EDIT: DAO Vote: Snapshot

We started a bug bounty program for Lido a while ago; since then, there have been two valid admissions out of two, both of no practical impact.

Immunefi's handling of bounty programs is nothing but professional, and they attract the brightest security minds in the space.

It's time to increase and expand Lido's bug bounty program.

Expanding bug bounty program beyond Ethereum

Lido's going increasingly more multichain. With bLuna and soon stSOL in its box of products, it's important to secure all of our mission-critical code.

LEGO's got a mandate to manage Lido's bounty program, within allotted limits, and going to handle that increase. We will add separate programs on Immunefi, to limit potential compromise, with the same terms as the existing bounty program but a different set of targets.

Increasing bug bounty program

Lido's a very mission-critical project and is a very lucrative target. The realities of the bug bounty market for DeFi these days also set the bar for critical vulnerabilities bounties quite high. It's time to increase Lido's bug bounty to a reasonably big level.

I propose granting LEGO the power to select critical targets and vulnerability types and raise a bounty for them up to $2m depending on potential impact.

We should designate a subset of targets and subset of vulnerabilities that will get a maximal payout, starting with:

- Lido on ETH's governance contracts, liquid staking contracts, oracle contracts, and node operators registry
- Solido (Lido for Solana) contracts and governance multisig contracts
- bLuna's essential smart contracts

Make bug bounty payment more discreet

One more change is needed to be done for LEGO processes: currently, all payments of boulder and larger size need to be posted on research.lido.fi with details; that is not a great process when it's a payment for a (yet or ever) unmitigated vulnerability in smart contracts.

I propose an amendment to LEGO rules that would allow bug bounty payments to go before specifying the exact reason of payment, at the condition that the reason will be disclosed within 90 days.

Next steps

The first change is being discussed and implemented as I write this.

The second and third amendments are not within LEGO's mandate, so it requires a snapshot vote, which will come after the discussion on this topic is concluded.