TL;DR

Request for bounties pending from before the setup of the Aave <> Immunefi official bug bounty program, amounting a grand total of $86’500.

Context

Before the setup of the Aave <> Immunefi bug bounty program onSeptember 25th 2023, security reports by white hats where evaluated in an ad-hoc basis, proposing bounties/rewards following an approach like on this proposal. That was not optimal, as there was no formal scope defined, or strict ranges of bounties depending on severity and impact.

Currently, every report is being processed via Immunefi and the rules of the Aave program, however, there were other reports submitted via other channel before that (usually security@aave.com). As these reports should be evaluated at time of submission for fairness, and outside of the Immunefi scope defined afterwards, we think it is a good idea to reward them separately and retro-actively outside the program.

Reports

First of all, we want to clarify certain aspects for the community:

- The proposed rewards and evaluation metrics follow the ones we did ad-hoc in the pastHERE, as we don’t think it is fair for the white-hats to apply the rewards ranges on the current Immunefi program and out-of-scope rules, as they were defined afterwards.
- In one of the cases, we recommended the white hat to submit the report via Immunefi, in order to have access to the mediation procedure of the platform. As this mediation process was finally requested by the white hat, Immunefi charges the corresponding fee of 10% of the amount, which we think is legitimate.
- At the moment, we are not disclosing the full details of some of the reports

, because even if none of them create any risk for Aave now, one has dependencies with another report (not disclosed yet) and the other could increase risk to non-Aave entities.

1. Inconsistent validation on Aave v2/v3

When calling borrow()

with stable rate mode on Aave v2 and v3, one of the validations is that not more than a percentage of the total available liquidity can be borrowed at once.

However, swapBorrowRateMode()

doesn’t validate the same, which is unexpected and could lead to more stable rate borrowings than intended.

It is important to highlight that this is not possible at the moment, with minting of stable rate disabled.

Reported by

: @StErMi

Severity:

Low

The issue didn’t create any immediate problem in the protocol, but overexposure to stable rate mode is not expected.

Likelihood:

Certain

This problem was present on the deployed versions of Aave v2 and v3, on those assets with stable rate enabled.

Proposed bounty:

10’000 USD

2. Inconsistent HF (Health Factor) behaviour swap borrow rate mode

When swapping borrow rate mode, the HF of an user is not validated, as debt should remain the same. However, under edge scenarios, the HF of an user could slightly change (by ~1 unit of lowest asset’s decimals).

Reported by

: @StErMi

Severity:

No impact

This is not a bug or creates any exploit scenario, but it is unexpected behaviour.

Likelihood:

Certain

This problem was present on the deployed versions of Aave v2 and v3, on those assets with stable rate enabled.

Proposed bounty:

5’000 USD

3. Price manipulation of asset listed on Aave

By executing a complex strategy (involving compromising the asset’s trusted infrastructure), it could be possible to inflate the price of one of the assets listed on Aave v2.

Even if this belongs more to the centralisation risk of the asset, and we don’t consider a bug of the protocol, it was taken into account for off-boarding consideration of the asset by risk providers of Aave, and we believe it is fair to reward retro-actively.

As this risk still exist on the asset itself and more protocols could be using it, even if we don’t really see any immediate risk, we will not be disclosing at the moment details of it, until the team applies extra measures.

Reported by

: @RobertMCForster

Severity:

Critical

Being a price manipulation, the impact on the protocol would hypotetically be important.

Likelihood:

Not likely

The attack involves compromising asset’s infrastructure (which would directly disqualify on the current Aave <> Immunefi program), together with extra techniques; so we consider it theoretically possible, but highly improbable.

Proposed bounty:

65’000 USD. Additionally, 6’500 USD as Immunefi fee.

Next steps

During the next days, we will create an ARFC Snapshot, for the approval of the rewards by the community. If positive, afterwards we will proceed with an on-chain governance proposal, releasing the funds to the corresponding addresses.