smart state

> Smart Contract Audit

CRYOWAR

KILL WITH SKILL

Jan 25
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
- 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

ENTRYPOINT.RS

CONTRACT METHODS ANALYSIS:

-
  ```
  process_instruction(
    program_id: &Pubkey,
    accounts: &[AccountInfo],
    instruction_data: &[u8],
  )
  ```
  Vulnerabilities not detected

STRUCTURE OF CONTRACT

INSTRUCTION.RS

CONTRACT METHODS ANALYSIS:

- unpack(input: &[u8])
  Vulnerabilities not detected
- unpack_to_u64(input: &[u8])
  Vulnerabilities not detected

STRUCTURE OF CONTRACT

PROCESSOR.RS

CONTRACT METHODS ANALYSIS:

-
  ```
  process(
        program_id: &Pubkey,
        accounts: &[AccountInfo],
        instruction_data: &[u8],
    )
  ```
  Vulnerabilities not detected

STRUCTURE OF CONTRACT

UTILS.RS

CONTRACT METHODS ANALYSIS:

-
  ```
  close_account(
    account_to_close: &AccountInfo,
    sol_receiving_account: &AccountInfo,
    account_to_close_data_byte_array: &mut
  RefMut<&mut [u8]>,
  )
  ```
  Vulnerabilities not detected

-
  ```
  rewards_per_token(
    total_cwar_staked: u64,
    last_time_reward_applicable: u64,
    total_stake_last_update_time: u64,
    cwar_reward_rate: u64,
    cwar_reward_per_token_stored: u128,
  )
  ```
  Vulnerabilities not detected

-
  ```
  earned(
    balance_cwar_staked: u64,
    reward_per_token_stored: u128,
    reward_per_token_complete: u128,
    reward_per_token_pending: u64,
  )
  ```
  Vulnerabilities not detected

-
  ```
  update_rewards(
    cwar_pool: &mut CwarPool,
    user: Option<&mut User>,
    total_cwar_staked: u64,
  )
  ```
  Vulnerabilities not detected

-
  ```
  last_time_reward_applicable(reward_duration_end: u64, now_unix_timestamp: i64)
  ```
  Vulnerabilities not detected

STRUCTURE OF CONTRACT

PROCESSOR/ADD_FUNDER.RS

CONTRACT METHODS ANALYSIS:

- process_add_funder(accounts: &[AccountInfo])
  Vulnerabilities not detected

STRUCTURE OF CONTRACT

PROCESSOR/CLAIM_REWARDS.RS

CONTRACT METHODS ANALYSIS:

PAYABLE

- process_close_pool(accounts: &[AccountInfo], program_id: &Pubkey)

  Vulnerabilities not detected

Tokens out, public

STRUCTURE OF CONTRACT

PROCESSOR/CLOSE_USER.RS

CONTRACT METHODS ANALYSIS:

Vulnerabilities not detected

STRUCTURE OF CONTRACT

PROCESSOR/CREATE_USER.RS

CONTRACT METHODS ANALYSIS:

-
  ```
  process_create_user(
    accounts: &[AccountInfo],
    nonce: u8,
    program_id: &Pubkey,
  )
  ```
  Vulnerabilities not detected

-
  ```
  create_and_allocate_account_raw<'a>(
    owner_program_id: Pubkey,
    new_account_info: &AccountInfo<'a>,
    system_program_info: &AccountInfo<'a>,
    payer_info: &AccountInfo<'a>,
    size: usize,
    signer_seeds: &[&[u8]],
  )
  ```
  Vulnerabilities not detected

```
◆ assert_derivation(
    program_id: &Pubkey,
    account: &AccountInfo,
    path: &[&[u8]],
  )
```

Vulnerabilities not detected

```
◆ get_user_storage_address(
    user_wallet: &Pubkey,
    pool_storage: &Pubkey,
    program_id: &Pubkey,
  )
```

Vulnerabilities not detected

```
◆ get_user_storage_address_and_bump_seed(
    user_wallet: &Pubkey,
    pool_storage: &Pubkey,
    program_id: &Pubkey,
  )
```

Vulnerabilities not detected

STRUCTURE OF CONTRACT

PROCESSOR/FUND_POOL.RS

CONTRACT METHODS ANALYSIS:

-
  ```
  process_fund_pool(
    accounts: &[AccountInfo],
    amount: u64,
    program_id: &Pubkey,
  )
  ```
  Vulnerabilities not detected

STRUCTURE OF CONTRACT

PROCESSOR/INITIALIZE_CWAR_POOL.RS

CONTRACT METHODS ANALYSIS:

-
  ```
  process_initialize_cwar_pool(
    accounts: &[AccountInfo],
    reward_duration: u64,
    pool_nonce: u8,
    program_id: &Pubkey,
  )
  ```
  Vulnerabilities not detected

STRUCTURE OF CONTRACT

PROCESSOR/REMOVE_FUNDER.RS

CONTRACT METHODS ANALYSIS:

PAYABLE

- process_remove_funder(accounts: &[AccountInfo])

Vulnerabilities not detected

Tokens in, only funder

STRUCTURE OF CONTRACT

PROCESSOR/STAKE_CWAR.RS

CONTRACT METHODS ANALYSIS:

PAYABLE

◆
```
process_stake_cwar(
   accounts: &[AccountInfo],
   amount_to_deposit: u64,
   program_id: &Pubkey,
)
```

Vulnerabilities not detected

Tokens in, public

STRUCTURE OF CONTRACT

PROCESSOR/
UNSTAKE_CWAR.RS

CONTRACT METHODS ANALYSIS:

PAYABLE

- process_unstake_cwar(
  accounts: &[AccountInfo],
  amount_to_withdraw: u64,
  program_id: &Pubkey,
)

Vulnerabilities not detected

Tokens out, public

STRUCTURE OF CONTRACT

PROCESSOR/CLOSE_POOL.RS

CONTRACT METHODS ANALYSIS:

- process_close_pool(accounts: &[AccountInfo], program_id: &Pubkey)
  Vulnerabilities not detected

VERIFICATION CHECK SUMS

Contract Name	Bytecode hash (SHA 256)
entrypoint.rs	b1a6a56820022d19fb4383073876abb6bb756cc7b711e078774ebfca14bd5c6d
instruction.rs	038f84c30c96fd6b3610433657f9fdf6d561c9c1037eafc8dfa5e46b5c887b01
processor.rs	568ad955a5ebea432a3a6fb80046966025c1c196a47662cbe9a8b15aa6bf9f9f
utils.rs	aeeee9ca77085e5fccb0b58714e3ae5177aa7589a6a3c0feb58d155d967c9dd8

Contract Name	Bytecode hash (SHA 256)
processor/add_funder.rs	9b6ce51089ab17674d709e2a9f51cd6533c5c23949c82205dbeb6de254f9e40d
processor/claim_rewards.rs	7fb45df0a30213227acaeae7f18fd986451af19ecd06f94a684a113d6436e889
processor/close_user.rs	440bff1a48f87bd71a09e14fd4bde30352f3f186370d5c72935d37d12bb3b000
processor/create_user.rs	3245db16d204af077bf5dacb31cfb964e3425fca2bb119891728e26e2cae62e0

Contract Name	Bytecode hash (SHA 256)
processor/fund_pool.rs	ebaae3c41d82a3081f6032aa1bab13598205e976668c778a39dc0085e612f326
processor/initialize_cwar_pool.rs	eaace4b18c7f179ffd449901ae80f7c13f351c8365c79bf73b65ee4cb349812f
processor/remove_funder.rs	4b19d64ead745856fe8c7b7d2874239a683f252dfd1120f1af72d184a535efad
processor/stake_cwar.rs	a6896736601995c269c47e2fdb81351252c2481766754994f1cc9b8e742dea82

Contract Name	Bytecode hash (SHA 256)
processor/unstake_cwar.rs	fd1086cc32a1f2cb37a5ad18c1129bc040543c094bc7b6d068dd98793a02d21e
processor/close_pool.rs	41b39236537d7ff909dd7419882c24700576de5de47dc08e45b6fee4911deb30

Get In Touch

info@smartstate.tech

smartstate.tech