G0 Group

Security Review of

Gnosis Protocol V2

May 2021

Gnosis Protocol V2 / May 2021

Files in scope

All solidity files in:

https://github.com/gnosis/gp-v2-contracts/tree/7184fc98c05d2d336d90ee4e6b36429457a56d43

Current status

All reported issues have been fixed by the developer

Report

Issues

1. Rounding in settle function favors solvers

type: security / severity: minor

In `GPv2Settlement.computeTradeExecution`, it's theoretically possible to fill orders that have `order.sellAmount > order.buyAmount` in increments so small, that `outTransfer.amount == 0` and `inTransfer.amount > 0`. Hypothetically a whole order could be filled this way without the buyer receiving a single unit of the desired asset, in practice this attack will be rendered unprofitable by the gas costs in the vast majority of cases. Still, it would probably be better to round up instead of down when calculating `outTransfer.amount` to make sure the user, who is in the passive role, can never be shortchanged by the solver.

status - fixed

Issue has been fixed and is no longer present in

https://github.com/gnosis/gp-v2-contracts/tree/5d90c5842b30b8c8945512e613971675897570a9

Notes

1. `order.appData` is currently an unused variable, except for serving as a salt for the hashed order digest