Summary

missing-zero-check

Impact: Low

Confidence: Medium

☐ ID-0

AccessControl.constructor(address,address)._admin lacks a zero-check on :
- admin = _admin

contracts/AccessControl.sol#L23

☐ ID-1

AccessControl.constructor(address,address)._keeper lacks a zero-check on :
- keeper = _keeper

contracts/AccessControl.sol#L23

calls-loop

Impact: Low

Confidence: Medium

☐ ID-2

Uniswap.swapExactInputSingle(uint256,address,address,address) has external calls inside a loop: amountOut = swapRouter.exactInputSingle(params)

contracts/Uniswap.sol#L24-L44

☐ ID-3

PriceConsumerV3.getLatestPrice(AggregatorV3Interface) has external calls inside a loop: (price) = _feed.latestRoundData()

contracts/PriceConsumerV3.sol#L45-L50

☐ ID-4

TransferHelper.safeApprove(address,address,uint256) has external calls inside a loop: (success,data) = token.call(abi.encodeWithSelector(IERC20.approve.selector,to,value))

node_modules/@uniswap/v3-periphery/contracts/libraries/TransferHelper.sol#L43-L50

reentrancy-benign

Impact: Low
Confidence: Medium

☐ ID-5

Reentrancy in PortfolioManager.addOrder(address,PortfolioManager.OrderType,int256,uint256):
External calls:
- (success,data) = assetToCharge.call(abi.encodeWithSelector(0x23b872dd,msg.sender,address(this),_amount))
  State variables written after the call(s):
- orders.push(Order(_asset,_orderType,_price,_amount,msg.sender))

contracts/PortfolioManager.sol#L60-L107

reentrancy-events

Impact: Low
Confidence: Medium

☐ ID-6

Reentrancy in PortfolioManager.addOrder(address,PortfolioManager.OrderType,int256,uint256):
External calls:
- (success,data) = assetToCharge.call(abi.encodeWithSelector(0x23b872dd,msg.sender,address(this),_amount))

)

Event emitted after the call(s):

- OrderAdded(_asset,_price)

contracts/PortfolioManager.sol#L60-L107

pragma

Impact: Informational
Confidence: High

- [ ] ID-7
  Different versions of Solidity are used:
  - Version used: ['0.8.16', '>=0.5.0', '>=0.6.0', '>=0.7.5', '^0.8.0']
  - ^0.8.0
  - ^0.8.0
  - >=0.5.0
  - >=0.7.5
  - v2
  - >=0.6.0
  - 0.8.16
  - [0.8.16](contracts/IWETH .sol#L2)
  - 0.8.16
  - 0.8.16
  - 0.8.16
  - 0.8.16
  - v2

node_modules/@chainlink/contracts/src/v0.8/interfaces/AggregatorV3Interface.sol#L2

solc-version

Impact: Informational
Confidence: High

- [ ] ID-8
  solc-0.8.16 is not recommended for deployment
- [ ] ID-9
  Pragma version0.8.16 necessitates a version too recent to be trusted. Consider deploying with

0.6.12/0.7.6/0.8.7

contracts/Uniswap.sol#L2

- [ ] ID-10

    Pragma version^0.8.0 allows old versions

node_modules/@chainlink/contracts/src/v0.8/interfaces/AggregatorV3Interface.sol#L2

- [ ] ID-11

    Pragma version0.8.16 necessitates a version too recent to be trusted. Consider deploying with 0.6.12/0.7.6/0.8.7

contracts/PortfolioManager.sol#L2

- [ ] ID-12

    Pragma version^0.8.0 allows old versions

node_modules/@openzeppelin/contracts/token/ERC20/IERC20.sol#L4

- [ ] ID-13

    Pragma version>=0.6.0 allows old versions

node_modules/@uniswap/v3-periphery/contracts/libraries/TransferHelper.sol#L2

- [ ] ID-14

    Pragma version>=0.5.0 allows old versions

node_modules/@uniswap/v3-core/contracts/interfaces/callback/IUniswapV3SwapCallback.sol#L2

- [ ] ID-15

    Pragma version0.8.16 necessitates a version too recent to be trusted. Consider deploying with 0.6.12/0.7.6/0.8.7

contracts/PriceConsumerV3.sol#L2

- [ ] ID-16

    Pragma version0.8.16 necessitates a version too recent to be trusted. Consider deploying with 0.6.12/0.7.6/0.8.7

contracts/Objects.sol#L2

- [ ] ID-17

    Pragma version0.8.16 necessitates a version too recent to be trusted. Consider deploying with

0.6.12/0.7.6/0.8.7

contracts/AccessControl.sol#L2

☐ ID-18

Pragma version[0.8.16](contracts/IWETH .sol#L2) necessitates a version too recent to be trusted. Consider deploying with 0.6.12/0.7.6/0.8.7

contracts/IWETH .sol#L2

low-level-calls

Impact: Informational
Confidence: High

☐ ID-19

Low level call in TransferHelper.safeTransferETH(address,uint256):
- (success) = to.call{value: value}(new bytes(0))

node_modules/@uniswap/v3-periphery/contracts/libraries/TransferHelper.sol#L56-L59

☐ ID-20

Low level call in PortfolioManager.addOrder(address,PortfolioManager.OrderType,int256,uint256):
- (success,data) = assetToCharge.call(abi.encodeWithSelector(0x23b872dd,msg.sender,address(this),_amount))

contracts/PortfolioManager.sol#L60-L107

☐ ID-21

Low level call in TransferHelper.safeApprove(address,address,uint256):
- (success,data) = token.call(abi.encodeWithSelector(IERC20.approve.selector,to,value))

node_modules/@uniswap/v3-periphery/contracts/libraries/TransferHelper.sol#L43-L50

☐ ID-22

Low level call in TransferHelper.safeTransferFrom(address,address,address,uint256):
- (success,data) = token.call(abi.encodeWithSelector(IERC20.transferFrom.selector,from,to,value))

node_modules/@uniswap/v3-periphery/contracts/libraries/TransferHelper.sol#L13-L22

- ☐ ID-23

  Low level call in TransferHelper.safeTransfer(address,address,uint256):
  - (success,data) = token.call(abi.encodeWithSelector(IERC20.transfer.selector,to,value))

node_modules/@uniswap/v3-periphery/contracts/libraries/TransferHelper.sol#L29-L36

naming-convention

Impact: Informational

Confidence: High

- ☐ ID-24

  Parameter PortfolioManager.executeOrders(uint256[])._orders is not in mixedCase

contracts/PortfolioManager.sol#L168

- ☐ ID-25

  Parameter
  PortfolioManager.addOrder(address,PortfolioManager.OrderType,int256,uint256)._asset is not in
  mixedCase

contracts/PortfolioManager.sol#L61

- ☐ ID-26

  Parameter
  PortfolioManager.addOrder(address,PortfolioManager.OrderType,int256,uint256)._orderType is
  not in mixedCase

contracts/PortfolioManager.sol#L62

- ☐ ID-27

  Parameter
  PortfolioManager.addOrder(address,PortfolioManager.OrderType,int256,uint256)._amount is not
  in mixedCase

contracts/PortfolioManager.sol#L64

- ☐ ID-28

  Parameter PriceConsumerV3.getLatestPrice(AggregatorV3Interface)._feed is not in mixedCase

contracts/PriceConsumerV3.sol#L46

- [ ] ID-29

  Parameter
  PortfolioManager.addOrder(address,PortfolioManager.OrderType,int256,uint256)._price is not in
  mixedCase

contracts/PortfolioManager.sol#L63

similar-names

Impact: Informational
Confidence: Medium

- [ ] ID-30

  Variable IUniswapV3SwapCallback.uniswapV3SwapCallback(int256,int256,bytes).amount0Delta
  is too similar to
  IUniswapV3SwapCallback.uniswapV3SwapCallback(int256,int256,bytes).amount1Delta

node_modules/@uniswap/v3-core/contracts/interfaces/callback/IUniswapV3SwapCallback.sol#L17