Fixed: potential vulnerability in contract used during private beta

Tian Li
Sep 30, 2019 · 1 min read

On 12:54 am September 18th, the security researcher samczsun notified us of a potential vulnerability on a contract we used to beta test margin and lending functionality. **The fix was deployed and verified at 5:50 am September 18th. No funds were lost.**

We refrained from releasing any information until September 30th, because we were notified that similar vulnerabilities were found in publicly launched projects with substantial funds at risk.

Neither ddex.io nor hydro relayers are affected by this issue. The potential vulnerability occurs only within an isolated set of contracts we deployed for beta testing purposes. Approximately 122 ETH worth of ETH and DAI were at risk.

The exploit worked by drastically altering the DAI price of uniswap and eth2dai, the two projects we used to source DAI price. In a simulated contract call, samczsun used approximately 25000 of ETH to drastically alter the price of DAI, which allowed borrowing to occur with very little actual collateral, resulting in a profit of approximately 70 ETH. Samczsun's excellent post provides more detail.

We are extremely impressed with and grateful of samczsun's research and disclosure, and are rewarding this find with a bug bounty of $10,000.

Ethereum