TL;DR

Present to the community the bug bounty program created in collaboration with Immunefi, to be approved by the Aave Governance.

Aave bug bounty program

Following the pre-approval of the community onSnapshot and the discussion on the previous governance forum thread we have been collaborating with Immunefi in order to define the specifics of a bug bounty program adapted to Aave's needs.

All the details can be found on the program draftHERE (draft as it requires full on-chain governance approval), but the most important points are the following:

- Bug bounty program for the Aave DAO ran in the Immunefi platform.
- Through his role as a service provider of the DAO, BGD will be in charge of review and decision-making regarding bounty submissions, more precisely in the following items: Aave v2, Aave v3, Aave Governance v2, and Aave Safety Module.

Given their involvement in developing GHO,@AaveLabs (props for initiating the conversation with Immunefi at the start of the project) will be in charge of review and decision-making regarding GHO, with review support from BGD.

- The program will be ongoing until the Aave Governance signals to stop it. Evaluation of submissions is dependent on the agreement with the service provider of the DAO in charge (in this case, ourselves, BGD). At the moment, our successfully approved Aave <> BGD Phase 2 will cover this for the following 6 months (from 04/08/2023).
- Standard Immunefi bug submission procedural terms (e.g. PoC guidelines), but customized Threats Definition, adapted to Aave's needs.
- Payments are to be done directly by Aave governance proposals, in stablecoins or AAVE (30 days USD price average), or a mix of them. BGD will create a governance proposal for the community to provide feedback on the currency criteria.
- Systems covered:
- Aave v2 (critical and high vulnerabilities for Aave v2 Ethereum, only critical for other networks, in the process of migration).
- Aave v3.
- Aave Safety Module.
- Aave Governance v2.
- GHO stablecoin.

Additional Aave official systems will be added once live, if deemed reasonable the technical service providers of Aave.

- Aave v2 (critical and high vulnerabilities for Aave v2 Ethereum, only critical for other networks, in the process of migration).
- Aave v3.
- Aave Safety Module.
- Aave Governance v2.
- GHO stablecoin.
- Payout ranges (details and conditions on full document):
- Critical: $50'000 to $1'000'000.
- High: $10'000 to $75'000.
- Medium: $10'000.
- Low: $1'000.
- Critical: $50'000 to $1'000'000.

- High: $10’000 to $75’000.
- Medium: $10’000.
- Low: $1’000.
- To not create governance overload, bug bounty payouts via governance proposal will be batched with a minimum frequency of once a month.
- The Immunefi fee is the standard 10% on top of each bug bounty payout.
- Official and Former Official Contributors (as defined on the bug bounty document) are not eligible for bounty.
- Generally, no KYC requirements, but the reviewer reserves the right to apply mechanisms to avoid submissions by Official Contributors, on high and critical reports.
- Once approved, BGD will be able to modify technical aspects of the program to keep it updated, while not creating governance overhead. But any fundamental aspect (like payout size), will need to be approved via governance.

Next steps

After some days to gather feedback from the community, as technical service providers to Aave, we will submit a proposal on behalf of Immunefi, which will factually activate the program, if approved.