Title: [ARFC] Continuous Security Proposal Aave <> Certora

« post updated »

Author: @Shelly - Certora

Date: 2023-12-07

Summary

We offer to extend the existing formal verification and manual review services and provide additional security services:

1. Governance proposal reviews - Review every governance proposal in the on-chain stage as suggested by BGDLabs.
2. We will assist Aave and BGD in reviewing Immunify bug bounties per request.

This proposal asks for a 1-year duration with a budget of $1.5m, starting from the 14th of September 2023.

Motivation

During the 18 months of services, we have reviewed 169 smart contacts consisting of over 51,289 Solidity lines. We have prevented 28 significant bugs. Full breakdown of our work can be found in this spreadsheet.

Continuous Formal Verification (Auditing and Formal Verification integrated into CI)

Following the success of the collaboration in the last 18 months, we offer to continue this service in the same format - new code is formally verified and manually reviewed. Our open-source CVL specification rules are checked using the Certora Prover and become publicly available when the code is released. The formal tests are also integrated into Aave's CI system to continuously check changes introduced into the code. Reports are delivered upon demand at the end of each project. We have recently released a free version of the Certora Prover and the community can use this to validate the outputs.

The Aave and BGD teams will play a key role in rule writing going forward. These teams are highly technical and have insights into high-level properties of the protocol. Our team will review these rules and ensure the Certora Prover can formally prove these rules or find a bug. Our team will add more rules and manually review the code.

Governance Proposal Review

Following BGD's suggestion to add a third party to the governance proposals verification process, we will allocate a dedicated team to review each proposal on the on-chain stage within 3.5 days.

Each proposal's payload will be reviewed by the dedicated team, and we will verify that it does what it's supposed to do according to its description/AIP. We will also check that there are no unwanted effects on the codebase, which is supposed to stay unchanged.

Our job will be done after a review by BGD at an earlier stage. BGD will also assist with onboarding to guarantee the highest quality of service.

Incident Investigation Support Services

Triaging and validating all the incoming bug reports for a massive protocol, such as Aave, can be highly time-consuming and distracting for the developing entities. Many of the reported issues turn out to be benign. However, at the time of the report, the severity and feasibility of bugs are still unknown. Therefore, it is crucial to investigate them with full seriousness and urgency. We offer to establish an incident investigation support team available 24/7 to support emergency cases. In every incident, we will write a rule that confirms or rejects the existence of a bug and later use it to test the validity of the fix. After every incident, we will update the specifications and incorporate the new tests in the CI.

In past commitments, we have played a crucial role in two critical incident responses. In one case, we concluded that there was no bug in the system. In another case, we identified a missing rule, wrote it, and used it to catch a tricky bug in the suggested fix before the code was deployed.

Specification

The annual price for the project is $1.5M: $1M is paid in GHO vested linearly over one year, and $500,000 is paid in Aave tokens vested linearly over one year. A 30-day termination is possible after a vote. We reduced the price of $2.7M from last year to reflect the bear market and inlined with the reduced project review capacity.

The Aave and the BGD team will also assist by writing their CVL rules.

Next Steps

1. Gather community feedback on this ARFC.
2. If consensus is reached, escalate this proposal to ARFC snapshot stage.
3. If ARFC snapshot outcome is YAE, escalate to AIP stage.

Disclaimer

Certora is presenting this ARFC independently and is not compensated by any third party for creating this ARFC.

Copyright