The Price Oracle is a critical part of the protocol and is used throughout to define the price for all assets. For example, when a position is liquidated, the value of the collateral is compared to the borrow balance using prices taken from this oracle.

Current owner of Price Oracle

This is the mainnet contract for Price Oracle V2

: 0xa50ba011c48153de246e5192c8f9258a2ba79ca9

The Price Oracle V2

contract is Ownable

and its owner

is currently 0xb9062896ec3a615a4e4444df183f0531a77218ae which is a proxy with implementation set toGnosis Multisig. As you can see here, the owners of the multisig are 5 EOA accounts which I assume are members of the core team. Any three of these 5 people together can transact with the price oracle freely without any delay or timelock.

What can the owner do?

Among other things, the owner

of Price Oracle V2

can run the following restricted function of the price oracle:

/// @notice External function called by the Aave governance to set or replace sources of assets /// @param assets The addresses of the assets /// @param sources The address of the source of each asset function setAssetSources(address[] calldata assets, address[] calldata sources) external onlyOwner

This function can be used to replace the price feed source for any asset on Aave. For example, the current price feed source for BAL is set to Chainlink BAL/ETH feed.

Can the owner compromise user funds?

Yes. A malicious owner

can perform the following simple attack:

1. Replace the price feed for an asset with a dummy contract that returns an arbitrary price of zero.
2. Find a position where the collateral is the asset whose price is now zero.
3. Liquidate the position (now possible since the collateral is worthless).
4. Receive the collateral after liquidation.
5. Change the price feed back to its original value.

Here is a different attack:

1. Replace the price feed for BAL with a dummy contract that returns a huge number.
2. Give 1 BAL as collateral to the protocol.
3. Borrow a huge amount of any other asset (now possible since the collateral has immense value).
4. Change the price feed back to its original value.
5. Disappear with the borrowed amount and abandon the 1 BAL.

In other words, any three of the 5 people in the core team multisig can compromise user funds.

Proposal

Giving the core team access to user funds may be acceptable in new/small projects that don’t have proper decentralized

governance. Aave is neither new - the governance system is mature - nor small - the TVL is currently over $18 billion.

No matter how much we trust these 5 people, they should not have access to $18 billion of user funds. People can be hacked, human error on their behalf can put the funds at risk. I don’t believe any existing DeFi project with comparable TVL currently gives its core team access to user funds. I also don’t believe the community is fully aware of this. I personally discovered this by accident and was thoroughly surprised.

The proposal is to move control over the Price Oracle to the governance. If this proposal is not accepted, the responsible bare minimum would be to add a time lock preventing immediate changes to the oracle.