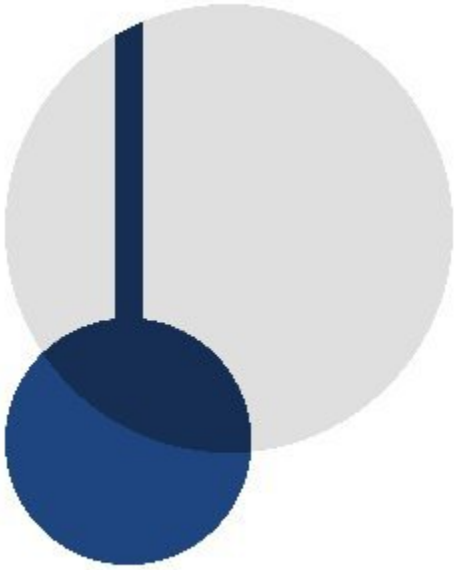

Table of Contents

Scope

The scope of the audit is limited to https://github.com/pendle-finance/contracts/, for changes in 011548854721880225187 45f2ca08104955b8b2b.

The following files were reviewed, related to the AVAX integrations include:
Private repo commit: c1c5d81b0afc0b885112a6669b66cb6e4b922126
LiquidityMiningBaseV1
LiquidityMiningBaseV1Multi
ForgeBaseV2
YieldTokenHolderBaseV2Multi
LiquidityMiningBaseV2Multi
PendleBenQiForge
PendleBenYieldContractDeployer
PendleBenQiYieldTokenHolder
GenericLiquidityMiningMulti
JoeLpLiquidityMining
TraderJoeForge
TraderJoeYieldContractDeployer
TraderJoeYieldTokenHolder
RewardManagerMulti
PendleSimpleERC20TokenHolder

Private repo commit: 5c6300b10909c0dbf1560651b7cbc4e1394fa6df
PendleWonderlandForge.sol

Summary of Findings

In performing a security audit of Pendle AVAX Integration, several issues of concern were found. For each finding, a summary of the issue is documented, along with any other finer details regarding the issue. Security recommendations are also provided where applicable.

The table below shows a breakdown of security findings found categorized by severity or risk and impact. A finding that has been reported is listed as pending, and if that finding is satisfactorily mitigated, it will be categorized as resolved.

Severity	**Resolved**	**Unresolved**	**Total**
Critical	0	0	0
High	0	0	0
Medium	1	0	1
Low	2	1	3
Info	2	0	2

Issues

PEN-001: Wrong usage of msg.sender instead of to address for userExpiries in _stake

Severity: Medium
Status: Resolved
The _stake function allows a specification of the address to stake for, but when updating the userExpiries mapping, it uses msg.sender instead of the address that is being staked for. This can result in the expiry information for the to address not being updated, and thus, the to address will not be able to call redeemRewards and redeemLpInterests.

Recommendations
Use the to address instead of msg.sender when checking for and updating userExpiries.

Resolution
The to address is now correctly used.

Note
Discovered during testing by the Pendle team.

PEN-002: Possible for duplicate tokens to be in newPairTokens and newTrioTokens

Severity: Low
Status: Resolved
If duplicate tokens are passed as parameters for newPairTokens or newTrioTokens, they will be accepted as there is currently no check to ensure that there are no duplicates.

Recommendations
Add checks to ensure that none of the tokens are duplicates.

Resolution
Duplication checks have been added.

PEN-003: migrateMasterChef does not set allowance of old Masterchef to zero

Severity: Low
Status: Resolved
During migration of the MasterChef, the old Masterchef still retains its old granted allowance from the Yield Token Holder contract.

Recommendations
Approve the allowance to zero for the old Masterchef.

Resolution
The old Masterchef's allowance will be approved to zero.

PEN-004: Lack of events for migrateMasterChef in forge

Severity: Info
Status: Resolved
migrateMasterChef is a sensitive state change that changes the Masterchef contract address. However, there is no event emitted.

Recommendations
Emit an event in the forge's migrateMasterChef function.

Resolution
The recommended event emission was added.

PEN-005: Funds can be deposited back into the Masterchef after setUpEmergencyModeV2 has been called

Severity: Low
Status: Acknowledged
As the Masterchef will still have token allowance after setUpEmergencyModeV2, anyone can call afterReceiveTokens to force a deposit back into the Masterchef.

Recommendations
The allowance approved to the Masterchef can be set to zero in setUpEmergencyModeV2 to prevent forced depositing back into the Masterchef.

Resolution
The issue has been acknowledged by the Pendle team, but no change has been made yet as there has been no situation where setUpEmergencyModeV2 has been required to be called. In the case it should be called, this issue will be handled by the EmergencyHandler by immediately making the token withdrawals in the same transaction as setUpEmergencyModeV2 is called in.

PEN-006: MEMO address can be obtained from wMEMO instead of constructor parameter

Severity: Info
Status: Resolved

In PendleWonderlandForge's constructor, the MEMO address is passed as a parameter into the constructor. The error of setting a MEMO address that does not tally to the MEMO address of wMEMO can be avoided by obtaining the MEMO address directly from the wMEMO contract.

Recommendations
The MEMO address in the parameter can be removed, and obtained by the following:
MEMO = IERC20(_wMEMO.MEMO());

Resolution
The recommended change in the constructor has been made.