

This was the message from Rocketpool

Hey everyone!

We have now examined the sophisticated node exploit and have designed a fix for it. This issue is not just related to our own node architecture, so we are reaching out to other affected staking setups that operate with a similar setup and hope to have this exploit patched for future staking protocols & pools as well.

The changes required on our end are relatively minimal and we are working on them as we speak. The whitehat who revealed the exploit (who chose to remain anonymous) has also agreed to verify our fix once it is in place. We awarded them with our maximum bounty of \$100,000 USD as a reward for finding this very esoteric exploit on Ethereum staking pools. We will be also asking our friends at Sigma Prime to review any of these minimal changes as an extra precaution. This will not be on the same scale as their previous audits, as these changes are quite small.

We will be doing a full public disclosure of the exploit and how it affects pools once we have reached out to similar projects and helped them implement a fix as well.

So does the bug found also affect us in any way?