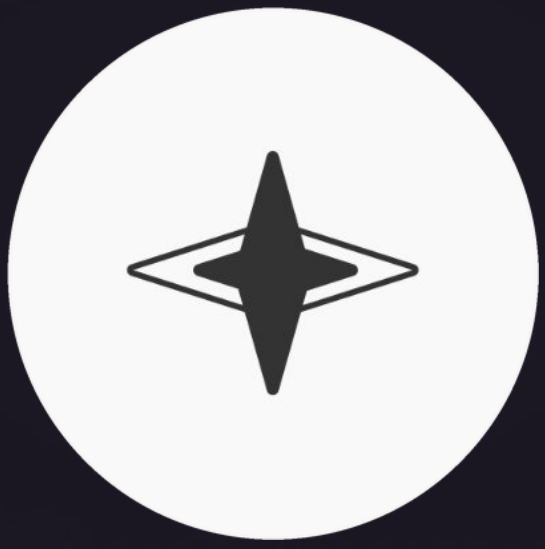
SHERLOCK

Security Review For Vyro Finance



Collaborative Audit Prepared For: **Vyro Finance**
Lead Security Expert(s): **KupiaSec**
Date Audited: **March 12 - March 13, 2026**

Introduction

Vyro CDP is a non-custodial borrowing protocol on Unichain that mints vyUSD, an over-collateralized stablecoin backed by ETH, wstETH, and UNI. Borrowers select their own interest rate band based on their risk tolerance, producing market-driven borrowing costs.

Scope

Repository: summerstonexyz/vyro

Audited Commit: 596e7cb764602da6539ff75d66d65bc090919a45

Files:

- contracts/src/ActivePool.sol
- contracts/src/AddressesRegistry.sol
- contracts/src/BoldToken.sol
- contracts/src/BorrowerOperationsAdjustFacet.sol
- contracts/src/BorrowerOperations.sol
- contracts/src/CollateralRegistry.sol
- contracts/src/CollSurplusPool.sol
- contracts/src/DebtInFrontHelper.sol
- contracts/src/DefaultPool.sol
- contracts/src/Dependencies/AddRemoveManagers.sol
- contracts/src/Dependencies/AggregatorV3Interface.sol
- contracts/src/Dependencies/Constants.sol
- contracts/src/Dependencies/LiquityBase.sol
- contracts/src/Dependencies/LiquityMath.sol
- contracts/src/GasPool.sol
- contracts/src/Governance/TimelockedMultiSigGovernor.sol
- contracts/src/Helpers/AdjustHelper.sol
- contracts/src/Helpers/TroveAdjustLib.sol
- contracts/src/HintHelpers.sol
- contracts/src/Interfaces/IActivePool.sol
- contracts/src/Interfaces/IAddRemoveManagers.sol
- contracts/src/Interfaces/IAddressesRegistry.sol

- contracts/src/Interfaces/IBoldRewardsReceiver.sol
- contracts/src/Interfaces/IBoldToken.sol
- contracts/src/Interfaces/IBorrowerOperationsAdjustFacet.sol
- contracts/src/Interfaces/IBorrowerOperations.sol
- contracts/src/Interfaces/ICollateralRegistry.sol
- contracts/src/Interfaces/ICollSurplusPool.sol
- contracts/src/Interfaces/ICommunityIssuance.sol
- contracts/src/Interfaces/IDebtInFrontHelper.sol
- contracts/src/Interfaces/IDefaultPool.sol
- contracts/src/Interfaces/IHintHelpers.sol
- contracts/src/Interfaces/IInterestRouter.sol
- contracts/src/Interfaces/ILiquityBase.sol
- contracts/src/Interfaces/ILQTYStaking.sol
- contracts/src/Interfaces/ILQTYToken.sol
- contracts/src/Interfaces/IMainnetPriceFeed.sol
- contracts/src/Interfaces/IMultiTroveGetter.sol
- contracts/src/Interfaces/IPriceFeed.sol
- contracts/src/Interfaces/IRedemptionHelper.sol
- contracts/src/Interfaces/ISortedTroves.sol
- contracts/src/Interfaces/IStabilityPoolEvents.sol
- contracts/src/Interfaces/IStabilityPool.sol
- contracts/src/Interfaces/ITroveEvents.sol
- contracts/src/Interfaces/ITroveManager.sol
- contracts/src/Interfaces/ITroveNFT.sol
- contracts/src/Interfaces/IUNIPriceFeed.sol
- contracts/src/Interfaces/IWETH.sol
- contracts/src/Interfaces/IWSTETHPriceFeed.sol
- contracts/src/Interfaces/IWSTETH.sol
- contracts/src/MultiTroveGetter.sol
- contracts/src/NFTMetadata/MetadataNFT.sol
- contracts/src/NFTMetadata/utils/baseSVG.sol

- contracts/src/NFTMetadata/utils/bauhaus.sol
- contracts/src/NFTMetadata/utils/FixedAssets.sol
- contracts/src/NFTMetadata/utils/JSON.sol
- contracts/src/NFTMetadata/utils/SVG.sol
- contracts/src/NFTMetadata/utils/Utils.sol
- contracts/src/PriceFeeds/CompositePriceFeed.sol
- contracts/src/PriceFeeds/MainnetPriceFeedBase.sol
- contracts/src/PriceFeeds/UNIPriceFeed.sol
- contracts/src/PriceFeeds/WETHPriceFeed.sol
- contracts/src/PriceFeeds/WSTETHPriceFeed.sol
- contracts/src/RedemptionHelper.sol
- contracts/src/SortedTroves.sol
- contracts/src/StabilityPool.sol
- contracts/src/TroveManager.sol
- contracts/src/TroveNFT.sol
- contracts/src/Types/BatchId.sol
- contracts/src/Types/LatestBatchData.sol
- contracts/src/Types/LatestTroveData.sol
- contracts/src/Types/TroveChange.sol
- contracts/src/Types/TroveId.sol
- contracts/src/Zappers/BaseZapper.sol
- contracts/src/Zappers/GasCompZapper.sol
- contracts/src/Zappers/Interfaces/IExchangeHelpers.sol
- contracts/src/Zappers/Interfaces/IExchangeHelpersV2.sol
- contracts/src/Zappers/Interfaces/IExchange.sol
- contracts/src/Zappers/Interfaces/IFlashLoanProvider.sol
- contracts/src/Zappers/Interfaces/IFlashLoanReceiver.sol
- contracts/src/Zappers/Interfaces/ILeverageZapper.sol
- contracts/src/Zappers/Interfaces/IZapper.sol
- contracts/src/Zappers/LeftoversSweep.sol
- contracts/src/Zappers/LeverageLSTZapper.sol

- contracts/src/Zappers/LeverageWETHZapper.sol
- contracts/src/Zappers/Modules/Exchanges/CurveExchange.sol
- contracts/src/Zappers/Modules/Exchanges/Curve/ICurveFactory.sol
- contracts/src/Zappers/Modules/Exchanges/Curve/ICurvePool.sol
- contracts/src/Zappers/Modules/Exchanges/Curve/ICurveStableswapNGFactory.sol
- contracts/src/Zappers/Modules/Exchanges/Curve/ICurveStableswapNGPool.sol
- contracts/src/Zappers/Modules/Exchanges/HybridCurveUniV3ExchangeHelpers.sol
- contracts/src/Zappers/Modules/Exchanges/HybridCurveUniV3ExchangeHelpersV2.sol
- contracts/src/Zappers/Modules/Exchanges/HybridCurveUniV3Exchange.sol
- contracts/src/Zappers/Modules/Exchanges/UniswapV3/INonfungiblePositionManager.sol
- contracts/src/Zappers/Modules/Exchanges/UniswapV3/IPoolInitializer.sol
- contracts/src/Zappers/Modules/Exchanges/UniswapV3/IQuoterV2.sol
- contracts/src/Zappers/Modules/Exchanges/UniswapV3/ISwapRouter.sol
- contracts/src/Zappers/Modules/Exchanges/UniswapV3/IUniswapV3Factory.sol
- contracts/src/Zappers/Modules/Exchanges/UniswapV3/IUniswapV3Pool.sol
- contracts/src/Zappers/Modules/Exchanges/UniswapV3/UniPriceConverter.sol
- contracts/src/Zappers/Modules/Exchanges/UniV3Exchange.sol
- contracts/src/Zappers/Modules/Exchanges/UniV4Exchange.sol
- contracts/src/Zappers/Modules/FlashLoans/BalancerFlashLoan.sol
- contracts/src/Zappers/Modules/FlashLoans/Balancer/vault/IFlashLoanRecipient.sol
- contracts/src/Zappers/Modules/FlashLoans/Balancer/vault/IVault.sol
- contracts/src/Zappers/Modules/FlashLoans/MorphoFlashLoanProvider.sol
- contracts/src/Zappers/Modules/Testnet/TestnetExchangeBoldMinter.sol
- contracts/src/Zappers/Modules/Testnet/TestnetExchange.sol
- contracts/src/Zappers/Modules/Testnet/TestnetFlashLoanProvider.sol
- contracts/src/Zappers/WETHZapper.sol

Final Commit: 0d0e5f9ae6d2496965db5cf358fe17f643240d25

Findings

Each issue has an assigned severity:

- High issues are directly exploitable security vulnerabilities that need to be fixed.
- Medium issues are security vulnerabilities that may not be directly exploitable or may require certain conditions in order to be exploited. All major issues should be addressed.
- Low/Info issues are non-exploitable, informational findings that do not pose a security risk or impact the system's integrity. These issues are typically cosmetic or related to compliance requirements, and are not considered a priority for remediation.

Issues Found

High	Medium	Low/Info
0	0	1

Issues Not Fixed and Not Acknowledged

High	Medium	Low/Info
0	0	0

Issue L-1: Unnecessary code [RESOLVED]

Source:
https://github.com/sherlock-audit/2026-03-vyro-finance-mar-12th-2026/issues/89

Vulnerability Detail

In the `_getCanonicalRateWithFallbackInfo` function, L139 is useless. Since the function returns early in the above steps, L139 is never executed.

```
        if (!secondaryDown && _isCanonicalRateAboveLowerBound(secondaryRate)) {
            return (secondaryRate, false, address(0));
        }

        if (secondaryDown || !_isCanonicalRateAboveLowerBound(secondaryRate)) {
            return (0, true, address(canonicalRateSecondaryOracle.aggregator));
        }

@>      return (0, true, address(canonicalRateOracle.aggregator));
```

Code Snippet

https://github.com/sherlock-audit/2026-03-vyro-finance-mar-12th-2026/blob/dadba12718a1417a4a38c81c29e0b2ddbeeed4db/vyro/contracts/src/PriceFeeds/WSTETHPriceFeed.sol#L139

Tool Used

Manual Review

Recommendation

Remove the line 139.

Discussion

chriswessels

Acknowledged

Disclaimers

Sherlock does not provide guarantees nor warranties relating to the security of the project.

Usage of all smart contract software is at the respective users' sole risk and is the users' responsibility.