Introduction

This pre-proposal TEMP CHECK asks the AaveDAO to approve a bug bounty program hosted on Immunefi. Immunefi proposes to engage with community contributors, the Aave Companies and BGD Labs, who would support the bug bounty program as technical experts in terms of receiving and evaluating bug reports as well as providing their view on what should and shouldn't be covered under the program, pending DAO approval.

Motivation

Currently, the Aave Protocol boasts a TVL of over USD 5 billion. A key reason why the protocol has managed to amass such impressive liquidity is due to the DAOs security-focused culture. Users of the protocol feel safe when using Aave.

As the Protocol continues to develop thanks to impressive work done by DAO contributors, with some notable innovations being V3 and GHO, it continues to be incredibly important that as much care is taken to ensure that users feel safe when using the protocol.

One great way to further protect user funds is to enact an effective and standardized bug bounty program. A bug bounty program encourages security researchers to continuously look through our codebase and responsibly disclose any bugs that they find, especially as new types of vulnerabilities are being discovered. Additionally, it provides a last option for blackhat hackers who find a bug to disclose it instead of exploiting it and get rewarded with clean funds.

About Immunefi

Immunefi is the leading bug bounty and security services platform for Web3, featuring the world's largest Web3 security community and bug bounty programs. Immunefi guards many billions in users' funds across projects like Wormhole, MakerDAO, Polygon, Chainlink, Lido, Stacks, Optimism, and many more. The company has prevented exploitation of vulnerabilities that put tens of billions of dollars at risk across hundreds of projects.

Implementation

Immunefi proposes to work together with two other community contributors, Aave Companies and BGD Labs, in order to ensure that the bug bounty program is written and maintained to an optimal level, ranging from the assets that are covered by the program, SLAs with regards to response times, rewards for valid bug reports, as well as points of clarification within the program. The terms of implementation in this section is thus not set in stone but will be the starting point for the program.

The assets considered as in-scope of the bug bounty program will be those that are identified as critical to the operation of the Protocol. However, in order to ensure maximum safety for Aave users, a bug report would be considered as in-scope regardless of the asset being listed or not as long as it is a Critical-level smart contract report with funds being directly at risk.

All rewards for bug reports will utilize the Immunefi Vulnerability Severity Classification System. If Immunefi develops a new classification system, the one implemented into the Aave bug bounty program may be changed to reflect these changes, and would request a review from both Aave Companies and BGD Labs. For the Aave bug bounty program, we will begin with covering Low to Critical vulnerabilities for smart contract assets. Additional severity levels will be considered shortly after its launch.

The reward amounts will be as follows:

Smart Contracts

Critical

Up to USD 1 000 000

High

Up to USD 100 000

Medium

USD 5 000

Low

USD 1 000

Critical smart contract vulnerabilities will be further capped at 10% of direct funds at risk. In cases of repeatable attacks, only the first attack is considered unless the smart contract cannot be upgraded or paused. If the attack impacts a smart contract directly holding funds that cannot be upgraded or paused, the amount of funds at risk will be calculated with the first attack

being at 100% of the funds that could be stolen and then a reduction of 25% from the amount of the first attack for every 300 blocks the attack needs for subsequent attacks from the first attack, rounded down. For avoidance of doubt, if a second attack would happen at 600 blocks and then a third at 900 blocks, the funds at risk would be counted at 50% and 25% from the first attack, respectively.

However, there is a minimum reward of USD 150 000 such that the reward amount is above that of High in order to prevent hackers from sitting on a bug report while potential economic damage increases.

Rewards over USD 150 000 will be paid out in batches of up to USD 150 000 until the full reward amount is paid out. The first batch will be paid out within the SLA period for resolving a bug report and the monthly payout starts in the succeeding calendar month if the first Monday falls 15 days after the first payout.

High smart contract vulnerabilities will be further capped at up to 100% of the funds affected. In the event of temporary freezing, the reward doubles for every additional 5 blocks that the funds could be temporarily frozen, rounded down to the nearest multiple of 5, up to the hard cap of USD 100 000. This is implemented in order to account for the increased relative impact based on the duration of the freezing of funds. There is, however, a minimum reward of USD 7 500 for High smart contract vulnerabilities.

In addition to the standard bug report information requested by Immunefi in its bug submission page, a runnable proof of concept (PoC) will be required for all smart contract bug reports. Exceptions may be made in cases where the vulnerability is objectively evident from simply mentioning the vulnerability and where it exists.

All bug report submitters must comply with the Immunefi rules. Employees and team members of the community contributor teams (including Aave Companies and BGD Labs in case the DAO supports that they are nominated to assist Immunefi), including those who held this status within 12 calendar months of a bug report date, are not eligible for any reward.

Payments will be made in stablecoins that are held in the treasury.

Immunefi Fee

As its standard fee, Immunefi will charge the DAO a performance fee based on the reward paid out to the bug bounty hunter, charged on top of the reward. This standard fee is 10%. Effectively this means that if a bug bounty hunter receives a reward of USD 1 000, Immunefi would be paid an additional fee of USD 100.

Immunefi will charge no onboarding or maintenance fees for hosting and assisting with the bug bounty program. Any add-on services will be dealt separately, if ever additional services are desired in the future.

Engagement with the DAO

As part of the above-mentioned program, it is required that there are entities directly in contact with Immunefi who can work on behalf of the DAO to review submissions and engage with security researchers along with other tasks. Naturally, as part of the bug bounty program extremely sensitive information could be shared.

If this program and our engagement with it is approved by the DAO, the responsibility of both companies will be the following:

- Engage with Immunefi in defining and launching the bug bounty program.
- Review all bug bounty submissions and assign a level of severity.
- Respond and engage with the security researcher to resolve and patch any vulnerabilities, though it is understood that the security researcher’s responsibility ends at providing information about the bug and not providing work for fixing.
- Any other stated responsibility as set out by the Immunefi statement of work.
- Update the DAO on important information regarding the program.

BGD Labs and Aave Companies in their capacity in supporting Immunefi would also seek to comply with the necessary SLAs wherever it is not restricted by governance systems within the Protocol, such as payments. This would be to ensure that security researchers can expect the same level of responsiveness that they do with other bug bounty programs on Immunefi.

Conclusion

This TEMP CHECK proposes an Immunefi bug bounty program for the AaveDAO. The intention of this program is to properly incentivise white hats to test the security of the protocol and report recognised vulnerabilities. If approved, Aave Companies and BGD Labs would engage with Immunefi on behalf of the DAO.

//Edit. This [TEMP CHECK] was edited on April 5, 2023 at 18:06 CEST to correct information about the role of community

contributors.