1inch Exchange Audit

26 Feb 2021, Igor Gulamov

Introduction

Igor Gulamov conducted the audit of 1inch exchange smart contracts.

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

Scope

Diff

OneInchExchange.sol
OneInchUnoswap.sol
helpers/Permitable.sol
helpers/UniERC20.sol
helpers/RevertReasonParser.sol

Issues

We found no critical issues. The major issue is fixed at e6a827dc53a60018fb3b41d5c520a79e70ebec06.

We consider the commit e6a827dc53a60018fb3b41d5c520a79e70ebec06 as a safe version from the informational security point of view.

Critical

Major

1. https://github.com/1inch-exchange/1inch-contract/blob/d3def083b875d3e04faf2caee758a1c4aaf43b7d/contracts/OneInchUnoswap.sol#L133

In case when `unoswap` is called internally from `unoswapWithPermit`, it will try to swap using `permit` data, because all calldata optodes will correspond to top-level function call arguments.

Warnings

1. https://github.com/1inch-exchange/1inch-contract/blob/d3def083b875d3e04faf2caee758a1c4aaf43b7d/contracts/OneInchUnoswap.sol#L95

`calldataload` load data from tx. In case of internal usage of the function data, loaded by `calldataload` will be not corresponded to current function arguments. Ensure, that the argument sequence is the same for all functions calling the current one internally or make the function external.

Comments

Severity Terms

Comment

Comment issues are generally subjective in nature, or potentially deal with topics like "best practices" or "readability". Comment issues in general will not indicate an actual problem or bug in code.

The maintainers should use their own judgment as to whether addressing these issues improves the codebase.

Warning

Warning issues are generally objective in nature but do not represent actual bugs or security problems.

These issues should be addressed unless there is a clear reason not to.

Major

Major issues will be things like bugs or security vulnerabilities. These issues may not be directly exploitable, or may require a certain condition to arise in order to be exploited.

Left unaddressed these issues are highly likely to cause problems with the operation of the contract or lead to a situation which allows the system to be exploited in some way.

Critical

Critical issues are directly exploitable bugs or security vulnerabilities.

Left unaddressed these issues are highly likely or guaranteed to cause major problems or potentially a full failure in the operations of the contract.