CoW-AMM Module Audit

This document presents the finding of a smart contract audit conducted by Côme du Crest for Gnosis.

Scope

The scope include the contract `CowAmmModule.sol` of cowprotocol/cow-amm as of commit f075b10 and associated libraries: `SafeModuleSafeERC20.sol`, and `SafeModuleAddress`.

Context

This audit follows a previous audit on CoW-AMM, the constant product AMM that enables programmatic orders for an AMM on CoW protocol. The goal of the audited module is to allow for easy deployment and setup of CoW-AMMs.

As written in documentation, to create a constant product AMM users need to:

- Deploy a Safe
- Change the Safe's fallback handler to `ExtensibleFallbackHandler`
- Set the Safe's domain verifier for CoW Protocol to `ComposableCoW`
- Deposit and approve the tokens for trading on CoW Protocol
- Create the AMM order on `ComposableCoW`

The `CoWAmmModule` contract's `createAmm()` function can be used to automate most of these tasks, it can:

- Change the Safe's fallback handler to `ExtensibleFallbackHandler`
- Set the Safe's domain verifier for CoW Protocol to `ComposableCoW`
- Approve the tokens for trading on CoW Protocol
- Create the AMM order on `ComposableCoW`

The only thing left to the user is to deploy a safe, deposit tokens into it in the right proportions for the constant product AMM, enable the module on the safe, and call `createAmm()` with the right parameters. This is less constraining and error prone to the user.

Status

The audit has been sent to the development team.

Issues

No serious issues have been discovered.