TLDR

This is a proposal for Aave to collaborate with Hats.finance to create an on-chain, free, non-custodial, scalable and permissionless incentives pool for hackers/auditors to protect the Aave smart contracts.

Abstract

The direct losses from hacks and exploits between 2020-2022 are above $15B, and yet, the solutions currently being offered are not decentralized, permissionless, scalable, and continuous and open to everybody like Aave is.

This proposal aims to create an incentives pool on Hats Protocol for hackers/auditors to help protect the Aave smart contracts. The goal of the vault is to incentivize responsible vulnerability disclosure for Aave. Liquidity can be added (with $AAVE and/or yield-bearing tokens) permissionless and LPs will be rewarded with $HAT tokens once the liquidity mining program is launched.

Motivation

Hats.finance is an on-chain decentralized bug bounty platform specifically designed to prevent crypto-hack incidents by offering the right incentives. Additionally, Hats.finance allows anyone to add liquidity to a smart bug bounty. Hackers can disclose vulnerabilities responsibly without KYC & be rewarded with scalable prizes & NFTs for their work.

Smart bug bounty programs are a win-win for everyone. They can be created easily with a few on-chain transactions (it takes less than 1 hour to set up a vault on Hats), and are free of charge. Hats will only charge a fee once an incident has been successfully mitigated. The protocol will retain 10% of the payout as fee from the security researcher. Scenarios of an exploit are way more costly and can cause irreversible damage. More importantly, the bounty program is transparent, decentralized, and gives power to the community of the project.

On-chain submission:

With the values of Ethereum, which are lighting our way, we decided to take a different approach to bug bounty compared to the traditional and centralized bug bounty platforms.

The submitter writes a detailed vulnerability description on Hats dApp. The submission is encrypted with the project PGP key. The user hashes the encrypted description (automatically) and sends a transaction on-chain with that Hash (only the Hash of the encrypted report is going on-chain), While sending the encrypted message to the routing bot.

The tx fee acts as a spam filter and can be set to a higher value (in the future).

The routing bot verifies that the Hash of the encrypted message was published on-chain and publishes the encrypted message to the committee group together with a link to a front-end open source tool to decrypt the messages that are stored on IPFS that is part of Hats dApp.

Specification

In case that the proposal gets accepted, Aave is expected to:

1- Choose and set up a committee

2- Vote for DAO participation amount

Onboarding action items:

- Choosing a committee: The committee is preferably the public multisig contract of Aave or a multisig specifically set up to manage the bounty program.
- The Committees responsibility:
- Triage incoming vulnerability reports/claims from auditors/hackers (get back to the reporter within 12 hours).
- Approve claims within a reasonable time frame (Max. of 6 days)
- Set up repositories and contracts under review. (A list of all contracts covered by the bounty program separated by severity)
- Triage incoming vulnerability reports/claims from auditors/hackers (get back to the reporter within 12 hours).

- Approve claims within a reasonable time frame (Max. of 6 days)
- Set up repositories and contracts under review. (A list of all contracts covered by the bounty program separated by severity)

Rationale

The key advantage of Hats solution compared to traditional, centralized bug bounty services:

- Bug bounty vaults are loaded with the native or yield bearing token of each project. Reducing the free floating supply while giving the token additional utility.
- Scalable bounty network — vault TVL increases with success / token appreciation of the project.
- Open & Permissionless — Anyone can participate in the protection of an asset they are a stakeholder of and any hacker, anywhere in the world, can participate anonymously when disclosing exploits (no KYC needed)
- In the future when providing liquidity (taking risk) every depositor could earn $HAT tokens.
- Continuous — As long as tokens are locked in the vault, hackers are incentivized to disclose vulnerabilities through Hats, instead of exploiting the project.

Additional advantages of deployment of the existing Aave bug bounty program on Hats Protocol:

- Aave can reach out to many more security researchers (aka white hat hackers) with a bounty on Hats protocol and each scrutiny will make Aave safer.
- Aave can fund the bug bounty vault on Hats with its own native token ($AAVE or yield bearing token)
- The bounty reward for the submitter is not paid at once to reduce the price pressure on the project token.

Since Aave DAO will be farming $HAT tokens with its bounty (after TGE), it's a cost negative opportunity for Aave DAO.

Key Examples

A security researcher recently found a critical severity within Premia Finance's staking contracts and got rewarded $70k for his responsible disclosure:

[https://twitter.com/HatsFinance/status/1663243357160890369]

In one of the recent audit competitions, the security researchers could find 3 critical severities in Raft Finance's code in a 7 days long audit contest even if the project went under an extensive audit by one of the top-tier auditing firms in the space:

Medium – 5 Jun 23

Raft Finance Audit Competition- Final Note

It's been a record-breaking month for the Hats team! We are proud to officially end our competition with Raft Finance and share the list of…

Reading time: 6 min read