Cowswap Order Signer / December 2023

Files in scope

All solidity files in https://github.com/gnosis/cow-order-signer/tree/1602e66071a250e8841dc8126453884a075c7c1f/contracts:

Current status

No issues directly affecting the code under review have been discovered.

Issues

1. Chain.id being baked in during deployment in GPv2Signing allows replaying signatures between chains

type: security / severity: note

In `GPv2Signing.sol` the `domainSeparator` component of signatures is calculated once on contract deployment and then stored as an immutable value. Part of this value is the `chainid` chain identifier that changes when chain undergoes a fork. Since the value won't be recalculated after the fork, the old `chainid` will be used for signature validation which will make signatures from the original chain valid both on the original chain and on the new branch, preventing the signer to perform safe independent operations on both branches. This issue concerns `GPv2Signing` contract which is not directly in scope but is contained in the repository. Since the contracts under audit don't work with offchain signatures, this issue is not directly relevant.

status - fixed

The issue has been previously acknowledged by the developer and is included in the review for the sake of completeness.