Your Funds are Safe.

bZx Team
Sep 30, 2019 · 2 min read

On Tuesday September 3rd, samczun, the security researcher who found the critical bug in 0x, alerted us to an exploit leveraging our implementation of Kyber's price feeds. We have confirmed that the exploit exists and has never been used. The exploit was immediately patched.

The premise of the attack involved manipulating the price feed with a sandwich attack at the time of taking out the loan. This was an attack vector that both ourselves and our auditors did not detect. Despite the fact that great pains had been taken to protect against price feed manipulation, most of that effort was spent focused on the liquidation process.

The first variant of the exploit leveraged the Oasis OTC market, allowing Kyber's permissioned sanity prices to be manipulated to arbitrary values for ETHDAI. According to the comments in the code the OTC market should match an order with an arbitrage price, but the actual code itself did not execute in this fashion. This exploit only works for the prices of ETHDAI and no other pairs.

The second variant of the exploit leveraged the fact that Kyber sometimes routes orders to Uniswap. This allowed an attacker to time and size the trade to get routed to the Uniswap reserve, start a sandwich attack, take out a loan, and conclude the sandwich attack while incurring only trade fees.

To prevent this attack and all future variants we now make two calls to Kyber to ensure that `ask > bid`, indicating that no arbitrage prices are being included in the price feed. As long as a Kyber asset has at least one fed-price or orderbook reserve, this also protects against a double sandwich attack on both sides of the trading pair.

We regard security solemnly, and it's important to us that we take all the measures possible to minimize the chance of incidents like this occurring. We have been conducting additional internal audits as we work toward publishing a reference

implementation of the codebase. We will also be investigating the commission of a second independent security audit.

We are thankful to members of the community like samczun for strengthening the security of the ecosystem.

-

If you have questions, visit us on Telegram or Discord.

Blockchain