



Protocol Audit Report

Version 1.0

Vesko.io

December 5, 2024

2024-11-CONCRETE

Vesko.io

November 23, 2024

Issues Found

Severity	Number of Issues Found
Gas	1
Non Critical	1
Informational	1
Total	3

Gas

[G-1] Perform validations early to avoid unnecessary writes or external calls

Description: In `/src/registries/VaultRegistry.sol` in the `addVault` function, a check can be performed before making external calls and working with state variables.

Recommended Mitigation:

```
1 function addVault(address vault_, bytes32 vaultId_) external override
  onlyOwner {
2     if (vault_ == address(0)) revert VaultZeroAddress();
3
4     if (vaultExists[vault_]) {
5         revert VaultAlreadyExists();
6     }
```

```
7
8   + if (allVaultsCreated.length == totalVaultsAllowed) revert
    TotalVaultsAllowedExceeded(allVaultsCreated.length);
9
10  vaultExists[vault_] = true;
11  vaultIdToArray[vaultId_].push(vault_);
12  allVaultsCreated.push(vault_);
13
14  - if (allVaultsCreated.length > totalVaultsAllowed) revert
    TotalVaultsAllowedExceeded(allVaultsCreated.length);
15
16  address underlyingAsset = IERC4626(vault_).asset();
17
18  assert(vaultsByToken[underlyingAsset].add(vault_));
19
20  if (vaultsByToken[underlyingAsset].length() > vaultByTokenLimit) {
21      revert VaultByTokenLimitExceeded(underlyingAsset, vaultsByToken
    [underlyingAsset].length());
22  }
23  emit VaultAdded(vault_, vaultId_);
24 }
```

Non Critical Issues

[NC-1] In ImplementationRegistry the comments suggest that the `getHistoricalImplementationAddresses` function gets all the implementations ever added but that is not the case because `removeImplementation` deletes implementations from a state variable (`allImplementations`) that is returned in `getHistoricalImplementationAddresses`

Code Snippets:

```
1 // removeImplementation function:
2 allImplementations.pop();
3
4 // getHistoricalImplementationAddresses function:
5 return allImplementations;
```

Informational

[I-1] Typo in Errors

- “InvalidSubstraction” should be “InvalidSubtraction”

```
1 error InvalidSubstraction();
```

- “Withdrawl” is a typo; it should be “Withdrawal.”

```
1 error InvalidWithdrawlQueue();  
2 error UnfinalizedWithdrawl(address queue);
```

- “Rewardrate” is not camel-cased properly. It should be “RewardRate.”

```
1 error SwapperBaseRewardrate();  
2 error SwapperBonusRewardrateUser();  
3 error SwapperBonusRewardrateCtToken();  
4 error SwapperBonusRewardrateSwapToken();
```