

Security Review of

CoW TWAP Orders

January 2023

CoW TWAP Orders / January 2023

Files in scope

All solidity files in <https://github.com/rndlabs/cowswap-twap-orders/tree/33b3ca714f3f33f3fb185e27f16dae0fdd9331ca/src>:

Current status

All discovered issues have been fixed by the developer. No known issues are present in: <https://github.com/rndlabs/cowswap-twap-orders/tree/c59dd2908a08f9935c839cafeeb17c410340230f/src>

Issues

1. Missing input validation in `verifyTrade`

type: incorrect implementation / severity: minor

`TWAPOrder.validate` is called in `CowFallbackHandler.dispatch` but not in `CowFallbackHandler.verifyTrade`, which means “invalid” trades can be executed and invalid assert conditions can be reached in `TWAPOrderMathLib.isValidSignature` calls in `TWAPOrderMathLib.sol` on lines 25,26,27.

status - fixed

The issue has been fixed and is no longer present in: <https://github.com/rndlabs/cowswap-twap-orders/tree/c59dd2908a08f9935c839cafeeb17c410340230f/src>

2. Inconsistent input validation

type: incorrect implementation / severity: minor

Order validation conditions implemented on following lines don't match.

- `TWAPOrderMathLib.sol:line25` & `TWAPOrder.sol:line62`
- `TWAPOrderMathLib.sol:line26` & `TWAPOrder.sol:line63`

status - fixed

The issue has been fixed and is no longer present in: <https://github.com/rndlabs/cowswap-twap-orders/tree/c59dd2908a08f9935c839cafeeb17c410340230f/src>