G0 Group

Security Review of

Reality 3.0

August 2021

Reality 3.0 / August 2021

Files in scope

- https://github.com/RealityETH/monorepo/blob/064855bfd8c80a0bcf3da7b73936ce477e99b635/packages/contracts/development/contracts/RealityETH-3.0.sol
- https://github.com/RealityETH/monorepo/blob/064855bfd8c80a0bcf3da7b73936ce477e99b635/packages/contracts/development/contracts/RealityETH_ERC20-3.0.sol

Current status

All issues have been fixed by the developer. There are no know issues in https://github.com/RealityETH/monorepo/blob/e4584d7cf6ab2d9a5b129bd970b7d4517811ae6a.

Issues

1. Incorrect bond payout on UNRESOLVED_ANSWER

type: faulty implementation / severity: medium

When last answer is unrevealed and best answer is UNRESOLVED_ANSWER, the bond from the unrevealed answer will be paid to `address(0)` instead of to the winner which would we be the case if the best answer wasn't an UNRESOLVED_ANSWER.

status - fixed

Issue has been fixed and is no longer present in

https://github.com/RealityETH/monorepo/blob/e4584d7cf6ab2d9a5b129bd970b7d4517811ae6a

2. Arbitration can be initiated even with no valid answer, resulting in premature finalisation after the arbitration is cancelled

type: security / severity: medium

Arbitration can be initiated after an answer commitment is posted, even if no revealed answers have been posted, after this arbitration is cancelled the question will be finalised after `finalize_ts` seconds, even though no answer has been provided. In results all bonds will be paid out to `address(0)`, bounty will become unretrievable and `best_answer` will be set to `0`.

status - fixed

Issue has been fixed and is no longer present in

https://github.com/RealityETH/monorepo/blob/e4584d7cf6ab2d9a5b129bd970b7d4517811ae6a

3. answer_takeover_fee credited to second answer depends on the way answers are processed

type: security / severity: medium

In `claimWinnings` `answer_takeover_fee` is inconsistently calculated, it is being subtracted from `bounty` if the winning answer and second best answer are processed in one go, but if they are processed separately, the whole `bounty` amount is reserved for the winner and can't by used for the fee.

status - fixed

Issue has been fixed and is no longer present in

https://github.com/RealityETH/monorepo/blob/e4584d7cf6ab2d9a5b129bd970b7d4517811ae6a

Notes

RealityETH_ERC20-3.0.sol should not be used with ERC20-like token contracts that implement callbacks like ERC777 due to potential re-entrancy issues.