TL;DR

Proposal for setting up a Request of Bounty Payout

procedure to make more agile payments to security researchers (white hats) who submitted a valid report on Immunefi.

How does Aave <> Immunefi work?

Since Oct 18th, the Aave <> Immunefi program has been live, currently accepting bug bounty submissions for all critical smart contract components of the Aave ecosystem.

In our role of engaged technical service provider for the Aave DAO, BGD acts as a reviewer of the program, evaluating all the different reports, and if applicable, categorizing them into severity levels.

Additionally, Avara Labs acts as the reviewer for the GHO system, which they developed.

The end-to-end procedure is the following:

- A white hat reports a bug.
- After passing an automatic Immunefi filtering, the reviewer team receives the report on the platform.
- We evaluate if eligible, their criticality, and their impact on live systems.
- We initiate any applicable procedure if the report implies a fix on Aave.
- We propose a bounty, after usually a discussion with the white hat.
- We introduce the bounty into the pipeline of payouts from the Aave DAO (we are in this stage

).

It is possible to argue that the program has been a success until now, after receivingthis report which led to the protection of the Aave system. Nevertheless, we think that the payout procedure should be slightly modified.

Bounty payout proposal

Following the definition in the bug bounty program, the payout of bounties to security researchers is scheduled to happen at the end of the following month, via an on-chain proposal that will release the funds from the Aave Collector to each recipient, in batch.

However, we have noticed certain friction in this framework, for the following reasons:

- Disclosure schedules and their limitations are different from one valid report to another.

Sometimes it could be possible to disclose a report before a fix, for example in cases where the problem is Low or even Medium. In other cases, fixes and disclosures take longer, depending on their nature, and given that all Aave updates happen via governance proposals.

- Due to the previous reason, important interdependencies are created: for example, a fix of a Low valid report could be slightly more complicated than a High one, even if less critical. But at the same time, operationally could be better to batch both of them.
- The funds to be released are controlled by the Aave DAO, so there is no way of doing it without a governance proposal, which is a hard requirement due to decentralization.

Even if reducing operational overhead is important, we believe paying relatively prompt bounties is as important, and we propose the following:

- Once a month, we will create a Request for Bounty Payout governance forum post, followed by a Direct-to-AIP on-chain proposal.

On this request, we will batch all pending Low, Medium, and, depending on our evaluation, High bounties payouts, but without disclosing the report itself

.

The objective is to avoid creating blockers on those payouts due to disclosure policies that are non-critical, as the amounts should be always relatively small.

- Even if the community has implicitly (via our service provider engagement) and explicitly (via the approval of our role as reviewer in Immunefi) trusted in our evaluation criteria, to reduce further any lack of transparency, we will request a representative of Immunefi to comment on each Request for Bounty Payout round, confirming that effectively the requested amount is pending to be paid.
- Disclosure of the discovered issues (potentially paid before, but not necessarily) will happen after the Request for Bounty Payout, whenever we believe is appropriate, taking into account the strategy fixes or any other security and operational considerations.
- In the same on-chain proposal, we will include the Immunefi fee, which amounts to 10% of the notional of the bounties.
- Unless there is a security reason to not do it, for Criticals we will always try to fix it before both disclosure and payout, as amounts are higher and we believe the community deserves full visibility on them.

Next steps

To not create unnecessary delays on Immunefi pending payouts, we will do the following 2 items in parallel:

1. Create an ARFC for the approval of the Request for Bounty Payout framework, which will formalize the procedure. Given that this belongs more to their scope of engagement, we will coordinate with @ACI for this step.
2. Publish on the forum the first Request for Bounty Payout, batching different payments of pending Low and Medium bounties.