# Findings in Detail

### IMPACT - CRITICAL
### [C-1] manipulate perpetual trade parameters and steal assets

When calling the following three unprivileged instructions

- mint_with_mango_depository
- redeem_from_mango_depository
- rebalance_mango_depository_lite

the following four accounts should be provided to indicate which perpetual market the users are dealing with.

```
/* programs/uxd/src/instructions/mango_dex/mint_with_mango_depository.rs */
043 | pub struct MintWithMangoDepository<'info> {
143 |     /// #16 [MangoMarkets CPI] `depository`'s `collateral_mint` perp market
144 |     #[account(mut)]
145 |     pub mango_perp_market: AccountInfo<'info>,
147 |     /// #17 [MangoMarkets CPI] `depository`'s `collateral_mint` perp market orderbook bids
148 |     #[account(mut)]
149 |     pub mango_bids: AccountInfo<'info>,
151 |     /// #18 [MangoMarkets CPI] `depository`'s `collateral_mint` perp market orderbook asks
152 |     #[account(mut)]
153 |     pub mango_asks: AccountInfo<'info>,
155 |     /// #19 [MangoMarkets CPI] `depository`'s `collateral_mint` perp market event queue
156 |     #[account(mut)]
157 |     pub mango_event_queue: AccountInfo<'info>,
173 | }
```

However, the existing checks on the mango_perp_market account are insufficient. It's possible to provide valid but inconsistent perp market accounts such that normal users can manipulate the perp order parameters and steal assets.

For example, when users interact with the ETH depository, to be consistent, the PERP-ETH mango perp market accounts are expected. However, as shown below, it's possible to use PERP-BTC or PERP-SOL related accounts and manipulate the transaction parameters.