Context

On November 8th, 2024, the GlueX Protocol suffered an exploit via one of the contracts onboarded to lower the execution cost of swaps against a specific type of DEX. The attack vector allowed any address to transfer collected fees out of the settlement contract. This exploit resulted in a substantial loss over the span of one hour, which is how long the attack vector remained open. The size of the losses would have been catastrophic to the solver involved if the attack vector would have remained open for a longer period of time.

This is not the first time solvers have faced the reality of the risks involved with the CoW Protocol holding fees in the settlement contract(see Barter's Exploit).

While in both cases the exploit resulted from smart contracts deployed by the solvers, the reality is that every liquidity source integrated by a solver increases their risk of being liable for a similar attack. To date, most liquidity sources that can be integrated by solvers have been heavily audited and battle-tested. However, as more diverse liquidity sources emerge (e.g., with Uniswap V4 pools) and DeFi evolves, the risk of integrating an exploitable liquidity source increases.

In theory, it is the responsibility of solvers to audit every contract of new liquidity sources to which they will be granting allowances; however, the reality is that solver teams may not have the knowledge, funds, or resources to execute such audits at the same pace at which DeFi evolves. On the other hand, it is in the protocol's best interest to have solvers onboard new sources of liquidity as soon as possible to attract new business and support partnerships with other protocols (as was the case with the Maker-Sky migration).

Purpose of Post

With this post, we would like to hear the opinions of the core team and other solver teams:

- Is this a risk that everyone is willing to continue taking?
- What can be done immediately to fully or partially mitigate this risk?

The result of this discussion should ideally be a CIP to address this issue moving forward.

Preliminary High-level CIP

CoW DAO should limit the amount of funds available in the settlement contract to a maximum of $5,000 worth of any collection of tokens. Any funds exceeding this threshold should be transferred to a fee collection contract within the same CowSwap settlement transaction in which the fees are generated.

Note

We are very thankful with the CowSwap team for having recognized the attack vector as promptly as they did. Without their support at the time, GlueX Protocol would have experienced losses multiple factors larger than the losses incured.