Title

: [ARFC] BGD. Security budget request - December 2023

Author

: BGD Labs (@bgdlabs)

Date

: 2023-12-8

Summary

Request for a budget of $121’200 for 2 security review procedures on Aave, together with a refund of $30’000 to BGD for the Aave Governance v3 extra voting tokens audit.

Motivation

Part of our scope Aave <> BGD Phase II is the planning, engagement, and coordination with security partners of the DAO.

During the previous year and a half, Aave was in a pretty intensive delivery phase (Aave v3 improvements, GHO, Aave Governance v3, a.DI), and we thought it was appropriate to have continuous engagement with 2 security firms like Certora and SigmaPrime.

Even if this worked well, and we still think that Certora should stay with a continuous engagement, we also think that there is room for optimisation, and it is a good idea to do more ad-hoc requests for the security budget, depending on the needs.

This ARFC is an initial request, for budget required in the short term on item part of our development services scope, together with another more general we consider pretty important.

Specification

This request has 3 components, which we want to explain to the community:

1. Compensation for Mixbytes review of Governance v3 tokens

During the activation of Aave Governance v3 on October 17th, we detected a problem with the voting assets, which required the cancellation of the proposal, the development of a fix, and re-apply security procedures.

Given that it was already audited code, we also decided to do an extra security review by another security firm, Mixbytes.

For the sake of speed and reducing bureaucratic blockers, BGD paid for the cost of said security review of $30’000, and now we will include on this proposal a refund request for that amount.

1. Compensation for security review on a feature of Aave 3.1

Also part of our Phase 2 scope is to do a series of improvements to Aave v3, in order to reach a 3.1 version, from the current 3.0.2.

Generally, we are confident with Certora reviewing all the planned items until now, but there is one exception (an specific feature) to which we thought an extra review was required, and we engaged Emanuele Ricci (@StErMi), a top-level security researcher with knowledge of Aave to do it.

We will be publishing soon everything to be included into v3.1.

Same as with Mixbytes, BGD has paid the cost of said security review of $12’000, and now we include the refund request on this proposal.

1. Engagement with Spearbit for Aave v3 ad-hoc review

Aave v2/v3 is a production system with billions of dollars in size, and one of the most evaluated protocols security-wise.

However, security is a continuous process, and always worth it to improve whenever it feels necessary.

During the last 1-2 months, we have noticed different security exploits in the space following similar patterns. None of them affected Aave, but apart from our continuous analysis of the system security-wise, we think it is necessary to do an extra round of review in critical parts of Aave, for additional assurance.

We have coordinated an engagement for this review scope with Spearbit, one of the leading security firms in the space, that will involve 3 of their top researchers checking in-depth different components that we identify as critical on Aave.

This engagement is scheduled to start in the second part of December, and different from the others, the payment requested in the proposal will be direct to Spearbit, for an amount of $109’200.

For the sake of transparency, we will ask the 3 counterparties (Mixbytes,@StErMi , and Sperbit) to confirm the validity of the previous items in this forum post.

Disclaimer

This is a proposal created by BGD Labs, in the context of providing technical services to the Aave DAO as defined and formally approved here.

Next steps

Following existing governance procedures, we will create an ARFC Snapshot, followed by an on-chain AIP if the results on Snapshot are positive.

Given that this is a new procedure/framework that will be repeated in the future, we welcome any feedback of service providers like @ACI for it it should be formalised in a different way.

Copyright

Copyright and related rights waived via CC0.