MixBytes()

1INCH

SECURITY REVIEW

NOVEMBER 05
2020

TABLE OF CONTENTS

01 SCOPE OF WORK

Commit: aa1d1c54546f38b912a24722134ab0c2ae94860d

* OneInchExchange.sol
* OneInchFlags.sol
* helpers/RevertReasonParser.sol
* helpers/UniERC20.sol
* GasDiscountCalculator.sol

Contarct Address: 0x111111125434b319222CdBf8C261674aDB56F3ae

DETECTED ISSUES

CRITICAL

1. OneInchExchange.sol#L89

If the `isDiscountChi` flag is set and `_claim` is being executed, when the `oneInchCaller.makeCalls` call is rolled back, the tokens transferred during `_claim` will not be returned to the owner.

A similar situation can occur with any other tokens transferred by separate messages (calls) from the balances of the owners (for example, using pre-issued allowances) for an exchange that ultimately did not take place.

Also, the problem concerns the ether sent to the `swap` call.

The simplest and most reliable solution to the problem is to rollback the entire swap call if `oneInchCaller.makeCalls` fails and not try to burn the CHI token.

Status:

Fixed at **487f7af**

MAJOR

Not found.

WARNINGS

1. OneInchExchange.sol#L151

There is no way to resume the work of the contract after a pause (by calling `_unpause ()`). We recommend that you make sure that this is intended, and if so, then note it in the comments in the code.

Status:

ACKNOWLEDGED

2. RevertReasonParser.sol#L13

It is worth making sure that the 256-bit number in memory at `data + 68` does not exceed `data.length - 68` that is the length of the abi-encoded string is true.

Status:

Fixed at 9af8a58

3. OneInchExchange.sol#L77-L80

Such calculations may work incorrectly or not work at all for tokens that perform some internal balance replenishment before the balance is modified, but do not do the corresponding adjustments in their `balanceOf` functions.

An example of such replenishments would be “dividends”. Examples of such tokens are **first version of KICK** or **this library**.

Status:

Partially Fixed at 9af8a58

4. OneInchExchange.sol#L30

The `desc.guaranteedAmount` field is not used in the `OneInchExchange` code nor in any code called from `OneInchExchange.swap`. We recommend that you ensure that all planned logic is implemented.

Status:

ACKNOWLEDGED

5. OneInchExchange.sol#L49

The `desc.flags.isDirectSwap ()` flag is not used in the `OneInchExchange` code nor in any code called from `OneInchExchange.swap`. We recommend that you ensure that all planned logic is implemented.

Status:

ACKNOWLEDGED

COMMENTS

1. OneInchFlags.sol#L14-L36

The `flags & flag == flag` expressions can be rewritten as `flags & flag! = 0`. So you don't have to repeat the constant.

2. OneInchExchange.sol#L91

In the `else` branch, here you can offer an emit event indicating an unsuccessful exchange with a reason from the `reason` among the arguments.

3. OneInchFlags.sol#L26

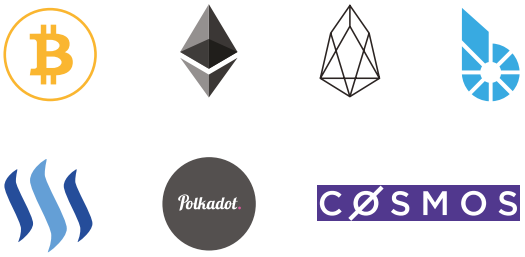
The `isDiscountChi ()` flag, if desired, can be replaced with the combination `isBurnFromMsgSender () || isBurnFromTxOrigin ()`.

ABOUT MIXBYTES

MixBytes is a team of blockchain developers, auditors and analysts keen on decentralized systems. We build open-source solutions, smart contracts and blockchain protocols, perform security audits, work on benchmarking and software testing solutions, consult universities and enterprises, do research, publish articles and documentation.

Stack

Blockchains



JOIN US