smart state

new generation of
smart contract audit

Kamino Finance

Aug 27
2022

TABLE OF CONTENTS

METHODOLOGY

MAIN TESTS LIST:

- Best code practices
- ERC20/BEP20 compliance (if applicable)
- FA2 compliance (if applicable)
- Logical bugs
- General Denial Of Service(DOS)
- Locked ether
- Private data leaks
- Using components with known vulns
- Weak PRNG
- Unused vars
- Unchecked 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

YVAULTS/PROGRAMS/YVAULTS/SRC/LIB.RS

CONTRACT METHODS ANALYSIS:

- initialize_strategy(
  ctx: Context<InitializeStrategy>,
  token_a_collateral_id: u64,
  token_b_collateral_id: u64,
)
  Vulnerabilities not detected

- initialize_global_config(ctx: Context<InitializeGlobalConfig>)
  Vulnerabilities not detected

- update_global_config(
  ctx: Context<UpdateGlobalConfig>,
  key: u16,
  index: u16,
  value: [u8; VALUE_BYTE_ARRAY_LEN],
)
  Vulnerabilities not detected

- update_treasury_fee_vault(
  ctx: Context<UpdateTreasuryFeeVault>,
  collateral_id: u16,
)
  Vulnerabilities not detected

- update_admin_authority(ctx: Context<UpdateAdminAuthority>)
  Vulnerabilities not detected

- update_strategy_config(
    ctx: Context<UpdateStrategyConfig>,
    mode: u16,
    value: u64,
)
  Vulnerabilities not detected

- update_reward_mapping(
    ctx: Context<UpdateRewardMapping>,
    reward_id: u8,
    collateral_token: u8,
)
  Vulnerabilities not detected

- open_liquidity_position(
    ctx: Context<OpenLiquidityPosition>,
    tick_lower_index: i64,
    tick_upper_index: i64,
    bump: u8,
)
  Vulnerabilities not detected

- deposit(
    ctx: Context<Deposit>,
    token_max_a: u64,
    token_max_b: u64
)
  Vulnerabilities not detected

- invest(ctx: Context<Invest>)
  Vulnerabilities not detected

- deposit_and_invest(
  ctx: Context<DepositAndInvest>,
  token_max_a: u64,
  token_max_b: u64,
)
  Vulnerabilities not detected

- withdraw(
  ctx: Context<Withdraw>,
  shares_amount: u64
)
  Vulnerabilities not detected

- executive_withdraw(
  ctx: Context<ExecutiveWithdraw>,
  action: u8
)
  Vulnerabilities not detected

- collect_fees(ctx: Context<CollectFees>)
  Vulnerabilities not detected

- collect_rewards(ctx:
  Context<CollectRewards>)
  Vulnerabilities not detected

- swap_rewards(
  ctx: Context<SwapRewards>,
  token_a_in: u64,
  token_b_in: u64,
  reward_id: u8,
  min_collateral_token_out: u64,
)
  Vulnerabilities not detected

- swap_uneven_vaults(ctx:
  Context<SwapUnevenVaults>)
  Vulnerabilities not detected

STRUCTURE OF CONTRACT

YVAULTS/PROGRAMS/YVAULTS/SRC/ORCA_STATE.RS

CONTRACT METHODS ANALYSIS:

- to_orca_reward_info(&self)
  Vulnerabilities not detected
- to_orca_whirlpool(self)
  Vulnerabilities not detected
- to_orca_position(&self)
  Vulnerabilities not detected
- initialized(&self)
  Vulnerabilities not detected

STRUCTURE OF CONTRACT

YVAULTS/PROGRAMS/YVAULTS/SRC/INSTRUCTIONS/SWAP_UNEVEN_VAULTS.RS

CONTRACT METHODS ANALYSIS:

- handler(
  ctx: Context<OpenLiquidityPosition>,
  tick_lower_index: i64,
  tick_upper_index: i64,
  bump: u8,
)
  Vulnerabilities not detected

STRUCTURE OF CONTRACT

YVAULTS/PROGRAMS/YVAULTS/SRC/INSTRUCTIONS/COLLECT_FEES.RS

CONTRACT METHODS ANALYSIS:

- `handler(ctx: Context<CollectFees>)`
  Vulnerabilities not detected

- `transfer_fees_to_treasury_vault(`
  `ctx: &Context<CollectFees>,`
  `bump: u8,`
  `a_amount: u64,`
  `b_amount: u64,`
  `)`
  Vulnerabilities not detected

STRUCTURE OF CONTRACT

YVAULTS/PROGRAMS/YVAULTS/SRC/INSTRUCTIONS/WITHDRAW.RS

CONTRACT METHODS ANALYSIS:

- handler(
  ctx: Context<Withdraw>,
  shares_amount: u64
)
  Vulnerabilities not detected

STRUCTURE OF CONTRACT

YVAULTS/PROGRAMS/YVAULTS/SRC/INSTRUCTIONS/UPDATE_REWARD_MAPPING.RS

CONTRACT METHODS ANALYSIS:

- handler(
  ctx: Context<UpdateRewardMapping>,
  reward_id: u8,
  collateral_token: u8,
)
  Vulnerabilities not detected

STRUCTURE OF CONTRACT

YVAULTS/PROGRAMS/YVAULTS/SRC/INSTRUCTIONS/ORCA_SWAP.RS

CONTRACT METHODS ANALYSIS:

- handler(
  ctx: Context<OrcaSwap>,
  amount: u64,
  other_amount_threshold: u64,
  sqrt_price_limit: u128,
  amount_specified_is_input: bool,
  a_to_b: bool,
)
  Vulnerabilities not detected

STRUCTURE OF CONTRACT

YVAULTS/PROGRAMS/YVAULTS/SRC/INSTRUCTIONS/DEPOSIT.RS

CONTRACT METHODS ANALYSIS:

- handler(
  ctx: Context<Deposit>,
  max_a: u64,
  max_b: u64
)
  Vulnerabilities not detected

- get_prices(
  scope_account: &AccountInfo,
  strategy: &mut WhirlpoolStrategy,
)
  Vulnerabilities not detected

- get_prices_with_scope(
  scope_prices: &OraclePrices,
  strategy: &WhirlpoolStrategy,
  current_slot: u64,
)
  Vulnerabilities not detected

STRUCTURE OF CONTRACT

YVAULTS/PROGRAMS/YVAULTS/SRC/INSTRUCTIONS/UPDATE_GLOBAL_CONFIG.RS

CONTRACT METHODS ANALYSIS:

- handler(
  ctx: Context<UpdateGlobalConfig>,
  key: u16,
  index: u16,
  value: &[u8; VALUE_BYTE_ARRAY_LEN],
)
  Vulnerabilities not detected

STRUCTURE OF CONTRACT

YVAULTS/PROGRAMS/YVAULTS/SRC/INSTRUCTIONS/UPDATE_STRATEGY_CONFIG.RS

CONTRACT METHODS ANALYSIS:

- handler(ctx: Context<UpdateStrategyConfig>)
  Vulnerabilities not detected

STRUCTURE OF CONTRACT

YVAULTS/PROGRAMS/YVAULTS/SRC/INSTRUCTIONS/UPDATE_ADMIN_AUTHORITY.RS

CONTRACT METHODS ANALYSIS:

- handler(ctx: Context<UpdateAdminAuthority>)
  Vulnerabilities not detected

STRUCTURE OF CONTRACT

YVAULTS/PROGRAMS/YVAULTS/SRC/INSTRUCTIONS/EXECUTIVE_WITHDRAW.RS

CONTRACT METHODS ANALYSIS:

- handler(
  ctx: Context<ExecutiveWithdraw>,
  action: u8
)
  Vulnerabilities not detected

CONTRACT METHODS ANALYSIS:

- `handler(ctx: Context<Invest>)`
  Vulnerabilities not detected

STRUCTURE OF CONTRACT

YVAULTS/PROGRAMS/YVAULTS/SRC/INSTRUCTIONS/INVEST.RS

STRUCTURE OF CONTRACT

YVAULTS/PROGRAMS/YVAULTS/SRC/INSTRUCTIONS/SWAP_REWARDS.RS

CONTRACT METHODS ANALYSIS:

- handler(
  ctx: Context<SwapRewards>,
  token_a_in: u64,
  token_b_in: u64,
  reward_collateral_id: u8,
  min_collateral_token_out: u64,
)
  Vulnerabilities not detected

- transfer_fees_to_treasury_vault(
  ctx: &Context<SwapRewards>,
  bump: u8,
  a_amount: u64,
  b_amount: u64,
)
  Vulnerabilities not detected

STRUCTURE OF CONTRACT

YVAULTS/PROGRAMS/YVAULTS/SRC/INSTRUCTIONS/COLLECT_REWARDS.RS

CONTRACT METHODS ANALYSIS:

- handler(ctx: Context<CollectRewards>)
  Vulnerabilities not detected

- reward_vault(
      ctx: &Context<CollectRewards>, reward_
      index: usize
)
  Vulnerabilities not detected

- strategy_reward_vault(
      whirlpool_strategy: &WhirlpoolStrategy,
      reward_index: usize,
)
  Vulnerabilities not detected

- whirlpool_reward_vault(
      ctx: &Context<CollectRewards>,
      reward_index: usize,
)
  Vulnerabilities not detected

STRUCTURE OF CONTRACT

YVAULTS/PROGRAMS/YVAULTS/SRC/INSTRUCTIONS/DEPOSIT_AND_INVEST.RS

CONTRACT METHODS ANALYSIS:

- handler(
  ctx: Context<DepositAndInvest>,
  max_a: u64,
  max_b: u64
)
  Vulnerabilities not detected

- get_prices(
  scope_account: &AccountInfo,
  strategy: &mut WhirlpoolStrategy,
)
  Vulnerabilities not detected

- get_prices_with_scope(
  scope_prices: &OraclePrices,
  strategy: &WhirlpoolStrategy,
  current_slot: u64,
)
  Vulnerabilities not detected

STRUCTURE OF CONTRACT

YVAULTS/PROGRAMS/YVAULTS/SRC/INSTRUCTIONS/INITIALIZE_GLOBAL_CONFIG.RS

CONTRACT METHODS ANALYSIS:

- handler(ctx: Context<InitializeGlobalConfig>)
  Vulnerabilities not detected

STRUCTURE OF CONTRACT

YVAULTS/PROGRAMS/YVAULTS/SRC/INSTRUCTIONS/UPDATE_TREASURY_FEE_VAULT.RS

CONTRACT METHODS ANALYSIS:

- handler(
  ctx: Context<UpdateTreasuryFeeVault>,
  collateral_id: u16
)
  Vulnerabilities not detected

STRUCTURE OF CONTRACT

YVAULTS/PROGRAMS/YVAULTS/SRC/CONFIG/GLOBAL_CONFIG_OPERATIONS.RS

CONTRACT METHODS ANALYSIS:

- initialize(
  global_config: &mut GlobalConfig,
  admin_authority: Pubkey
)
  Vulnerabilities not detected

- update_u64_config(
  global_config: &mut GlobalConfig,
  key: GlobalConfigOption,
  value: u64,
)
  Vulnerabilities not detected

- update_treasury_fee_vault(
  global_config: &mut GlobalConfig,
  treasury_fee_vault: &Pubkey,
  collateral_id: u16,
)
  Vulnerabilities not detected

STRUCTURE OF CONTRACT

YVAULTS/PROGRAMS/YVAULTS/SRC/UTILS/ASSERTIONS.RS

CONTRACT METHODS ANALYSIS:

- require(
  value: bool,
  err: VaultError
)
  Vulnerabilities not detected

CONTRACT METHODS ANALYSIS:

- u8_to_bool(v: u8)
  Vulnerabilities not detected

STRUCTURE OF CONTRACT

YVAULTS/PROGRAMS/YVAULTS/SRC/UTILS/TYPES.RS

STRUCTURE OF CONTRACT

YVAULTS/PROGRAMS/YVAULTS/SRC/UTILS/ORCA_OPERATIONS.RS

CONTRACT METHODS ANALYSIS:

- cpi_collect_fees(
  ctx: &Context<CollectFees>,
  base_vault_authority_bump: u8
)
  Vulnerabilities not detected

- cpi_collect_rewards(
  ctx: &Context<CollectRewards>,
  base_vault_authority_bump: u8,
  token_a_vault: Pubkey,
  token_b_vault: Pubkey,
  reward_index: usize,
)
  Vulnerabilities not detected

- cpi_update_fees_and_rewards_fees_ix(ctx: &Context<CollectFees>)
  Vulnerabilities not detected

- cpi_update_fees_and_rewards_rewards_ix(ctx: &Context<CollectRewards>)
  Vulnerabilities not detected

- cpi_increase_liquidity_orca_deposit_and_invest(
  ctx: &Context<DepositAndInvest>,
  base_vault_authority_bump: u8,
  liquidity_amount: u128,
  token_max_a: u64,
  token_max_b: u64,
)

  Vulnerabilities not detected

- cpi_increase_liquidity_orca(
  ctx: &Context<Invest>,
  base_vault_authority_bump: u8,
  liquidity_amount: u128,
  token_max_a: u64,
  token_max_b: u64,
)

  Vulnerabilities not detected

- cpi_swap_uneven_vaults_orca(
  ctx: &Context<SwapUnevenVaults>,
  strategy: &mut WhirlpoolStrategy,
  effects: &SwapUnevenVaultsEffects,
)

  Vulnerabilities not detected

- cpi_decrease_liquidity_orca(
  ctx: &Context<ExecutiveWithdraw>,
  base_vault_authority_bump: u8,
  liquidity_amount: u128,
  token_min_a: u64,
  token_min_b: u64,
)

  Vulnerabilities not detected

- cpi_decrease_liquidity_orca_user(
  ctx: &Context<Withdraw>,
  base_vault_authority_bump: u8,
  liquidity_amount: u128,
  token_min_a: u64,
  token_min_b: u64,
)

  Vulnerabilities not detected

- cpi_open_position_orca(
  ctx: &Context<OpenLiquidityPosition>,
  tick_lower_index: i32,
  tick_upper_index: i32,
  position_bump: u8,
)

  Vulnerabilities not detected

- cpi_orca_swap(
  ctx: Context<OrcaSwap>,
  amount: u64,
  other_amount_threshold: u64,
  sqrt_price_limit: u128,
  amount_specified_is_input: bool,
  a_to_b: bool,
)

  Vulnerabilities not detected

- vault_amount(
  ctx: &Context<CollectRewards>,
  reward_index: usize
)

  Vulnerabilities not detected

STRUCTURE OF CONTRACT

YVAULTS/PROGRAMS/YVAULTS/SRC/UTILS/ENUMS.RS

CONTRACT METHODS ANALYSIS:

- from(x: LiquidityCalculationMode)
  Vulnerabilities not detected

STRUCTURE OF CONTRACT

YVAULTS/PROGRAMS/YVAULTS/SRC/UTILS/SCOPE.RS

CONTRACT METHODS ANALYSIS:

- get_price_account<'a, 'info>(scope_price_account: &'a AccountInfo<'info>,)
  Vulnerabilities not detected
- get_price_account_from_account_data(data: &[u8])
  Vulnerabilities not detected
- get_price_usd(
  scope_prices: &ScopePrices,
  token: impl TryInto<ScopeConversionChain>,
  current_slot: clock::Slot,
)
  Vulnerabilities not detected

- `get_price(`
  `scope_prices: &ScopePrices,`
  `token: impl TryInto<ScopePriceId>,`
  `current_slot: clock::Slot,`
  `)`

  Vulnerabilities not detected

- `get_price_max_age(token: ScopePriceId)`

  Vulnerabilities not detected

- `get_prices(`
  `scope_prices: &AccountInfo,`
  `strategy: &mut WhirlpoolStrategy,`
  `)`

  Vulnerabilities not detected

STRUCTURE OF CONTRACT

YVAULTS/PROGRAMS/YVAULTS/SRC/UTILS/SHARES.RS

CONTRACT METHODS ANALYSIS:

- mint<'info>(
  token_program: AccountInfo<'info>,
  shares_mint: AccountInfo<'info>,
  shares_mint_authority: AccountInfo<'info>,
  user_shares_ata: AccountInfo<'info>,
  shares_authority_bump: u64,
  shares_to_mint: u64,
)
  Vulnerabilities not detected

- burn<'info>(
  shares_mint: AccountInfo<'info>,
  user_shares_ata: AccountInfo<'info>,
  user: AccountInfo<'info>,
  token_program: AccountInfo<'info>,
  shares_to_burn: u64,
)
  Vulnerabilities not detected

STRUCTURE OF CONTRACT

YVAULTS/PROGRAMS/YVAULTS/SRC/UTILS/PRICE.RS

CONTRACT METHODS ANALYSIS:

- calc_market_value_token_usd<'a>(
  amount: u64,
  price: impl Into<Option<&'a Price>>,
  token_decimals: u8,
)
  Vulnerabilities not detected

- calc_token_amount_from_usd_value<'a>(
  usd_value: u64,
  price: impl Into<Option<&'a Price>>,
  token_decimals: u8,
)
  Vulnerabilities not detected

- calc_scaled_a_to_b_price(price_a: &Price, price_b: &Price)
  Vulnerabilities not detected

- ten_pow(exponent: u8)
  Vulnerabilities not detected

STRUCTURE OF CONTRACT

YVAULTS/PROGRAMS/YVAULTS/SRC/UTILS/CLMM_CALCS.RS

CONTRACT METHODS ANALYSIS:

- get_amount_b_for_liquidity(
  mut sqrt_price_a: u128,
  mut sqrt_price_b: u128,
  liquidity: u128,
  round_up: bool,
)
  Vulnerabilities not detected

- get_amount_a_for_liquidity(
  mut sqrt_price_a: u128,
  mut sqrt_price_b: u128,
  liquidity: u128,
  round_up: bool,
)
  Vulnerabilities not detected

- get_amounts_for_liquidity(
  current_sqrt_price: u128,
  mut sqrt_price_a: u128,
  mut sqrt_price_b: u128,
  liquidity: u128,
  mode: LiquidityCalculationMode,
)

  Vulnerabilities not detected

- get_liquidity_for_amount_a(
  amount: u64,
  mut sqrt_price_a: u128,
  mut sqrt_price_b: u128,
  round_up: bool,
)

  Vulnerabilities not detected

- get_liquidity_for_amount_b(
  amount: u64,
  mut sqrt_price_a: u128,
  mut sqrt_price_b: u128,
  round_up: bool,
)

  Vulnerabilities not detected

- get_liquidity_for_amounts(
  current_sqrt_price: u128,
  mut sqrt_price_a: u128,
  mut sqrt_price_b: u128,
  amount_a: u64,
  amount_b: u64,
  round_up: bool,
)

  Vulnerabilities not detected

- quote_position_add_liquidity(
  is_token_a: bool,
  current_sqrt_price: u128,
  sqrt_price_lower: u128,
  sqrt_price_upper: u128,
  amount: u64,
  slippage_tolerance_bps: u64,
)

  Vulnerabilities not detected

- quote_position_add_liquidity_below_range(
  is_token_a: bool,
  sqrt_price_lower: u128,
  sqrt_price_upper: u128,
  amt: u64,
  slippage: u64,
)

  Vulnerabilities not detected

- quote_position_add_liquidity_above_range(
  is_token_a: bool,
  sqrt_price_lower: u128,
  sqrt_price_upper: u128,
  amount: u64,
  slippage: u64,
)

  Vulnerabilities not detected

- quote_position_add_liquidity_in_range(
  is_token_a: bool,
  sqrt_price: u128,
  sqrt_price_lower: u128,
  sqrt_price_upper: u128,
  input_amount: u64,
  slippage_tolerance_bps: u64,
)

  Vulnerabilities not detected

- quote_position_remove_liquidity(
  liquidity: u128,
  current_sqrt_price: u128,
  sqrt_price_lower: u128,
  sqrt_price_upper: u128,
  slippage_tolerance_bps: u64,
)

  Vulnerabilities not detected

- quote_position_remove_liquidity_below_range(
  liquidity: u128,
  sqrt_price_lower: u128,
  sqrt_price_upper: u128,
  slippage: u64,
)

  Vulnerabilities not detected

- quote_position_remove_liquidity_above_range(
  liquidity: u128,
  sqrt_price_lower: u128,
  sqrt_price_upper: u128,
  slippage: u64,
)

  Vulnerabilities not detected

- quote_position_remove_liquidity_in_range(
  liquidity: u128,
  sqrt_price: u128,
  sqrt_price_lower: u128,
  sqrt_price_upper: u128,
  slippage_tolerance_bps: u64,
)

  Vulnerabilities not detected

- adjust_for_slippage(
  amount: u128,
  slippage: u64,
  round_up: bool
)

  Vulnerabilities not detected

- max_investable_at_price(
  position: &Position,
  available_a: u64,
  available_b: u64,
  current_sqrt_price: u128,
  slippage_tolerance_bps: u64,
)

  Vulnerabilities not detected

- div_round_up(
    n: U192,
    d: U192
)
  Vulnerabilities not detected

- div_round_up_if(
    n: U192,
    d: U192,
    round_up: bool
)
  Vulnerabilities not detected

- calc_sqrt_price_from_price(price: f64)
  Vulnerabilities not detected

- calc_price_from_sqrt_price(price: u128)
  Vulnerabilities not detected

- calc_price_from_tick_index(tick_index: i32)
  Vulnerabilities not detected

- get_p_value(bps: u16)
  Vulnerabilities not detected

- price_range_of_index(
    i: i32,
    bps: u16
) -> (f64, f64)
  Vulnerabilities not detected

- tick_index_of_price(
    price: f64,
    bps: u16
)
  Vulnerabilities not detected

- tick_index_of_sqrt_price(
    sqrt_price: u128,
    bps: u16
)
  Vulnerabilities not detected

- get_start_tick_index(
    tick_index: i32,
    tick_spacing: i32,
    offset: Option<i32>
)
  Vulnerabilities not detected

- default_sqrt_price_limit(a_to_b: bool)
  Vulnerabilities not detected

- sqrt_price_limit_slippage_adjusted(
    sqrt_price: u128,
    a_to_b: bool,
    max_slippage: u64,
)
  Vulnerabilities not detected

- get_tick_array_pubkeys_for_swap(
    current_tick_index: i32,
    tick_spacing: u16,
    a_to_b: bool,
    whirlpool: &Pubkey,
)
  Vulnerabilities not detected

- pda_util_get_tick_array(
    program_id: &Pubkey,
    pool_address: &Pubkey,
    tick_index: i32,
)
  Vulnerabilities not detected

- get_amount_to_swap_a(
    available_a: U192,
    available_b: U192,
    min_token_a: U192,
    min_token_b: U192,
    sqrt_price: U192,
)
  Vulnerabilities not detected

- get_amount_to_swap_b(
    available_a: U192,
    available_b: U192,
    min_token_a: U192,
    min_token_b: U192,
    sqrt_price: U192,
)
  Vulnerabilities not detected

STRUCTURE OF CONTRACT

YVAULTS/PROGRAMS/YVAULTS/SRC/UTILS/MATH.RS

CONTRACT METHODS ANALYSIS:

- mul_fraction<T: Copy + CheckedHubbleOps + From<u64>>(
  amount: T,
  numerator: &T,
  denominator: &T,
)
  Vulnerabilities not detected
- mul_fraction_u192(
  amount: U192,
  numerator: U192,
  denominator: U192
)
  Vulnerabilities not detected
- mul_bps_u192(
  amount: U192,
  bps: u64
)
  Vulnerabilities not detected
- mul_pct<T: Copy + CheckedHubbleOps + From<u64>>(
  amount: T,
  pct: T
)
  Vulnerabilities not detected
- mul_bps<T: Copy + CheckedHubbleOps + From<u64>>(
  amount: T,
  bps: T
)
  Vulnerabilities not detected

STRUCTURE OF CONTRACT

YVAULTS/PROGRAMS/YVAULTS/SRC/OPERATIONS/VAULT_OPERATIONS.RS

CONTRACT METHODS ANALYSIS:

- `open_position(strategy: &mut WhirlpoolStrategy)`
  Vulnerabilities not detected

- `deposit(`
  `strategy: &mut WhirlpoolStrategy,`
  `whirlpool: &Whirlpool,`
  `position: &Position,`
  `prices: &TokenPrices,`
  `max_a_amount: u64,`
  `max_b_amount: u64,`
  `curr_timestamp: i64,`
  `)`
  Vulnerabilities not detected

- swap_reward(
    strategy: &mut WhirlpoolStrategy,
    config: &GlobalConfig,
    prices: &TokenPrices,
    token_a_in: u64,
    token_b_in: u64,
    reward_collateral_id: u8,
    min_collateral_token_out: u64,
)
  Vulnerabilities not detected

- swap_uneven_vaults(
    strategy: &WhirlpoolStrategy,
    whirlpool: &Whirlpool,
    position: &Position,
    prices: &TokenPrices,
    slippage: u64,
)
  Vulnerabilities not detected

- withdraw(
    strategy: &mut WhirlpoolStrategy,
    whirlpool: &Whirlpool,
    position: &Position,
    number_of_shares: u64,
    slippage: u64,
    curr_timestamp: i64,
)
  Vulnerabilities not detected

- executive_unfreeze(strategy: &mut WhirlpoolStrategy)
  Vulnerabilities not detected

- executive_withdraw(
    strategy: &mut WhirlpoolStrategy,
    whirlpool: &Whirlpool,
    position: &Position,
    action: &ExecutiveWithdrawAction,
    slippage: u64,
)

  Vulnerabilities not detected

- invest(
    strategy: &mut WhirlpoolStrategy,
    whirlpool: &Whirlpool,
    position: &Position,
    slippage_tolerance_bps: u64,
)

  Vulnerabilities not detected

- collect_fees(
    strategy: &mut WhirlpoolStrategy,
    position: &Position,
)

  Vulnerabilities not detected

- collect_rewards(
    strategy: &mut WhirlpoolStrategy,
    reward_0: u64,
    reward_1: u64,
    reward_2: u64,
)

  Vulnerabilities not detected

- pct_of_amounts(
      numerator: u64,
      denominator: u64,
      amounts: TokenAmounts,
)

  Vulnerabilities not detected

- get_percentage_of_amount(
  numerator: u64,
  denominator: u64,
  amount: u64,
)

  Vulnerabilities not detected

- get_price_per_full_share_impl(
  holdings: &Holdings,
  shares_issued: u64,
  shares_decimals: u64,
)

  Vulnerabilities not detected

- get_price_per_full_share(
  strategy: &WhirlpoolStrategy,
  whirlpool: &Whirlpool,
  position: &Position,
  prices: &TokenPrices,
)

  Vulnerabilities not detected

- underlying_unit(share_decimals: u64)

  Vulnerabilities not detected

- amounts_invested(
  whirlpool: &Whirlpool,
  position: &Position,
  mode: LiquidityCalculationMode,
)

  Vulnerabilities not detected

- amounts_usd_token(
  strategy: &WhirlpoolStrategy,
  token_amount: u64,
  is_a: bool,
  prices: &TokenPrices,
)

  Vulnerabilities not detected

- pending_fees(position: &Position)
  Vulnerabilities not detected

- pending_rewards(
    position: &Position,
    whirlpool: &Whirlpool
)
  Vulnerabilities not detected

- amounts_usd(
    strategy: &WhirlpoolStrategy,
    amounts: &TokenAmounts,
    prices: &TokenPrices,
)
  Vulnerabilities not detected

- reward_amount_usd(
    strategy: &WhirlpoolStrategy,
    amount: u64,
    prices: &TokenPrices,
    reward_collateral_id: u8,
)
  Vulnerabilities not detected

- rewards_total_usd_value(
    strategy: &WhirlpoolStrategy,
    rewards: &RewardsAmounts,
    prices: &TokenPrices,
)
  Vulnerabilities not detected

- amounts_available(strategy: &WhirlpoolStrategy)
  Vulnerabilities not detected

- holdings_usd(
    strategy: &WhirlpoolStrategy,
    available: TokenAmounts,
    invested: TokenAmounts,
    fees: TokenAmounts,
    rewards: RewardsAmounts,
    prices: &TokenPrices,
)
  Vulnerabilities not detected

- holdings(
  strategy: &WhirlpoolStrategy,
  whirlpool: &Whirlpool,
  position: &Position,
  prices: &TokenPrices,
  mode: LiquidityCalculationMode,
)

  Vulnerabilities not detected

- available_to_invest(strategy: &WhirlpoolStrategy) -> Result<(u64, u64),>

  Vulnerabilities not detected

- deposit_into_strategy(
  strategy: &mut WhirlpoolStrategy,
  a: u64,
  b: u64,
)

  Vulnerabilities not detected

- remove_reward(
  strategy: &mut WhirlpoolStrategy,
  reward_amount: u64,
  reward_collateral_id: u8,
)

  Vulnerabilities not detected

- withdraw_from_strategy(
  strategy: &mut WhirlpoolStrategy,
  a: u64,
  b: u64,
)

  Vulnerabilities not detected

- burn_shares(
  strategy: &mut WhirlpoolStrategy,
  amt: u64,
)

  Vulnerabilities not detected

- mint_shares(
  strategy: &mut WhirlpoolStrategy,
  amt: u64
)

  Vulnerabilities not detected

- strategy_reward_index(
  strategy: &WhirlpoolStrategy,
  reward_collateral_id: u8,
)

  Vulnerabilities not detected

- strategy_reward_vault(
  strategy: &WhirlpoolStrategy,
  reward_collateral_id: u8,
)

  Vulnerabilities not detected

- strategy_reward_amount(
  strategy: &mut WhirlpoolStrategy,
  reward_collateral_id: u8,
)

  Vulnerabilities not detected

- strategy_reward_decimals(
  strategy: &WhirlpoolStrategy,
  reward_collateral_id: u8,
)

  Vulnerabilities not detected

- assert_can_deposit_token_amount(
  strategy: &WhirlpoolStrategy,
  current_total_usd: U128,
  deposit_amount_usd: U128,
)

  Vulnerabilities not detected

- assert_strategy_in_range(
  position: &Position,
  whirlpool: &Whirlpool,
  err: VaultError,
)

  Vulnerabilities not detected

- assert_valid_orca_price(
  strategy: &WhirlpoolStrategy,
  prices: &TokenPrices,
  sqrt_orca_price: U192,
)

  Vulnerabilities not detected

STRUCTURE OF CONTRACT

YVAULTS/PROGRAMS/YVAULTS/SRC/OPERATIONS/FEES.RS

CONTRACT METHODS ANALYSIS:

- compute_generic_split(
  total_token_amount: u64,
  protocol_fee: u64,
)
  Vulnerabilities not detected

- compute_deposit_split(
  strategy: &WhirlpoolStrategy,
  token_a_amount: u64,
  token_b_amount: u64,
)
  Vulnerabilities not detected

- compute_withdraw_split(
  strategy: &WhirlpoolStrategy,
  token_a_to_withdraw: u64,
  token_b_to_withdraw: u64,
  token_a_to_disinvest: u64,
  token_b_to_disinvest: u64,
)
  Vulnerabilities not detected

- compute_fees_split(
    strategy: &WhirlpoolStrategy,
    token_a_amount: u64,
    token_b_amount: u64,
)
  Vulnerabilities not detected

- compute_rewards_split(
    strategy: &WhirlpoolStrategy,
    token_a_amount: u64,
    token_b_amount: u64,
    reward_collateral_id: u8,
)
  Vulnerabilities not detected

STRUCTURE OF CONTRACT

YVAULTS/PROGRAMS/YVAULTS/SRC/COMPONENTS/WITHDRAWAL_CAP_OPERATIONS.RS

CONTRACT METHODS ANALYSIS:

- update_counter(
  caps: &mut WithdrawalCaps,
  requested_amount: u64,
  action: WithdrawalCapAction,
  overflow_action: WithdrawalCapOverflowAction,
)
  Vulnerabilities not detected

- check_capacity_allows_withdrawals(
  caps: &mut WithdrawalCaps,
  requested_amount: u64,
)
  Vulnerabilities not detected

- check_last_interval_elapsed(
  caps: &mut WithdrawalCaps,
  curr_timestamp: u64,
)
  Vulnerabilities not detected

- add_to_withdrawal_accum(
  caps: &mut WithdrawalCaps,
  requested_amount: u64,
  curr_timestamp: u64,
)
  Vulnerabilities not detected

- sub_from_withdrawal_accum(
  caps: &mut WithdrawalCaps,
  requested_amount: u64,
  curr_timestamp: u64,
)
  Vulnerabilities not detected

- check_and_update_withdrawal_caps(
  caps: &mut WithdrawalCaps,
  requested_amount: u64,
  curr_timestamp: u64,
  action: WithdrawalCapAction,
)
  Vulnerabilities not detected

- change_withdrawal_cap(
  caps: &mut WithdrawalCaps,
  new_amount: u64,
  interval: u64,
  accum_action:
  WithdrawalCapAccumulatorAction,
)
  Vulnerabilities not detected

- initialize_withdrawal_cap(caps: &mut WithdrawalCaps)
  Vulnerabilities not detected

VERIFICATION CHECK SUMS

Contract Name	Bytecode hash (SHA 256)
yvaults/programs/yvaults/src/lib.rs	04c1bd299c992d348fc947c9d77525ea9a9ae91ac23f88dc80c89e6a6074ea7c
yvaults/programs/yvaults/src/orca_state.rs	54748eff9fa926c1a475e2d82f5c0bd661b6d8be819e8b68431fd9fca729db4d
yvaults/programs/yvaults/src/instructions/swap_uneven_vaults.rs	33c9ba471b7b63082ce9ea6599a3fe9d4502e81121ffa2843d193e4015ef299d
yvaults/programs/yvaults/src/instructions/collect_fees.rs	4e8baebba74823b3cf4a3ab7817b71184a121c33546a6052e8ae827dead6192d
yvaults/programs/yvaults/src/instructions/withdraw.rs	c1a242c1d7cf4e6223edf03f68a34e51a6e51462b826a3932e0cab89f393c7f9
yvaults/programs/yvaults/src/instructions/update_reward_mapping.rs	ed3bd80426c226f1c82f30d41c9061fe90e4d6d49ed9ae089240e957dd7481ed

Contract Name	Bytecode hash (SHA 256)
yvaults/programs/yvaults/src/instructions/orca_swap.rs	f2c4b0720aa9682cfc1ba5feeefd51cc2ad0221b35ca1a148eaf8e013502e485
yvaults/programs/yvaults/src/instructions/deposit.rs	f2dbd6d723b89aa3c28078a025ab6b480c06999d00be21fd1d2b3fbc703d2612
yvaults/programs/yvaults/src/instructions/update_global_config.rs	58d963105b61222def1157fcbd649a84295872442904a67250419a726f662bf1
yvaults/programs/yvaults/src/instructions/update_strategy_config.rs	23b87fd0dea9bc84a957762ff1c98ec1a7aa417d3230a6f2e133f8bbb61b55ca
yvaults/programs/yvaults/src/instructions/update_admin_authority.rs	be4fbfe1f6acc78ad342c7ab3af06ba1354fdbd51d27d5a9c8ddba3ec0a32972
yvaults/programs/yvaults/src/instructions/executive_withdraw.rs	42d41bbfbb2b25c3633b14f5338dc42d06f52efde6c8a93aa1a224334b0030e2

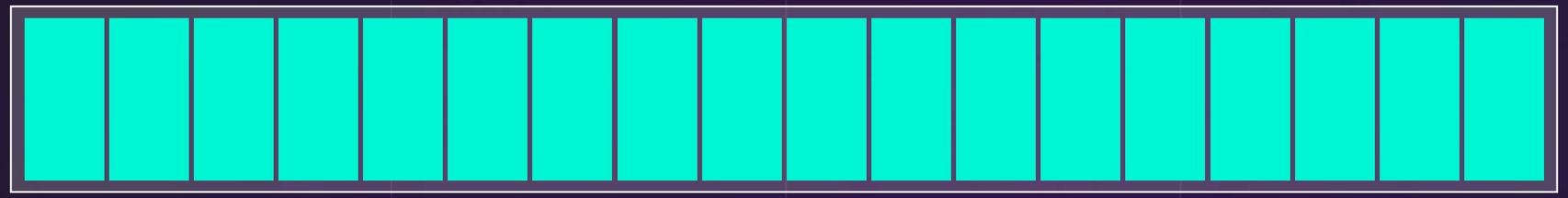
Contract Name	Bytecode hash (SHA 256)
yvaults/programs/yvaults/src/instructions/invest.rs	f736d8041cff050342633c2af0301d40a7364653c0e86ec8041e541179f58792
yvaults/programs/yvaults/src/instructions/swap_rewards.rs	c0c86f07d11c038ae0ee3a181b078e67b6e2ebefe44011aff8eafd42c0cddf8b
yvaults/programs/yvaults/src/instructions/collect_rewards.rs	fc309c2b1b730e1967f46515ab5455f75c39c28c6e29c4fbe602084f874913b9
yvaults/programs/yvaults/src/instructions/deposit_and_invest.rs	0b84c0978ab4093e91fd5c8ff7f4b5043e643bebd2a2da2b00222cd3afe4504a
yvaults/programs/yvaults/src/instructions/initialize_global_config.rs	fc23d610eb5ed7e14d1795083b13b9c62a6e2d91c338bf8caf4987d78cf517ae
yvaults/programs/yvaults/src/instructions/update_treasury_fee_vault.rs	5e7f518f00d9b64178a809893d9c4558ac8aeed6e6dee3da6408f086c63661c7

Contract Name	Bytecode hash (SHA 256)
yvaults/programs/yvaults/src/config/global_config_operations.rs	a299278da00b690e2f98349b10e2b929de186d5db81b64c35a36fcd2904bf7d7
yvaults/programs/yvaults/src/utils/assertions.rs	3125f6886d91fd61648cc6d6c18ac309c8132175d2c380942a51020db08722ec
yvaults/programs/yvaults/src/utils/types.rs	0bfc1c797f33697886bd6c54ea0f8ac6b477a7692fa078138c9fce7c256ee92e
yvaults/programs/yvaults/src/utils/orca_operations.rs	070e3c16e75b0b910722a8ffb1bf815fe50688f6a42f309fc29c34104513f055
yvaults/programs/yvaults/src/utils/enums.rs	ba3a9acf636468d490d4cd847ca51efd74097463be885a4eb035a271cea8b249
yvaults/programs/yvaults/src/utils/scope.rs	cf7fd980a3ddc7c106bca6254048c3f99b661c0b42ad80f9f3afa2b03b5ce542

Contract Name	Bytecode hash (SHA 256)
yvaults/programs/yvaults/src/utils/shares.rs	a88fdc47005bef1247a22b758b071f8babd5d7e21967aa06e0fa80592689e9af
yvaults/programs/yvaults/src/utils/price.rs	98d7ab89c3e605e2d8d44680455edff056b5a17864fe278e632652983b72dbf4
yvaults/programs/yvaults/src/utils/clmm_calcs.rs	337cb86829a021767766ed91e82f7824caaa2fad80f67074996de046aeaac8dc
yvaults/programs/yvaults/src/utils/math.rs	009f203c7367a26279b859aa31200af85e60ca6273906216be18a3431a2ad4bd
yvaults/programs/yvaults/src/operations/vault_operations.rs	c8c74ea07b8bc12e6db6503ca8f82b13bea124d047ff01f084dfbc48e1d73d2a
yvaults/programs/yvaults/src/operations/fees.rs	4a60c1e39ac2d546c3c28a6ae7a650bebc9aa3d5e5cb504a84704402c209d184

Contract Name	Bytecode hash (SHA 256)
yvaults/programs/yvaults/src/components/withdrawal_cap_operations.rs	f37a1ab3cfc8db5609a4bf73b43c57a561816d07547c2a85291af1cd98de111a

PROJECT EVALUATION



10/10

smart state

GET IN TOUCH

info@smartstate.tech
smartstate.tech

View this report on smartstate.tech