Dear Lido Community,

Over the past weekend, we upgraded our protocol to introduce V3, which included a new router to facilitate swaps and future aggregation plans. Unfortunately, the RouteProcessor2 contract contained a critical risk level approval bug, and users who approved the contract within the approximately 12 hours that it was live were at risk of being exploited from the contract. While we were working on mitigations to prevent as much damage as possible, a whitehat made a mistake while attempting to secure the funds using a public rpc. As a result, several other parties were able to replay the transaction, resulting in approximately 1800 WETH being drained from a single wallet. Some of these transactions were built by independent block builders, where in one case a substantial amount of ETH had been transferred as a MEV reward to the block builder that then redirected it to Lido Execution Rewards Vault.

We reached out over the weekend to several Lido contributors to discuss options for recouping these funds and were advised to continue the discussion within the community. We understand that Lido is a fully permissionless protocol, and therefore there may be no immediate levers that can be pulled to help capture these exploited funds. However, we wanted to initiate a conversation about possible options for recovering funds in this situation, which is unprecedented and could happen again in the future with block builders being bribed to build malicious transactions.

From our initial conversations, it appears that approximately 78 ETH was sent to the Lido Treasury, which could be an easy starting point for recovering some of the funds. For the rest of the funds, the majority of them have been or will be re-staked, and we are open to all ideas and suggestions for mitigating the situation and helping with the recovery process.

We apologize for any inconvenience this may have caused and are fully focused on doing everything we can to make everyone involved in the exploit whole. The Sushi community has much respect for Lido, and we thank you for the help we have received so far.

edit

: We've updated this proposal to include additional granular information below to help the Lido community understand the exact nature of the funds disbursement.

Within blocks 17007839 and 17007842 in total of 5 transactions related to Sushi RouteProcessor2 bug sifuvision.eth sent a total of 795.9761955 ETH to Lido: Execution Layer Reward within beaverbuild (within block 17007842) or directly (within block 17007839).

Transactions and ETH Amounts

91.9961955 ETH

10 ETH

5.1 ETH

678.88 ETH

10 ETH

Also as a correction to our 78 eth sent to the treasury statement. Those rewards were combined with rewards on CL and other rewards on EL and defined stETH rebase that reflects ETH inflow in protocol within the Oracle report on 2023-09-04. As a result of the Oracle report, according to Lido protocol specification, 5% of total rewards were transferred to treasury and 5% to node operators. With total rewards for 2023-09-04 being ~1,564.7 ETH, with 5% at ~ 78.23 ETH.

Therefore, the exact proportions applied to the total rewards gained as a consequence of the bug (795.9761955 ETH

) as it's a part of total rewards result in:

1. 5% (~39.8 ETH) going to the treasury
2. 5% (~39.8 ETH) were sent to node operators
3. 90% (~716.3 ETH) remained within the protocol and were staked according to the protocol specification combined with other rewards, resulting in 1056 ETH in total deposited from stETH token contract to beacon chain to different validators operated by different operators, 33 validators total