Everyone is aware of the recent CRV attack. I noticed this behavior on chain, provided a detailed writeup of the underlying vulnerability a week in advance of the attack, included the specific wallet executing the attack, and provided immediate actions to take to protect the protocol until longer-term solutions were implemented. Yet the security team sat on the report for a week and did nothing. Through sheer luck the attack was mostly averted, meaning the protocol lost only $1.5m, rather than the $20-$40m at risk.

The AAVE team has refused to pay any bug bounty payment for bringing the specific wallet and attack vector to their attention in advance of a targeted exploitation of AAVE vulnerabilities. The reasoning was that it was a “liquidity risk” and not an exploit.

[

image

1068×230 12.9 KB

](https://europe1.discourse-cdn.com/business20/uploads/aave/original/2X/f/f84da8ba41844838cd4d35a9e7729856bfac8068.png)

But my bug bounty didn’t only share a generalized liquidity risk within the protocol. It identified a specific attacker with the specific steps being taken to target a specific system vulnerability. Bug bounty programs exist to incentive early reporting of vulnerabilities, swaying people from exploiting the vulnerability in order to collect the bug bounty, and safeguard the protocol. What is the point of having a bug bounty program if early reporting of a concentrated attack is not included within the scope? All this means is that the incentive going forward is to exploit such system failures rather than report them.