Solana Top 10 Vulnerabilities

1. **Authority Mischecks:**

   #1 common vulnerability on Solana. Missing authentication of the authorities administering various program operations.

   CWE
   - Token account authorities (owner, delegate, close)
   - Program upgrade authority
   - Admin key spoofing setting program config parameters

2. **Account Validation**

   A program must check that all accounts are owned by programs and the associations stand. Absence of these checks opens up gateways for attackers to change account data in a faulty setting.

   CWE
   - Token account ownership
   - Missing has_one account validations (in Anchor framework)
   - NFT metadata and mint missing association checks

3. **Web 2.5 Vulnerabilities**

   API calls that build program transactions to validate the presence of a 3rd-party signer are vulnerable due to inconsistency of program specification across development teams.

   CWE
   - Unauthorized access to API
   - on-chain vs off-chain Access Control Rules (ACR) confusion

4. **Composability Issues**

   Composability through Cross Program Invocation (CPI) from program A to program B is common on Solana. Lack of detailed specification and expected behavior across programs is a common root cause for vulnerabilities.

   CWE
   - NFT metadata programs invalid account_metas during token operations (transfer, freeze, delegate)
   - DeFi aggregators and LP Vault strategies interacting with OpenBook/underlying trading markets

5. **Instruction Introspection Faults**

   Insufficient checks on the program_id, data, accounts and order of instructions in a transaction that usually happens through Sysvar instructions.

   CWE
   - Missing repayment instruction for Flash Loans
   - Invalid verification of NFT metadata during initialization

6. **Account Ownership Violation**

   Lack of proper account ownership verification allows attackers to exploit programs to read/write from/to incorrect accounts.

7. **Account reinitialization**

   Account reinitialization allows for an attacker to write data over the same account leading to arbitrary modification of the state.

   CWE
   - Missing init or zero constraints in Anchor.

8. **Non-Standard PDAs**

   The choice of seeds for PDAs have to be such that the account cannot be spoofed, duplicated to be used instead of the target intended account.

   CWE
   - Improper usage of nonce (not in order)
   - Extracanonical seeds for token accounts aside from the ATA program.

9. **Time to Create vs Time to Read/Write**

   Due to the compute budget limits on Solana, not all of the program instructions can be included into one transaction. Therefore, accounts can be created in one transaction and written/read from in another. The time difference between these transactions provides an opportunity for an attacker to interleave a malicious one hijacking the accounts.

   CWE
   - Token account creation and initialization
   - Temporary state storage between validation and transfer of tokens

10. Accounts in Vanilla Solana/ Remaining Accounts

Both accounts in vanilla Solana (without Anchor) and remaining accounts (with Anchor) are susceptible to vulnerabilities as the Account trait is not present to enforce the default anchor checks anymore.

CWE

- Discrepancy in the token accounts provided in the remaining accounts while transferring multiple token rewards for a staking/ LP incentive programs