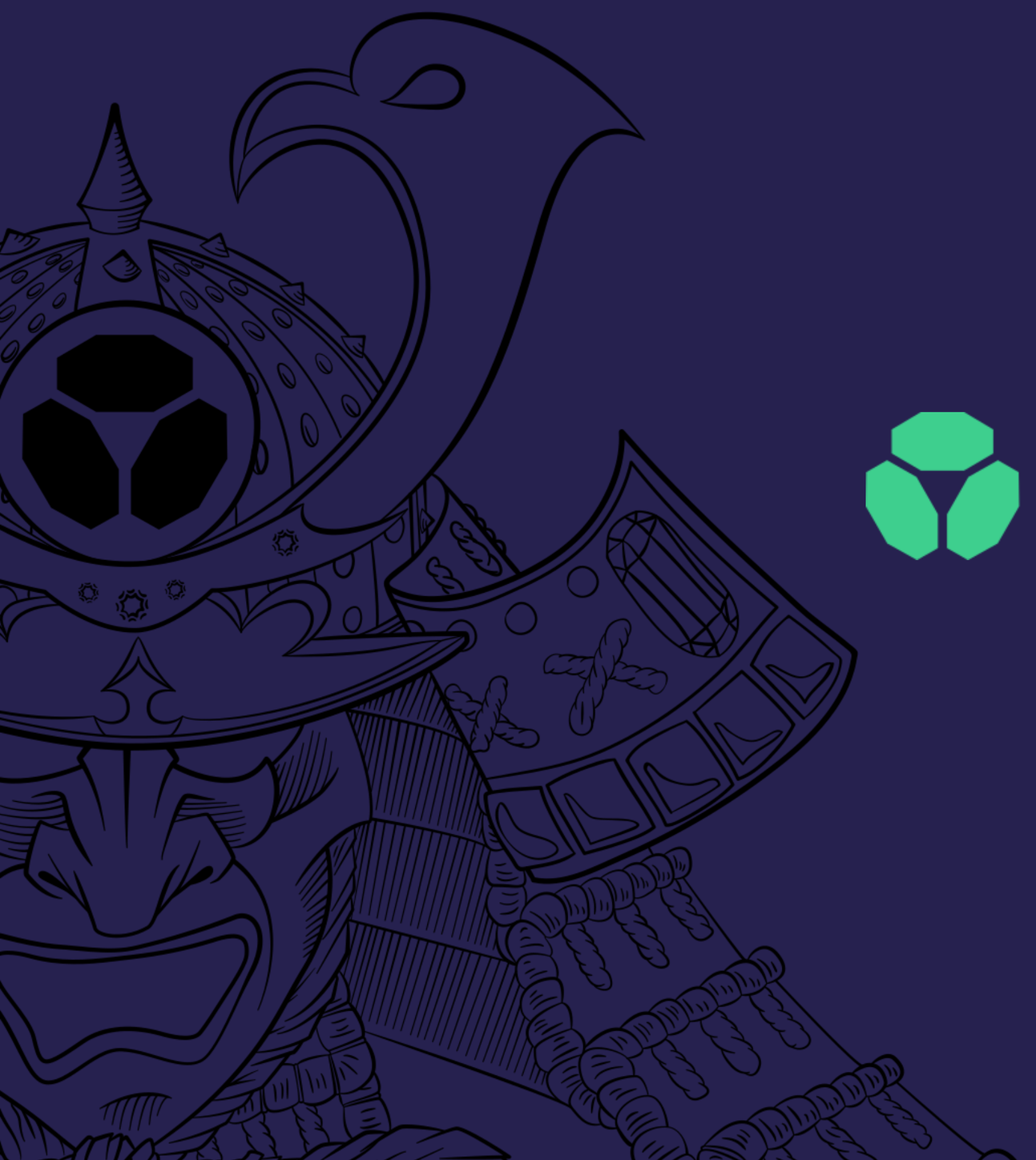

smart state

> Smart
Contract
Audit #

Dec 28
2021

TABLE OF CONTENTS

Table of contents 2

Methodology 3

Stucture of contacts 4

Verification check sums 92

METHODOLOGY

MAIN TESTS LIST:

- Best code practices
- ERC20/BEP20 compliance (if applicable)
- Logical bugs
- General Denial Of Service(DOS)
- Locked ether
- Private data leaks
- Using components with known vulns
- Weak PRNG
- Unsed vars
- Uncheked call return method
- Code with no effects
- Pool Asset Security (backdoors in the underlying ERC-20)
- Function visibility
- Use of deprecated functions
- Authorization issues
- Re-entrancy
- Arithmetic Over/Under Flows
- Hidden Malicious Code
- External Contract Referencing
- Short Address/ Parameter Attack
- Race Conditions / Front Running
- Uninitialized Storage Pointers
- Floating Points and Precision
- Signatures Replay

STRUCTURE OF CONTRACT

LIB.RS

CONTRACT METHODS ANALYSIS:

- initialize_borrowing_market(ctx: Context<InitializeBorrowingMarket>)
  Vulnerabilities not detected

- update_global_config(
    ctx: Context<UpdateGlobalConfig>,
    key: u16,
    value: u64,
)
  Vulnerabilities not detected

- approve_trove(ctx: Context<ApproveTrove>)
  Vulnerabilities not detected

PAYABLE

- deposit_collateral(
  ctx: Context<DepositCollateral>,
  amount_in_lamports: u64,
  collateral: u8,
)

Vulnerabilities not detected

Collateral tokens in, public

PAYABLE/FIXED

- borrow_stablecoin(ctx: Context<BorrowStable>, amount: u64)

Vulnerabilities not detected

Stable coins out, public

PAYABLE/FIXED

- deposit_collateral_and_borrow_stablecoin(
  ctx: Context<DepositCollateralAndBorrowStable>,
  deposit_amount: u64,
  deposit_asset: u8,
  borrow_amount: u64,
)

Vulnerabilities not detected

Collateral tokens in, stable

PAYABLE

- repay_loan(ctx: Context<RepayLoan>, amount: u64)

Vulnerabilities not detected

Stable coins in, public

PAYABLE/FIXED

- withdraw_collateral(
  ctx: Context<WithdrawCollateral>,
  amount: u64,
  collateral: u8,
)

Vulnerabilities not detected

Collateral tokens out, public

- stability_initialize(ctx: Context<InitializeStabilityPool>)

Vulnerabilities not detected

PAYABLE

- stability_provide(ctx: Context<ProvideStability>, amount: u64)

Vulnerabilities not detected

Stable coins in, public

PAYABLE

- stability_withdraw(ctx: Context<WithdrawStability>, amount: u64)

Vulnerabilities not detected

Stable coins out, public

FIXED

- try_liquidate(ctx: Context<TryLiquidate>)

  Vulnerabilities not detected

- harvest_liquidation_gains(
  ctx: Context<HarvestLiquidationGains>,
  token: u8,
)

  Vulnerabilities not detected

- clear_liquidation_gains(
  ctx: Context<ClearLiquidationGains>,
  token: u8,
)

  Vulnerabilities not detected

PAYABLE/FIXED

- add_redemption_order(
  ctx: Context<AddRedemptionOrder>,
  stablecoin_amount: u64,
)

  Vulnerabilities not detected

Stables coins in, public

- fill_redemption_order(
  ctx: Context<FillRedemptionOrder>,
  order_id: u64,
)

  Vulnerabilities not detected

- clear_redemption_order(
  ctx: Context<ClearRedemptionOrder>,
  order_id: u64,
)
  Vulnerabilities not detected

- staking_initialize(
  ctx: Context<InitializeStakingPool>,
  treasury_fee_rate: u16,
)
  Vulnerabilities not detected

- staking_approve(ctx: Context<ApproveStakingPool>)
  Vulnerabilities not detected

- staking_stake_hbb(ctx: Context<StakeHbbStakingPool>, amount: u64)
  Vulnerabilities not detected

- staking_harvest_reward(ctx: Context<HarvestRewardStakingPool>)
  Vulnerabilities not detected

- unstake_hbb(ctx: Context<UnstakeHbbStakingPool>, amount: u64)
  Vulnerabilities not detected

- unstake_hbb(ctx: Context<UnstakeHbbStakingPool>, amount: u64)
  Vulnerabilities not detected

- airdrop_hbb(ctx: Context<AirdropHbb>, amount: u64)
  Vulnerabilities not detected

PAYABLE

- airdrop_usdh(ctx: Context<AirdropUsdh>, amount: u64)
  Vulnerabilities not detected

Stable coins out, only admin

STRUCTURE OF CONTRACT

BORROWING_MARKET/BORROWING_OPERATIONS.RS

CONTRACT METHODS ANALYSIS:

- initialize_borrowing_market(
  market: &mut BorrowingMarketState,
  redemption_bootstrap_ts: u64,
)
  Vulnerabilities not detected

- approve_trove(
  market: &mut BorrowingMarketState,
  user: &mut UserMetadata,
)
  Vulnerabilities not detected

- deposit_collateral(
  market: &mut BorrowingMarketState,
  user: &mut UserMetadata,
  amount: u64,
  asset: CollateralToken,
)
  Vulnerabilities not detected

- borrow_stablecoin(
  market: &mut BorrowingMarketState,
  user: &mut UserMetadata,
  staking_pool: &mut StakingPoolState,
  requested_borrow_amount: u64,
  prices: &TokenPrices,
  now: u64,
)
  Vulnerabilities not detected

- repay_loan(
  market: &mut BorrowingMarketState,
  user: &mut UserMetadata,
  amount: u64,
)
  Vulnerabilities not detected

- deposit_and_borrow(
  market: &mut BorrowingMarketState,
  user: &mut UserMetadata,
  staking_pool: &mut StakingPoolState,
  borrow: u64,
  deposit: u64,
  deposit_asset: CollateralToken,
  prices: &TokenPrices,
  now: u64,
)
  Vulnerabilities not detected

- try_liquidate(
  liquidator: Pubkey,
  market: &mut BorrowingMarketState,
  user: &mut UserMetadata,
  stability_pool_state: &mut StabilityPoolState,
  epoch_to_scale_to_sum: &mut EpochToScaleToSum,
  token_prices: &TokenPrices,
  liquidations_queue: &mut RefMut<LiquidationsQueue>,
  now_timestamp: u64,
)
  Vulnerabilities not detected

- refresh_positions(
  market: &mut BorrowingMarketState,
  user: &mut UserMetadata,
)
  Vulnerabilities not detected

- deposit_collateral(
  market: &mut BorrowingMarketState,
  user: &mut UserMetadata,
  amount: u64,
  asset: CollateralToken,
  collateral_status: CollateralStatus,
)
  Vulnerabilities not detected

- set_addresses(user: &mut UserMetadata, owner: Pubkey, metadata: Pubkey)
  Vulnerabilities not detected

- assert_not_zero(value: u64, err: crate::BorrowError) -> Result<()
  Vulnerabilities not detected

- redistribute(
  market: &mut BorrowingMarketState,
  stablecoin_debt: u64,
  collateral: CollateralAmounts,
)
  Vulnerabilities not detected

- apply_pending_rewards(
  market: &BorrowingMarketState,
  user: &mut UserMetadata,
)
  Vulnerabilities not detected

- apply_pending_rewards(
  market: &BorrowingMarketState,
  user: &mut UserMetadata,
)
  Vulnerabilities not detected

- get_user_balances(market: &BorrowingMarketState, user: &UserMetadata)
  Vulnerabilities not detected

- get_pending_redistributed_stablecoin_reward(
  market: &BorrowingMarketState,
  user: &UserMetadata,
)
  Vulnerabilities not detected

- has_pending_rewards(market: &BorrowingMarketState, user: &mut UserMetadata)
  Vulnerabilities not detected

- update_reward_snapshots(market: &BorrowingMarketState, user: &mut UserMetadata)
  Vulnerabilities not detected

- compute_new_stake(market: &BorrowingMarketState, debt: u64)
  Vulnerabilities not detected

- update_user_stake_and_total_stakes(
    market: &mut BorrowingMarketState,
    user: &mut UserMetadata,
)
  Vulnerabilities not detected

- remove_stake(market: &mut BorrowingMarketState, user: &mut UserMetadata)
  Vulnerabilities not detected

- calculate_liquidation_effects(
    market: &BorrowingMarketState,
    user: &UserMetadata,
    stability_pool_state: &StabilityPoolState,
    prices: &TokenPrices,
)
  Vulnerabilities not detected

- liquidate_user(
    market: &mut BorrowingMarketState,
    user: &mut UserMetadata,
    stability_pool_state: &StabilityPoolState,
    token_prices: &TokenPrices,
)
  Vulnerabilities not detected

- update_system_snapshots_after_liquidation(market: &mut BorrowingMarketState, debt: u64)
  Vulnerabilities not detected

STRUCTURE OF CONTRACT

BORROWING_MARKET/
BORROWING_RATE.RS

CONTRACT METHODS ANALYSIS:

- from_amount(amount_to_borrow: u64, base_rate_bps: u16)
  Vulnerabilities not detected

- split_fees(requested_amount: u64, borrowing_rate: u16)
  Vulnerabilities not detected

- refresh_base_rate(
  market: &mut BorrowingMarketState,
  event: FeeEvent,
  now: u64,
)
  Vulnerabilities not detected

- calc_redemption_fee(base_rate: u16)
  Vulnerabilities not detected

- calc_borrowing_fee(base_rate: u16)
  Vulnerabilities not detected

- decay_base_rate(base_rate: u16, last_fee_
  event: u64, now: u64)
  Vulnerabilities not detected

- increase_base_rate(
    old_base_rate: u16,
    total_usdh_supply: u64,
    total_usdh_redeemed: u64,
)
  Vulnerabilities not detected

STRUCTURE OF CONTRACT

BORROWING_MARKET/
LIQUIDATION_CALCS.RS

CONTRACT METHODS ANALYSIS:

- try_borrow(
  requested_amount: u64,
  global_collateral: &CollateralAmounts,
  global_debt: u64,
  user_collateral: &CollateralAmounts,
  user_debt: u64,
  user_inactive_collateral: &CollateralAmounts,
  prices: &TokenPrices,
  current_mode: SystemMode,
  current_tcr: Decimal,
)

  Vulnerabilities not detected

- calc_system_mode(
  global_deposited_collateral: &CollateralAmounts,
  global_debt: u64,
  prices: &TokenPrices,
)

  Vulnerabilities not detected

- calc_liq_inputs(
  user_debt: u64,
  user_collateral: &CollateralAmounts,
  global_debt: u64,
  global_collateral: &CollateralAmounts,
  prices: &TokenPrices,
)

  Vulnerabilities not detected

- evaluate_liquidation_decision(
  user_debt: u64,
  user_collateral: &CollateralAmounts,
  global_debt: u64,
  global_collateral: &CollateralAmounts,
  usdh_in_sp: u64,
  prices: &TokenPrices,
)

  Vulnerabilities not detected

- split_stability_and_redistribution(
  usdh_in_sp: u64,
  user_debt: u64,
  user_collateral: &CollateralAmounts,
  liquidation_decision: LiquidationDecision,
  prices: &TokenPrices,
)

  Vulnerabilities not detected

- calculate_liquidation_effects(
  user_debt: u64,
  user_collateral: &CollateralAmounts,
  global_debt: u64,
  global_collateral: &CollateralAmounts,
  usdh_in_sp: u64,
  prices: &TokenPrices,
)
  Vulnerabilities not detected

- calculate_liquidation_split(
  collateral_deposited: &CollateralAmounts,
  liquidator_rate_bps: u16,
  clearer_rate_bps: u16,
)
  Vulnerabilities not detected

STRUCTURE OF CONTRACT

HANDLER_ADD_REDEMPTION_ORDER.RS

CONTRACT METHODS ANALYSIS:

- process(ctx: Context<AddRedemptionOrder>, stablecoin_amount: u64)

  Vulnerabilities not detected

STRUCTURE OF CONTRACT

HANDLER_ADD_REDEMPTION_ORDER.RS

CONTRACT METHODS ANALYSIS:

- process(mut ctx: Context<crate::ApproveStakingPool>)
  Vulnerabilities not detected
- set_accounts(ctx: &mut Context<crate::ApproveStakingPool>)
  Vulnerabilities not detected

STRUCTURE OF CONTRACT

HANDLER_APPROVE_TROVE.RS

CONTRACT METHODS ANALYSIS:

- process(mut ctx: Context<crate::ApproveTrove>)
  Vulnerabilities not detected
- assert_permissions(ctx: &Context<crate::ApproveTrove>)
  Vulnerabilities not detected
- set_accounts(ctx: &mut Context<crate::ApproveTrove>)
  Vulnerabilities not detected

STRUCTURE OF CONTRACT

HANDLER_BORROW_STABLECOIN.RS

CONTRACT METHODS ANALYSIS:

- process(ctx: Context<crate::BorrowStable>, stablecoin_amount: u64)

  Vulnerabilities not detected

STRUCTURE OF CONTRACT

HANDLER_CLEAR_LIQUIDATION_GAINS.RS

CONTRACT METHODS ANALYSIS:

- process(ctx: Context<crate::ClearLiquidationGains>,token: CollateralToken,)
  Vulnerabilities not detected

- assert_permissions(ctx: &Context<crate::ClearLiquidationGains>,token: CollateralToken,)
  Vulnerabilities not detected

STRUCTURE OF CONTRACT

HANDLER_CLEAR_REDEMPTION_ORDER.RS

CONTRACT METHODS ANALYSIS:

- process(ctx: Context<ClearRedemptionOrder>, order_id: u64)
  Vulnerabilities not detected

STRUCTURE OF CONTRACT

HANDLER_DEPOSIT_AND_BORROW.RS

CONTRACT METHODS ANALYSIS:

- process(ctx: Context<crate::DepositCollateralAndBorrowStable>, deposit_amount: u64,collateral: CollateralToken,borrow_amount: u64,)
  Vulnerabilities not detected

- assert_permissions(ctx: &Context<crate::DepositCollateralAndBorrowStable>,collateral: CollateralToken,)
  Vulnerabilities not detected

STRUCTURE OF CONTRACT

HANDLER_DEPOSIT_COLLATERAL.RS

CONTRACT METHODS ANALYSIS:

- process(ctx: Context<crate::DepositCollateral>,amount_in_lamports: u64,collateral: CollateralToken,)
  Vulnerabilities not detected

- assert_permissions(ctx: &Context<crate::DepositCollateral>,collateral: CollateralToken,)
  Vulnerabilities not detected

STRUCTURE OF CONTRACT

HANDLER_FILL_REDEMPTION_ORDER.RS

CONTRACT METHODS ANALYSIS:

- process(ctx: Context<FillRedemptionOrder>, order_id: u64)
  Vulnerabilities not detected
- deserialize_remaining_user_metadatas<'a, 'info, T>(ctx: &'a Context<'_, '_, '_, 'info, T>,borrowing_market_state: &'a Pubkey,)
  Vulnerabilities not detected
- accounts_to_metadatas<'a>(submitted_candidates_p: &'a mut Vec<ProgramAccount<UserMetadata>>,)
  Vulnerabilities not detected
- serialize_user_metadatas<T>(ctx: &Context<T>,submitted_candidates_p: &mut Vec<ProgramAccount<UserMetadata>>,)
  Vulnerabilities not detected

STRUCTURE OF CONTRACT

HANDLER_HARVEST_LIQUIDATION_GAINS.RS

CONTRACT METHODS ANALYSIS:

- process(ctx: Context<crate::HarvestLiquidationGains>,harvest_token: StabilityToken,)
  Vulnerabilities not detected

- assert_permissions(ctx: &Context<crate::HarvestLiquidationGains>,harvest_token: StabilityToken,)
  Vulnerabilities not detected

STRUCTURE OF CONTRACT

HANDLER_HARVEST_STAKING_REWARD.RS

CONTRACT METHODS ANALYSIS:

- process(ctx: Context<crate::HarvestRewardStakingPool>)
  Vulnerabilities not detected

- assert_permissions(ctx: &Context<crate::HarvestRewardStakingPool>)
  Vulnerabilities not detected

- assert_amount_not_zero(amount: u128)
  Vulnerabilities not detected

- assert_there_is_reward(
    rewards_tally: u128,
    amount_staked: u128,
    reward_per_token: u128,
)
  Vulnerabilities not detected

STRUCTURE OF CONTRACT

HANDLER_INITIALIZE_BORROWING_MARKET.RS

CONTRACT METHODS ANALYSIS:

- process(ctx: Context<crate::InitializeBorrowingMarket>)
  Vulnerabilities not detected

- to_set_authority_cpi_context(
  &self,
  account_to_context: pda::PDA,
)
  Vulnerabilities not detected

- to_set_authority_cpi_context_coll_vault(
  &self,
  token: CollateralToken,
)
  Vulnerabilities not detected

- assert_permissions(ctx: &Context<crate::InitializeBorrowingMarket>)

  Vulnerabilities not detected

- transfer_to_pda_collateral_vault(
  ctx: &Context<crate::InitializeBorrowingMarket>,
  token: CollateralToken,
  authority_pda: &PdaAddress,
)

  Vulnerabilities not detected

- transfer_to_pda(
  ctx: &Context<crate::InitializeBorrowingMarket>,
  mode: pda::PDA,
  authority_type: spl_token::instruction::AuthorityType,
)

  Vulnerabilities not detected

STRUCTURE OF CONTRACT

HANDLER_INITIALIZE_STABILITY_POOL.RS

CONTRACT METHODS ANALYSIS:

- process(
  ctx: Context<crate::InitializeStakingPool>,
  treasury_fee_rate: u16,
)
  Vulnerabilities not detected

- to_staking_cpi_context(&self)
  Vulnerabilities not detected

- transfer_staking_vault_account_ownership_to_pda(
  ctx: &Context<crate::InitializeStakingPool>,
)
  Vulnerabilities not detected

STRUCTURE OF CONTRACT

HANDLER_INITIALIZE_STAKING_POOL.RS

CONTRACT METHODS ANALYSIS:

- process(
  ctx: Context<crate::InitializeStakingPool>,
  treasury_fee_rate: u16,
)
  Vulnerabilities not detected

- to_staking_cpi_context(&self)
  Vulnerabilities not detected

- transfer_staking_vault_account_ownership_to_pda(
  ctx: &Context<crate::InitializeStakingPool>,
)
  Vulnerabilities not detected

STRUCTURE OF CONTRACT

HANDLER_REPAY_LOAN.RS

CONTRACT METHODS ANALYSIS:

- process(ctx: Context<RepayLoan>, stablecoin_amount: u64)
  Vulnerabilities not detected

STRUCTURE OF CONTRACT

HANDLER_STABILITY_APPROVE.RS

CONTRACT METHODS ANALYSIS:

- process(ctx: Context<crate::ApproveProvideStability>)
  Vulnerabilities not detected

STRUCTURE OF CONTRACT

HANDLER_STABILITY_PROVIDE.RS

CONTRACT METHODS ANALYSIS:

- process(ctx: Context<crate::ProvideStability>, amount: u64)
  Vulnerabilities not detected

- assert_permissions(
    ctx: &Context<crate::ProvideStability>,
    amount: u64,
)
  Vulnerabilities not detected

- assert_amount_not_zero(amount: u64)
  Vulnerabilities not detected

STRUCTURE OF CONTRACT

HANDLER_STABILITY_WITHDRAW.RS

CONTRACT METHODS ANALYSIS:

- process(ctx: Context<crate::WithdrawStability>, amount: u64)
  Vulnerabilities not detected
- assert_permissions(
  ctx: &Context<crate::WithdrawStability>,
  amount: u64,
)
  Vulnerabilities not detected
- assert_has_stake(user_total_stablecoin_provided: u64)
  Vulnerabilities not detected
- assert_amount_not_zero(amount: u64)
  Vulnerabilities not detected

STRUCTURE OF CONTRACT

HANDLER_STAKE_HBB.RS

CONTRACT METHODS ANALYSIS:

- process(ctx: Context<crate::StakeHbbStakingPool>, amount: u64)
  Vulnerabilities not detected

- ctx: &Context<crate::StakeHbbStakingPool>,
  amount: u64,
)
  Vulnerabilities not detected

- assert_amount_not_zero(amount: u64)
  Vulnerabilities not detected

STRUCTURE OF CONTRACT

HANDLER_TRY_LIQUIDATE.RS

CONTRACT METHODS ANALYSIS:

- process(ctx: Context<crate::TryLiquidate>)
  Vulnerabilities not detected

STRUCTURE OF CONTRACT

HANDLER_UNSTAKE_HBB.RS

CONTRACT METHODS ANALYSIS:

- process(ctx: Context<crate::UnstakeHbbStakingPool>, amount: u64)
  Vulnerabilities not detected

- assert_permissions(
    ctx: &Context<crate::UnstakeHbbStakingPool>,
    amount: u64,
)
  Vulnerabilities not detected

- assert_amount_not_zero(amount: u64)
  Vulnerabilities not detected

STRUCTURE OF CONTRACT

HANDLER_UPDATE_GLOBAL_CONFIG.RS

CONTRACT METHODS ANALYSIS:

- process(ctx: Context<UpdateGlobalConfig>, key: u16, value: u64)
  Vulnerabilities not detected

STRUCTURE OF CONTRACT

HANDLER_WITHDRAW_COLLATERAL.RS

CONTRACT METHODS ANALYSIS:

- process(
  ctx: Context<crate::WithdrawCollateral>,
  amount: u64,
  collateral: CollateralToken,
)
  Vulnerabilities not detected

- assert_permissions(
  ctx: &Context<crate::WithdrawCollateral>,
  collateral: CollateralToken,
)
  Vulnerabilities not detected

STRUCTURE OF CONTRACT

REDEMPTION/REDEMPTION_OPERATIONS.RS

CONTRACT METHODS ANALYSIS:

- add_redemption_order(
  redeemer: &mut UserMetadata,
  queue: &mut RefMut<RedemptionsQueue>,
  market: &mut BorrowingMarketState,
  prices: &TokenPrices,
  now_timestamp: u64,
  redemption_amount: u64,
)

  Vulnerabilities not detected

- fill_redemption_order(
  order_id: u64,
  market: &mut BorrowingMarketState,
  queue: &mut RefMut<RedemptionsQueue>,
  user_metadatas: &mut [&mut UserMetadata],
  filler_metadata: &UserMetadata,
  now_timestamp: u64,
)

  Any user can redeemded, even if they have positive colaterall ratio. Even if user has good collateral ratio he can be redeemed if there are no any other candidates. In your docs it is said that in order not to be redeemded users should have a high collateral ratio, however even if user has 160% collateral ratio and there are no other candidates he will get redeemed. We asssume that users should be able to protect them from getting redeemed via putting a field in user's metadata. So in case user has a high collateral ratio he can put a check mark so he won't be liquidated.

- clear_redemption_order<'a, 'b>(
  order_id: u64,
  redeemer: &'a mut UserMetadata,
  clearer: &'a mut UserMetadata,
  market: &'a mut BorrowingMarketState,
  redemptions_queue: &'a mut RefMut<RedemptionsQueue>,
  fillers_and_borrowers: &'a mut [&'b mut UserMetadata],
  now_timestamp: u64,
)

  Vulnerabilities not detected

- extract_transform_sort_candidates(
  market: &mut BorrowingMarketState,
  redemption_order: &RedemptionOrder,
  candidates: &mut [&mut UserMetadata],
  filler_metadata: &UserMetadata,
)

  Vulnerabilities not detected

- assert_unique(
  fillers_and_borrowers: &mut [&mut UserMetadata],
)

  Vulnerabilities not detected

- split_redemption_collateral(
  total: &CollateralAmounts,
  base_rate_bps: u16,
)

  Vulnerabilities not detected

- calculate_candidate(
  market: &mut BorrowingMarketState,
  user_metadata: &mut UserMetadata,
  prices: &TokenPrices,
  filler_metadata: Pubkey,
)

  Vulnerabilities not detected

- calc_redemption_amounts(
  fillers_and_borrowers: &mut [&mut UserMetadata],
  redemption_order: &RedemptionOrder,
  user_to_redeem_ix: usize,
  candidate_user_ix: usize,
  remaining_amount: u64,
)

  Vulnerabilities not detected

- next_fill_order<'a>(
  redemptions_queue: &'a mut RefMut<RedemptionsQueue>,
  order_id: u64,
  now: u64,
)

  Vulnerabilities not detected

- first_outstanding(
  redemptions_queue: &mut RefMut<RedemptionsQueue>,
)

  Vulnerabilities not detected

- add_redemption_order<'a, 'b>(
  amount: u64,
  queue: &'a mut RefMut<RedemptionsQueue>,
  redeemer: &'b UserMetadata,
  prices: &'b TokenPrices,
  now: u64,
  base_rate: u16,
)

  Vulnerabilities not detected

- collect_collateral_and_pay_debt(
  market: &mut BorrowingMarketState,
  order: &mut RedemptionOrder,
  fillers_and_borrowers: &mut [&mut UserMetadata],
)

  Vulnerabilities not detected

- collect_collateral_and_pay_debt(
  market: &mut BorrowingMarketState,
  order: &mut RedemptionOrder,
  fillers_and_borrowers: &mut [&mut UserMetadata],
)

  Vulnerabilities not detected

- flush_order(redemption_order: &mut RedemptionOrder)
  Vulnerabilities not detected

- close_redemption_order(order: &mut RedemptionOrder)
  Vulnerabilities not detected

- map_accounts_to_candidate_user<'a>(
    index: &usize,
    candidates: &'a [CandidateRedemptionUser],
    fillers_and_borrowers: &[&'a mut UserMetadata],
)
  Vulnerabilities not detected

- refresh_unfulfilled_order(redemption_order: &mut RedemptionOrder)
  Vulnerabilities not detected

- calculate_outstanding_redemption_amount(queue: &mut RefMut<RedemptionsQueue>)
  Vulnerabilities not detected

STRUCTURE OF CONTRACT

STABILITY_POOL/LIQUIDATIONS_QUEUE.RS

CONTRACT METHODS ANALYSIS:

- initialize_queue(queue: &mut RefMut<LiquidationsQueue>)
  Vulnerabilities not detected

- add_liquidation_event(
    liquidation_event: LiquidationEvent,
    queue: &mut RefMut<LiquidationsQueue>,
)
  Vulnerabilities not detected

- clear_liquidation_gains(
    queue: &mut RefMut<LiquidationsQueue>,
    token: CollateralToken,
    clearing_agent: Pubkey,
    now_timestamp: u64,
)
  Vulnerabilities not detected

- get(queue: &mut RefMut<LiquidationsQueue>, index: usize)
  Vulnerabilities not detected

- len(queue: &mut RefMut<LiquidationsQueue>)
  Vulnerabilities not detected

- get_next_index(queue: &mut RefMut<LiquidationsQueue>)
  Vulnerabilities not detected

- has_pending_liquidation_events(queue: &mut RefMut<LiquidationsQueue>)
  Vulnerabilities not detected

- remove_liquidation_event(queue: &mut RefMut<LiquidationsQueue>, index: usize)
  Vulnerabilities not detected

STRUCTURE OF CONTRACT

STABILITY_POOL/STABILITY_POOL_OPERATIONS.RS

CONTRACT METHODS ANALYSIS:

- initialize_stability_pool(
  stability_pool_state: &mut StabilityPoolState,
  liquidations_queue: &mut RefMut<LiquidationsQueue>,
  hbb_emissions_start_time: u64,
)
  Vulnerabilities not detected

- approve_new_user(
  stability_pool_state: &mut StabilityPoolState,
  stability_provider_state: &mut StabilityProviderState,
)
  Vulnerabilities not detected

- provide_stability(
  stability_pool_state: &mut StabilityPoolState,
  stability_provider_state: &mut StabilityProviderState,
  epoch_to_scale_to_sum: &mut EpochToScaleToSum,
  amount: u64,
  now_timestamp: u64,
)
  Vulnerabilities not detected

- withdraw_stability(
  stability_pool_state: &mut StabilityPoolState,
  stability_provider_state: &mut StabilityProviderState,
  epoch_to_scale_to_sum: &mut EpochToScaleToSum,
  amount: u64,
  now_timestamp: u64,
)

  Vulnerabilities not detected

- withdraw_stability(
  stability_pool_state: &mut StabilityPoolState,
  stability_provider_state: &mut StabilityProviderState,
  epoch_to_scale_to_sum: &mut EpochToScaleToSum,
  amount: u64,
  now_timestamp: u64,
)

  Vulnerabilities not detected

- update_pending_gains(
  stability_pool_state: &mut StabilityPoolState,
  stability_provider_state: &mut StabilityProviderState,
  epoch_to_scale_to_sum: &EpochToScaleToSum,
)

  Vulnerabilities not detected

- harvest_liquidation_gains(
  stability_pool_state: &mut StabilityPoolState,
  stability_provider_state: &mut StabilityProviderState,
  epoch_to_scale_to_sum: &mut EpochToScaleToSum,
  liquidations_queue: &mut RefMut<LiquidationsQueue>,
  now_timestamp: u64,
  harvest_token: StabilityToken,
)

  Vulnerabilities not detected

- harvest_pending_gains(
  stability_pool_state: &mut StabilityPoolState,
  stability_provider_state: &mut StabilityProviderState,
  harvest_token: StabilityToken,
)
  Vulnerabilities not detected

- liquidate(
  stability_pool_state: &mut StabilityPoolState,
  epoch_to_scale_to_sum: &mut EpochToScaleToSum,
  collateral_gain_to_stability_pool: CollateralAmounts,
  debt_to_offset: u64,
  now_timestamp: u64,
)
  Vulnerabilities not detected

- add_rewards_and_loss(
  stability_pool_state: &mut StabilityPoolState,
  epoch_to_scale_to_sum: &mut EpochToScaleToSum,
  gains: StabilityCollateralAmounts,
  usd_loss: u64,
)
  Vulnerabilities not detected

- trigger_hbb_issuance(
  stability_pool_state: &mut StabilityPoolState,
  epoch_to_scale_to_sum: &mut EpochToScaleToSum,
  now_timestamp: u64,
)
  Vulnerabilities not detected

- send_usd_to_stability_pool(
  stability_pool_state: &mut StabilityPoolState,
  amount: u64,
)

  Vulnerabilities not detected

- send_usd_to_depositor(
  stability_pool_state: &mut StabilityPoolState,
  amount: u64,
)

  Vulnerabilities not detected

- update_pending_gains(
  stability_provider_state: &mut StabilityProviderState,
  epoch_to_scale_to_sum: &EpochToScaleToSum,
)

  Vulnerabilities not detected

- get_new_user_snapshot(
  stability_pool_state: &StabilityPoolState,
  epoch_to_scale_to_sum: &EpochToScaleToSum,
  amount: u64,
)

  Vulnerabilities not detected

- get_compounded_usd_deposit(
  stability_pool_state: &StabilityPoolState,
  stability_provider_state: &StabilityProviderState,
)

  Vulnerabilities not detected

- compute_rewards_per_unit_staked(
  stability_pool_state: &mut StabilityPoolState,
  coll_to_add: StabilityCollateralAmounts,
  debt_to_offset: u64,
  total_usd_deposits: u64,
)

  Vulnerabilities not detected

- update_reward_sum_and_product(
  stability_pool_state: &mut StabilityPoolState,
  epoch_to_scale_to_sum: &mut EpochToScaleToSum,
  coll_gained_per_unit_staked: StabilityTokenMap,
  usd_loss_per_unit_staked: u64,
)

  Vulnerabilities not detected

- update_stability_pool_snapshot(
  stability_pool_state: &mut StabilityPoolState,
  epoch_to_scale_to_sum: &mut EpochToScaleToSum,
  new_p: u128,
  new_epoch: u64,
  new_scale: u64,
)

  Vulnerabilities not detected

- get_depositor_pending_gain(
  stability_provider_state: &StabilityProviderState,
  epoch_to_scale_to_sum: &EpochToScaleToSum,
)

  Vulnerabilities not detected

- get_pending_gain_from_snapshot(
  initial_deposit: u64,
  deposit_snapshot: &DepositSnapshot,
  epoch_to_scale_to_sum: &EpochToScaleToSum,
)

  Vulnerabilities not detected

- get_compounded_stake_from_snapshots(
  stability_pool_state_p: u128,
  stability_pool_state_current_scale: u64,
  stability_pool_state_current_epoch: u64,
  initial_stake: u64,
  snapshot: &DepositSnapshot,
)

  Vulnerabilities not detected

- compute_new_hbb_issuance(
  total_issued_so_far: u64,
  start_issuance_timestamp: u64,
  now_timestamp: u64,
)

  Vulnerabilities not detected

- expected_issuance_since_start(start: u64, now: u64)

  Vulnerabilities not detected

STRUCTURE OF CONTRACT

STAKING_POOL/STAKING_POOL_OPERATIONS.RS

CONTRACT METHODS ANALYSIS:

- initialize_staking_pool(staking_pool_state: &mut StakingPoolState)
  Vulnerabilities not detected

- approve_new_user(
  staking_pool_state: &mut StakingPoolState,
  user_staking_state: &mut UserStakingState,
)
  Vulnerabilities not detected

- user_stake(
  staking_pool_state: &mut StakingPoolState,
  user_staking_state: &mut UserStakingState,
  amount: u64,
)
  Vulnerabilities not detected

- user_harvest(
  staking_pool_state: &mut StakingPoolState,
  user_staking_state: &mut UserStakingState,
)
  Vulnerabilities not detected

- user_unstake(
  staking_pool_state: &mut StakingPoolState,
  user_staking_state: &mut UserStakingState,
  amount: u64,
)
  Vulnerabilities not detected

- split_fees(fees_to_pay: u64, treasury_fee_rate: u16) -> (u64, u64)
  Vulnerabilities not detected

- distribute_fees(staking_pool_state: &mut StakingPoolState, fees_to_pay: u64)
  Vulnerabilities not detected

STRUCTURE OF CONTRACT

STATE/BORROWING_MARKET_STATE.RS

CONTRACT METHODS ANALYSIS:

- fn new()
  Vulnerabilities not detected

- to_state_string(&self)
  Vulnerabilities not detected

STRUCTURE OF CONTRACT

STATE/BORROWING_VAULTS.RS

CONTRACT METHODS ANALYSIS:

- vault_address(&self, token: CollateralToken)
  Vulnerabilities not detected
- mint_address(&self, token: CollateralToken)
  Vulnerabilities not detected
- mint_address_for_stability_token(&self, token: StabilityToken)
  Vulnerabilities not detected

STRUCTURE OF CONTRACT

STATE/COLLATERAL_AMOUNTS.RS

CONTRACT METHODS ANALYSIS:

- is_zero_token(&self, token: CollateralToken)
  Vulnerabilities not detected
- token_amount(&self, token: CollateralToken)
  Vulnerabilities not detected
- of_token(amount: u64, token: CollateralToken)
  Vulnerabilities not detected
- of_token_f64(amount: f64, token: CollateralToken)
  Vulnerabilities not detected
- to_token_map(&self)
  Vulnerabilities not detected

STRUCTURE OF CONTRACT

STATE/DEPOSIT_SNAP-SHOT.RS

CONTRACT METHODS ANALYSIS:

- default()
  Vulnerabilities not detected
- new(sum: StabilityTokenMap, product: u128, scale: u64, epoch: u64)
  Vulnerabilities not detected

STRUCTURE OF CONTRACT

STATE/EPOCH_TO_SCALE_TO_SUM.RS

CONTRACT METHODS ANALYSIS:

- default()
  Vulnerabilities not detected

- get_sum(&self, epoch: u64, scale: u64)
  Vulnerabilities not detected

- set_sum(
  &mut self,
  epoch: u64,
  scale: u64,
  sum: StabilityTokenMap,
)
  Vulnerabilities not detected

- from(v: Vec<Vec<StabilityTokenMap>>)
  Vulnerabilities not detected

- unpack(data: &[u128; 1000])
  Vulnerabilities not detected

- pack(&self)
  Vulnerabilities not detected

- pack_to_zero_copy_account(
  &self,
  epoch_to_scale_to_sum_account: &mut Loader<EpochToScaleToSumAccount>,
  mode: LoadingMode,
)
  Vulnerabilities not detected

STRUCTURE OF CONTRACT

STATE/LIQUIDATIONS_QUEUE.RS

CONTRACT METHODS ANALYSIS:

- default()
  Vulnerabilities not detected
- empty()
  Vulnerabilities not detected
- new(
  liquidator: Pubkey,
  liquidator_gains: CollateralAmounts,
  clearer_gains: CollateralAmounts,
  stability_pool_gains: CollateralAmounts,
  event_timestamp: u64,
)
  Vulnerabilities not detected
- state/redemptions_queue.rs
  Vulnerabilities not detected

- from(val: RedemptionCandidateStatus)
  Vulnerabilities not detected

- from(val: RedemptionOrderStatus)
  Vulnerabilities not detected

- from(number: u8)
  Vulnerabilities not detected

STRUCTURE OF CONTRACT

STATE/REDEMPTIONS_QUEUE.RS

CONTRACT METHODS ANALYSIS:

- from(val: RedemptionCandidateStatus)
  Vulnerabilities not detected
- from(val: RedemptionOrderStatus)
  Vulnerabilities not detected
- from(number: u8)
  Vulnerabilities not detected

STRUCTURE OF CONTRACT

STATE/STABILITY_COL-LATERAL_AMOUNTS.RS

CONTRACT METHODS ANALYSIS:

- is_zero_token(&self, token: StabilityToken)
  Vulnerabilities not detected
- token_amount(&self, token: StabilityToken)
  Vulnerabilities not detected
- of_token(amount: u64, token: StabilityToken)
  Vulnerabilities not detected
- to_token_map(&self)
  Vulnerabilities not detected

STRUCTURE OF CONTRACT

STATE/STABILITY_POOL_STATE.RS

CONTRACT METHODS ANALYSIS:

- new(
    num_users: u64,
    total_users_providing_stability: u64,
    cumulative_gains_total: StabilityTokenMap,
    pending_collateral_gains: StabilityTokenMap,
    current_epoch: u64,
    current_scale: u64,
)

  Vulnerabilities not detected

STRUCTURE OF CONTRACT

STATE/STABILITY_PROVIDER_STATE.RS

CONTRACT METHODS ANALYSIS:

- approve_stability(&mut self, user_id: u64)
  Vulnerabilities not detected

- to_state_string(&self)
  Vulnerabilities not detected

STRUCTURE OF CONTRACT

STATE/STABILITY_TOKEN_MAP.RS

CONTRACT METHODS ANALYSIS:

- is_zero_token(&self, token: StabilityToken)
  Vulnerabilities not detected
- token_amount(&self, token: StabilityToken)
  Vulnerabilities not detected
- of_token(amount: u128, token: StabilityToken)
  Vulnerabilities not detected
- to_collateral_amounts(&self)
  Vulnerabilities not detected

STRUCTURE OF CONTRACT

STATE/STABILITY_VAULTS.RS

CONTRACT METHODS ANALYSIS:

- vault_address(&self, token: StabilityToken)
  Vulnerabilities not detected
- vault_address_for_collateral_token(&self, token: CollateralToken)
  Vulnerabilities not detected

STRUCTURE OF CONTRACT

STATE/STAKING_POOL_STATE.RS

CONTRACT METHODS ANALYSIS:

- new(
    total_stake: u128,
    reward_per_token: u128,
    total_distributed_rewards: u128,
    rewards_not_yet_claimed: u128,
)
  Vulnerabilities not detected

- initialize_staking_pool(&mut self)
  Vulnerabilities not detected

- to_state_string(&self)
  Vulnerabilities not detected

STRUCTURE OF CONTRACT

STATE/TOKEN_MAP.RS

CONTRACT METHODS ANALYSIS:

- is_zero_token(&self, token: CollateralToken)
  Vulnerabilities not detected
- token_amount(&self, token: CollateralToken)
  Vulnerabilities not detected
- of_token(amount: u128, token: CollateralToken)
  Vulnerabilities not detected
- to_collateral_amounts(&self)
  Vulnerabilities not detected

STRUCTURE OF CONTRACT

STATE/USER_STAKING_RATE.RS

CONTRACT METHODS ANALYSIS:

- to_state_string(&self)
  Vulnerabilities not detected

STRUCTURE OF CONTRACT

TOKEN_OPERATIONS/
HBB.RS

CONTRACT METHODS ANALYSIS:

- mint<'info>(
  amount: u64,
  hbb_mint_seed: u8,
  owner: Pubkey,
  program_id: &Pubkey,
  hbb_mint: AccountInfo<'info>,
  mint_to: AccountInfo<'info>,
  hbb_mint_authority: AccountInfo<'info>,
  token_program: AccountInfo<'info>,
)
  Vulnerabilities not detected

- transfer<'info>(
  amount: u64,
  from: &AccountInfo<'info>,
  to: &AccountInfo<'info>,
  authority: &AccountInfo<'info>,
  token_program: &AccountInfo<'info>,
)

  Vulnerabilities not detected

- user_unstake(
  staking_pool_state: &mut StakingPoolState,
  user_staking_state: &mut UserStakingState,
  amount: u64,
)

  Vulnerabilities not detected

- transfer_from_staking_pool<'info>(
  amount: u64,
  owner: Pubkey,
  to_account: &AccountInfo<'info>,
  from_vault: &AccountInfo<'info>,
  from_vault_authority: &AccountInfo<'info>,
  from_vault_authority_seed: u8,
  token_program: &AccountInfo<'info>,
  program_id: &Pubkey,
)

  Vulnerabilities not detected

STRUCTURE OF CONTRACT

TOKEN_OPERATIONS/
SOLTOKEN.RS

CONTRACT METHODS ANALYSIS:

- transfer_from_user<'info>(
  amount_in_lamports: u64,
  from: &AccountInfo<'info>,
  to: &AccountInfo<'info>,
  system_program: &AccountInfo<'info>,
)
  Vulnerabilities not detected

- transfer_from_vault<'info>(
  amount_in_lamports: u64,
  from: &AccountInfo<'info>,
  to: &AccountInfo<'info>,
)
  Vulnerabilities not detected

STRUCTURE OF CONTRACT

TOKEN_OPERATIONS/
SPLTOKEN.RS

CONTRACT METHODS ANALYSIS:

- mint<'info>(
  mint_coin: &AccountInfo<'info>,
  mint_to: &AccountInfo<'info>,
  mint_coin_authority: &AccountInfo<'info>,
  mint_coin_authority_seed: u8,
  pda_mode: crate::pda::PDA,
  token_program: &AccountInfo<'info>,
  program_id: &Pubkey,
  amount: u64,
)
  Vulnerabilities not detected

- burn<'info>(
  mint: &AccountInfo<'info>,
  burn_from: &AccountInfo<'info>,
  burn_authority: &AccountInfo<'info>,
  burn_authority_seed: u8,
  pda_mode: crate::pda::PDA,
  token_program: &AccountInfo<'info>,
  program_id: &Pubkey,
  amount: u64,
)

  Vulnerabilities not detected

- transfer_from_vault<'info>(
  amount: u64,
  mode: pda::PDA,
  to_vault: &AccountInfo<'info>,
  from_vault: &AccountInfo<'info>,
  from_vault_authority: &AccountInfo<'info>,
  from_vault_authority_seed: u8,
  token_program: &AccountInfo<'info>,
  program_id: &Pubkey,
)

  Vulnerabilities not detected

- transfer_from_user<'info>(
  amount: u64,
  from_ata: &AccountInfo<'info>,
  to: &AccountInfo<'info>,
  authority: &AccountInfo<'info>,
  token_program: &AccountInfo<'info>,
)

  Vulnerabilities not detected

STRUCTURE OF CONTRACT

TOKEN_OPERATIONS/
STABLECOIN.RS

CONTRACT METHODS ANALYSIS:

- mint<'info>(
  amount: u64,
  stablecoin_mint_seed: u8,
  owner: Pubkey,
  program_id: &Pubkey,
  stablecoin_mint: AccountInfo<'info>,
  mint_to: AccountInfo<'info>,
  stablecoin_mint_authority: AccountInfo<'info>,
  token_program: AccountInfo<'info>,
)
  Vulnerabilities not detected

- burn<'info>(
  amount: u64,
  burn_from: &AccountInfo<'info>,
  mint: &AccountInfo<'info>,
  burn_authority: &AccountInfo<'info>,
  burn_authority_seed: u8,
  pda_mode: crate::pda::PDA,
  program_id: &Pubkey,
  token_program: &AccountInfo<'info>,
)
  Vulnerabilities not detected

- transfer<'info>(
  amount: u64,
  from: &AccountInfo<'info>,
  to: &AccountInfo<'info>,
  authority: &AccountInfo<'info>,
  token_program: &AccountInfo<'info>,
)
  Vulnerabilities not detected

- transfer<'info>(
  amount: u64,
  from: &AccountInfo<'info>,
  to: &AccountInfo<'info>,
  authority: &AccountInfo<'info>,
  token_program: &AccountInfo<'info>,
)
  Vulnerabilities not detected

- transfer_from_borrowing_fees_vault<'info>(
  amount: u64,
  owner: Pubkey,
  to_vault: &AccountInfo<'info>,
  from_vault: &AccountInfo<'info>,
  from_vault_authority: &AccountInfo<'info>,
  from_vault_authority_seed: u8,
  token_program: &AccountInfo<'info>,
  program_id: &Pubkey,
)
  Vulnerabilities not detected

STRUCTURE OF CONTRACT

UTILS/BN.RS

CONTRACT METHODS ANALYSIS:

- serialize<W: Write>(&self, writer: &mut W)
  Vulnerabilities not detected
- deserialize(buf: &mut &[u8])
  Vulnerabilities not detected
- to_u64(self)
  Vulnerabilities not detected
- try_to_u64(self)
  Vulnerabilities not detected
- to_u128(self)
  Vulnerabilities not detected

- try_to_u128(self)
  Vulnerabilities not detected
- from_le_bytes(bytes: [u8; 32])
  Vulnerabilities not detected
- to_le_bytes(self)
  Vulnerabilities not detected
- to_u64(self)
  Vulnerabilities not detected
- try_to_u64(self)
  Vulnerabilities not detected
- to_u128(self)
  Vulnerabilities not detected
- try_to_u128(self)
  Vulnerabilities not detected
- from_le_bytes(bytes: [u8; 24])
  Vulnerabilities not detected
- to_le_bytes(self)
  Vulnerabilities not detected

STRUCTURE OF CONTRACT

UTILS/CORETYPES.RS

CONTRACT METHODS ANALYSIS:

- checked_add_assign(&mut self, rhs: Self) -> Result<()
  Vulnerabilities not detected
- checked_sub_assign(&mut self, rhs: Self) -> Result<()
  Vulnerabilities not detected
- checked_add_assign(&mut self, rhs: Self) -> Result<()
  Vulnerabilities not detected
- checked_sub_assign(&mut self, rhs: Self) -> Result<()
  Vulnerabilities not detected
- checked_add_assign(&mut self, rhs: Self) -> Result<()
  Vulnerabilities not detected

- checked_sub_assign(&mut self, rhs: Self) -> Result<()
  Vulnerabilities not detected
- from(value: u64, exp: u8)
  Vulnerabilities not detected
- f64(&self)
  Vulnerabilities not detected
- rom_f64(price: f64, token: CollateralToken)
  Vulnerabilities not detected
- fmt(&self, f: &mut fmt::Formatter<'_>)
  Vulnerabilities not detected
- new(sol_price: f64)
  Vulnerabilities not detected
- new_all(price: f64)
  Vulnerabilities not detected
- token_amount(&self, token: CollateralToken)
  Vulnerabilities not detected
- from(amount: f64)
  Vulnerabilities not detected
- from(amount: f64)
  Vulnerabilities not detected
- from(amount: f64)
  Vulnerabilities not detected

STRUCTURE OF CONTRACT

UTILS/FINANCE.RS

CONTRACT METHODS ANALYSIS:

- from(user: &UserMetadata, prices: &TokenPrices)
  Vulnerabilities not detected

- calc_coll_ratio(
    debt_usdh: u64,
    collateral_deposited: &CollateralAmounts,
    prices: &TokenPrices,
)
  Vulnerabilities not detected

- coll_ratio(debt_usdh: u64, market_value_usdh: u64)
  Vulnerabilities not detected

- calc_market_value_usdh(prices: &TokenPrices, amounts: &CollateralAmounts)
  Vulnerabilities not detected

- calc_market_value_usdh(prices: &TokenPrices, amounts: &CollateralAmounts)
  Vulnerabilities not detected

- ten_pow(exponent: u8)
  Vulnerabilities not detected

STRUCTURE OF CONTRACT

UTILS/MATH.RS

CONTRACT METHODS ANALYSIS:

- stablecoin_decimal_to_u64(number: f64)
  Vulnerabilities not detected

- coll_to_lamports(number: f64, collateral: CollateralToken)
  Vulnerabilities not detected

STRUCTURE OF CONTRACT

UTILS/ORACLE.RS

CONTRACT METHODS ANALYSIS:

- get_prices(
  pyth_sol_price_info: &AccountInfo,
  pyth_eth_price_info: &AccountInfo,
  pyth_btc_price_info: &AccountInfo,
  pyth_srm_price_info: &AccountInfo,
  pyth_ray_price_info: &AccountInfo,
  pyth_ftt_price_info: &AccountInfo,
)
  Vulnerabilities not detected

- get_price(pyth_price_info: &AccountInfo)
  Vulnerabilities not detected

STRUCTURE OF CONTRACT

UTILS/PDA.RS

CONTRACT METHODS ANALYSIS:

- collateral_vault_from(owner: &Pubkey)
  Vulnerabilities not detected
- liquidation_rewards_vault_from(owner: &Pubkey)
  Vulnerabilities not detected
- make_pda_pubkey(mode: PDA, program: &Pubkey)
  Vulnerabilities not detected
- make_pda_seeds<'a>(mode: &'a PDA, _program: &'a Pubkey)
  Vulnerabilities not detected
- make_seeds(owner: &Pubkey, tag: &'static str)
  Vulnerabilities not detected
- make_pda(owner: &Pubkey, tag: &str, program: &Pubkey)
  Vulnerabilities not detected
- drop_reward()
  Vulnerabilities not detected

VERIFICATION CHECK SUMS

Contract Name	Bytecode hash (SHA 256)
lib.rs	4765e25cced29162bcc9fb9a73bd6040e71905f54d8fa97b0415b5c45b06196e
borrowing_market/borrowing_operations.rs	09de7b06524527d7778ed6b9316f844c34540fd91b4178a2b98fb237f530f8de
borrowing_market/borrowing_rate.rs	dd64491f49b518f85b6aad7774774f9328eaf436fe0135ed4d79164899ae18fe
borrowing_market/liquidation_calcs.rs	5e93b8bdf4dbc56a38ce9b6d5cd92630b3ea0a847d34bb21cf42cfd83d5f01a5

Contract Name	Bytecode hash (SHA 256)
handler_add_redemption_order.rs	9ed2fd13e31d7bdad1650d6cece167f3219e032405c0f4b15301356ac527a454
handler_approve_staking_pool.rs	1230c0a2fdd2c97245377d4cbb525727706cfb18c8c12206992c12464a4b7f27
handler_approve_trove.rs	665cd28744c340f5da1baea1b2b38713ec3f93d4590d5963470df15b36abbb3f
handler_borrow_stablecoin.rs	a5e77334ce9856d8d2c0158872016e76c53bf4d1b888a9da68b4ceac50935c5f
handler_clear_liquidation_gains.rs	b5e73efca0938e5633c5ae8a375f64113c092f6c1885ebd9d6ae37c9a8fa4be3

Contract Name	Bytecode hash (SHA 256)
handler_clear_ redemption_order.rs	418ba5d5304b583b1b02823427e437f41fad4608fa4ebdf7b28 2648f369347f0
handler_deposit_ and_borrow.rs	cc0414e7d83ab5df2efb5ea2de822a5418680bb08dbba1b0fc 450e3816c7e962
handler_deposit_ collateral.rs	d674540d22dbe024d5d0af2c7adc970a515e0f2ec906b9fc4d 438e093bc11e58
handler_fill_ redemption_order.rs	9e7037213b7f80a065cfb919d99ec5f152de73cf7ebe106d78b9 2640eb4edc6b

Contract Name	Bytecode hash (SHA 256)
handler_harvest_liquidation_gains.rs	9e7037213b7f80a065cfb919d99ec5f152de73cf7ebe106d78b92640eb4edc6b
handler_harvest_staking_reward.rs	70bf713db9d17e4fb1ec2c6d895f8fe2f21355f9975d6035c287f3b8d91358fc
handler_initialize_borrowing_market.rs	3b12fd9a0ef0945e1c58823afbba10a7eefccb395af7f06b67ba1b12f3582419
handler_initialize_stability_pool.rs	81b47ab01be6c6b0fef60c73941ffb2ad4df8d66bd4520448dd0bc63e6b5bfac

Contract Name	Bytecode hash (SHA 256)
handler_initialize_staking_pool.rs	1659e0d28ce64781ec15ec5dbe9530fc07f97f7d5719998e4d666044dbf54ca6
handler_repay_loan.rs	1a6ae637540056ab72a9c02b4233dfe5664f58e9358849b532c90cd18372ee3d
handler_stability_approve.rs	1ecfe21b8f1c9ed65fe59cc6b1b409db4cc9301216d4e2a38fa944a2fdb840d3
handler_stability_provide.rs	9b4743bc6d19a0574918e9c286416af602fdc621d2a95faf11c0d1850a79b596

Contract Name	Bytecode hash (SHA 256)
handler_stability_withdraw.rs	b9db1ccd282774037f9feafe84dd6ca2520fa5e59e82e5b1ba313613421f334b
handler_stake_hbb.rs	ffbe82f8e436be2be7fe5dde42331f37505695dcbbd23b662e3868d13312fbc0
handler_try_liquidate.rs	02dd85e4bdc8f43d65895a6bbc824ee48d96a90a212d21eb3fa7edee9ca3e31f
handler_unstake_hbb.rs	b52a9444936d50108f1b6a53d75d552e6b1144b1505722032e676bd424408a88

Contract Name	Bytecode hash (SHA 256)
handler_update_global_config.rs	7cd69b3ef2937f04bda0064f4d8f3c836958bcacca37c10933aefe63744d6c23
handler_withdraw_collateral.rs	9eebc25834a5ef07a134113917fcc7e61b18a0128b3fb60b63c847751fb78de7
redemption/redemption_operations.rs	6085ebdddb99ea573195d97d055261f035df6f46f194c8f8aa66167ad354c9a1
stability_pool/liquidations_queue.rs	9bf2464598da8b3bea8954d97eaeadf22d4740ccb9dde39ae33522bc65f2168a

Contract Name	Bytecode hash (SHA 256)
stability_pool/stability_pool_operations.rs	63199b9d93ef564668fba852a552339b00b6fbe2bd1c1fed0543834f55bf2e0f
staking_pool/staking_pool_operations.rs	b4dbf8b9b5f9874ff98f8b99b3f047454ee3ecdedde16cc4d1d55c368c3a2aa6
state/borrowing_market_state.rs	5ec481a8648597ccb7be1032e294d568445131e8f95c27151b4f940be35507df
state/borrowing_vaults.rs	245363ce42372924daade038a83eb2d643b3fc13306ead2be7f19fecc6efd27f

Contract Name	Bytecode hash (SHA 256)
state/collateral_amounts.rs	c36492eaa764c8547145b845b4f6260c82f90509eda1d28606eb83ccfc943b6d
state/deposit_snapshot.rs	4cdad3042567b499df7000001637dc6fe1e6d13ebd47de2521207a630bf87536
state/epoch_to_scale_to_sum.rs	17b82053bb12be08e481628fe53d5c7ae96d6b049efa884fa1139ef0629e0160
state/liquidations_queue.rs	b0150645e53d04813637dc215c64796167e11758f8da9489370239d97755e9eb

Contract Name	Bytecode hash (SHA 256)
state/redemptions_queue.rs	8de6a67b3de28f6b89f75768b8bcb3531314ae5cb582fd04786d8c72e6b44301
state/stability_collateral_amounts.rs	c2955db03f996b718a86f456be9b6ad293401b933895a6b70b6c0415c5401e93
state/stability_pool_state.rs	34d5315d8d4aed0651d0672e2c91a598d696d7a4faece94de4f5627d19ee3c2d
state/stability_provider_state.rs	05d9493cce1d8cdcc0273e632f8eebb9362fab9e4a9ca0a26759f393135d57cc

Contract Name	Bytecode hash (SHA 256)
state/stability_token_map.rs	da6d3ccd97e607a86301aaecfdcead6a8dc1f86d676c909928098f5fff00087d
state/stability_vaults.rs	065eb038e6c8bf47eb594ab1723d27a9b4da5e7c4005b39d3ab1ecf8bf3c74b6
state/staking_pool_state.rs	5f4766bd3399de2f0fa2e120d4ed5d54e8725089624c7c0f2895b0a4fb28dcc4
state/token_map.rs	1ccc8d65bdaf6273ff4a2cc1445523bc48605136b8106bbe4b29ede502043c19

Contract Name	Bytecode hash (SHA 256)
state/user_staking_rate.rs	984f3ca4caf22c135e8106505d74dc1b7405997c10c8a64e65f8bb144bd19a16
token_operations/hbb.rs	42f0a91fdd1fd88d70c1e323798722dfe38d644c3a317ad4cc774d2e488774c8
token_operations/soltoken.rs	2199f358463025396f8d2441135788f6f458c88a4f57cc1c0c014c71c0085e42
token_operations/spltoken.rs	5b96cea6df12986f8eaedfa954b5bdc4948ecc815d2fa19ef1afd821b4f4033b

Contract Name	Bytecode hash (SHA 256)
token_operations/ stablecoin.rs	d04a8d8969cb3313b5d8c5eb078d801cdcaa2ab622a6b53d390480e93957138d
utils/bn.rs	820ddbd39b56f67535d7c669c15b78ab882eeefaafcbeeaf163cf9e6b79d9042
utils/coretypes.rs	0d9412491000f0dc9cb9b67707ac49dc910666be0b4eff1e4ec2b8d660641d44
utils/finance.rs	3b2b0a5374c6f9af1e353e213cd9bcb2cd4132ec83cf462b1259b4e6b8e5a54b

Contract Name	Bytecode hash (SHA 256)
utils/math.rs	831572f1310ccaf84e114a6294e7a2cb7c428ad41bb4727d895c9d6706aa4a94
utils/oracle.rs	6db368e5812a7e7e9fcc9cc1b2691d9dae0bb6589ede2340a0716249bd5b5054
utils/pda.rs	dea62afbfb81b65b05c2bfcf095d9a3cabcd2c1b675216ed9b1e0667a0379778

Get In Touch

info@smartstate.tech

smartstate.tech