There is a front-running exploit in the deposit contract that allows validator key holders to front-run withdrawal key holders and steal their funds. The exploit goes as follows:

1. “friendly staking service” (FSS) offers to run a validator for a user, with the user retaining access to their funds via the withdrawal key
2. FSS creates deposit data for the user to sign and broadcast to mainnet
3. FSS also creates an exploiting deposit data, with the same validator key but FSS’ own withdrawal credentials
4. When the user broadcasts their deposit transaction to Ethereum mainnet FSS front-runs it with the exploiting deposit transaction
5. Result is the user’s deposit is accepted with FSS’ withdrawal credentials

The general issue is that there is no check that a given deposit is either new or has the same withdrawal credentials if its validator key matches one for a previous deposit.