TL;DR

We would like to propose the Aave community to award a 50’000 USD bounty for a security disclosure by the Hacxyk team, involving a misconfiguration of the fallback oracle on the Aave v3 markets.

The disclosure

On 19th April, the Hacxyk team reached BGD via the samczsun and Aave Genesis Team with the following bug disclosure:

- Hacxyk analyzed the code of the AaveOracle contract on Github, and then its equivalent production deployment on the different V3 pools, for example this one in Polygon.
- The team noticed that when an asset doesn’t have a price feed, or when the main price feed (Chainlink) returns 0, the main function returning the price getAssetPrice() forwards the responsibility of getting the price to another smart contract, denominated fallback oracle.
- By checking the contract configured as _fallbackOracle on the different instances of v3 (e.g.this on Aave v3 Polygon, the team noticed that contract was a mock smart contract without access control on the function used to set new prices:

function setAssetPrice(address asset, uint256 price) external override { prices[asset] = price; emit AssetPriceUpdated(asset, price, block.timestamp); }

- This misconfiguration would mean, that if the proper conditions on the main AaveOracle are fulfilled, the Aave pool pointing to the oracle will consume a price from the fallback oracle, which anybody could set an arbitrary value, to force undesired behavior price-wise on the affected asset/s.

Impact evaluation by Hacxyk

On their disclosure, Hacxyk classified this misconfiguration as likely and severe.

The rationale was that an oracle price malfunction affects potentially the whole liquidity in the market (so severe) and as causes, historic cases of Chainlink malfunction, together with the risk of wrong order of usage of the PoolConfigurator setAssetSources()

(so likely).

In addition, Hacxyk pointed out that ~$3B of assets (the whole borrowable liquidity on v3) were at risk.

More extensive evaluation from Hacxyk can be readHERE.

Impact evaluation by BGD

From a technical point of view, we confirm the vulnerability disclosed by Hacxyc: on deployment of all the markets of Aave v3, a misconfiguration was executed on the fallback oracle, with a contract belonging to the testing phase slipping to mainnet deployments.

However, we don’t agree with the impact evaluation, as we classify the vulnerability as severe, but unlikely

. Our rationale is the following:

- We are not aware of any historic malfunction of Chainlink price submission, on what regards Aave v1, v2 and v3, for an aggregated of around 100 assets. The condition to trigger the fallback oracle usage is more extreme even (price submitted should be 0), case that we are aware from Chainlink that has extra validations on their infrastructure.
- The usage of the PoolConfigurator contract to call setAssetSources() on the AaveOracle is, or controlled by the Aave governance (fully on-chain process with 4 days duration), or by the Guardian (full review of listing payload by BGD and other community members). It is highly improbable that a wrong ordering of calling setAssetSource() could happen.
- We still consider severe the impact in terms of liquidity affected, but the numbers presented by Hacxyk were not precise: TVL of Aave v3 at the time of disclosure was ~$46m, combined with the existence of pretty strict supply and borrow caps given the short period of time after deployment of a complex system like Aave v3.

Remediation

From BGD, we have verified that, as the fallback oracle is a deprecated component on the Aave Oracle, their reference there for all Aave v3 markets has been set to address(0), removing the attack vector.

At the time of the disclosure by Hacxyk, the Aave V3 markets had been live for less than three weeks and the deployer wallet had maintained the capability to change some protocol parameters, as a security measure to prevent or mitigate unforeseen vulnerabilities given the V3 code base was not yet battle-tested. The change was therefore possible without passing through a governance proposal, or a community Guardian for the markets deployed on networks that don’t have the capability of receiving messages from Ethereum mainnet.

No unaudited code was executed or deployed to fix the issue, as changing the fallback oracle is a capability of the Pool Admin role configured for each market in each network.

Bounty recommendation

Given our previous impact evaluation, we will propose via Snapshot and on-chain governance proposal a 50’000 USD bounty for Hacxyk.