Aggregation router v5 pre release audit

27 Sep 2022, Igor Gulamov

Introduction

Igor Gulamov conducted the audit of 1inch Aggregation Router V5.

This review was performed by an independent reviewer under a fixed rate.

Scope

1inch-contract#v5-audit...v5-audit-pre-release-v2

- contracts/AggregationRouterV5.sol
- contracts/routers/ClipperRouter.sol
- contracts/routers/GenericRouter.sol
- contracts/routers/UnoswapRouter.sol
- contracts/routers/UnoswapV3Router.sol
- contracts/interfaces/IClipperExchangeInterface.sol
- contracts/interfaces/IAggregationExecutor.sol
- contracts/interfaces/IUniswapV3Pool.sol
- contracts/interfaces/IUniswapV3SwapCallback.sol
- contracts/helpers/Errors.sol

limit-order-protocol#d84378857 44543e3f057e84e1b0a05c4c211c553

- contracts/OrderMixin.sol
- contracts/OrderRFQMixin.sol
- contracts/OrderLib.sol
- contracts/OrderRFQLib.sol
- contracts/helpers/AmountCalculator.sol
- contracts/helpers/NonceManager.sol
- contracts/helpers/PredicateHelper.sol
- contracts/interfaces/IOrderMixin.sol
- contracts/interfaces/NotificationReceiver.sol
- contracts/libraries/ArgumentsDecoder.sol

- contracts/libraries/Callib.sol
- contracts/libraries/Errors.sol

solidity-utils#eec6b523860af5215a8dd196fe3aff3a4d252fc9

- contracts/EthReceiver.sol
- contracts/StringUtil.sol
- contracts/libraries/UniERC20.sol
- contracts/libraries/SafeERC20.sol
- contracts/libraries/ECDSA.sol
- contracts/libraries/RevertReasonForwarder.sol
- contracts/interfaces/IWETH.sol
- contracts/interfaces/IDaiLikePermit.sol

Issues

We found no critical and no major issues.

We consider 1inch-contract#bc00c75f2c99d62e1a206aa2f81c408caba4b370, limit-order-protocol#171c5d7bbb280d9f754404828051f2a47fb726df, solidity-utils#c35dc32fd91ee01f961df13ab7c30faf40be8b89 as safe from the informational security point of view.

1inch-contract

Warning

ClipperRouter.sol#L145

ClipperRouter.sol#L170
ClipperRouter.sol#L195
ClipperRouter.sol#L245

We propose replacing `shl` and `shr` with `and` opcode.

Fixed at 2c075e0c76c4978337a2eb452015c045e098cd0f.

GenericRouter.sol#L118

We propose fixing the memory leak with `mstore(0x40, ptr)`.

Fixed at c0d7ccf74cf42eaa67e7dbc8b4224899b5eb6c12.

limit-order-protocol

Warning

OrderMixin.sol#L264

For most cases, the caller can bypass increasing `offeredTakingAmount`, because `interaction` is caller-specific.

Will not fix. *That's by design. Increase in offeredTakingAmount is needed only in super specific cases.*

Comment

OrderMixin.sol#L94

We propose replacing the argument type from `memory` to `calldata` for external function.

Will not fix.

OrderRFQMixin.sol#L112

OrderRFQMixin.sol#L79

OrderRFQMixin.sol#L147

OrderRFQMixin.sol#L168

OrderRFQMixin.sol#L185

OrderRFQLib.sol#L30

We propose replacing the arugment type from `memory` to `calldata` for better optimization.

Will not fix.

AmountCalculator.sol#L10

`Callib` is not used in `AmountCalculator`.

Fixed at 2034c99db9da20834359d02017fc863c0c89cb53.

solidity-utils

Warning

EthReceiver.sol#L11

This expression forbids users to make deposits to contract from keypair-derivable addresses. But users can bypass it, using contract wallets, like Gnosis Safe.

Will not fix. *We'll add comment to describe intended usage of this contract.*

UniERC20.sol#L38

UniERC20.sol#L53

`transfer` is deprecated. Gas limits could be violated in future hardforks.

Fixed at 6b1a3dfbe5410b37fa9d3558b606990d9fb32e43.

UniERC20.sol#L75

We propose replacing strings with raw `bytes4` signatures.

Fixed at 9d366b2554a8a341a80098154e92ad5936f2032a.

ECDSA.sol#L32

ECDSA.sol#L56

We propose replacing `shl` and `shr` with `and` opcode.

Fixed at 318dd6760e3a446e5f73d7a8ca2bff5bc4554daa.

Comment

StringUtil.sol#L7

This library could be optimized in case of replacement `abi.encodePacked` expression with `mstore`,

Will not fix. *This requires rewriting completely in assembly. We'll keep it as it is for now.*