G0 Group

Security Review of

Hashi

May 2023

Hashi / May 2023

Files in scope

All solidity files in https://github.com/gnosis/hashi/tree/78445a57545a60266545ed6d8337fa3ef3c69b9c/contracts

Current status

All discovered issues have been fixed or addressed. No known issues are present in:
https://github.com/gnosis/hashi/tree/9f373635730b59478bf23215906fdb5ad525d3b7/packages/evm/contracts

Issues

1. In MessageExecutor.executeMessagesFromOracles, re-entrancy allows the same call to be executed multiple times.

type: security / severity: critical

In `MessageExecutor.executeMessagesFromOracles` `executed[id]` should be updated before external call, otherwise re-entrancy can lead to the call being executed multiple times.

status - fixed

The issue has been fixed and is no longer present in:
https://github.com/gnosis/hashi/tree/9f373635730b59478bf23215906fdb5ad525d3b7/packages/evm/contracts

2. In Yaru.executeMessages, re-entrancy can lead to sender variable changing before external call terminates

type: security / severity: major

If `Yaru.executeMessages` is re-entered, the `sender` variable can change before the original call terminates, due to this I'd recommend making this function non-reentrant, for example by checking that `sender == address(0)` at the beginning.

https://github.com/gnosis/hashi/blob/9d6a0eda0a92b352c575d83b5b64f5fe882c6438/packages/evm/contracts/Yaru.sol#L50

status - fixed

The issue has been fixed and is no longer present in:https://github.com/gnosis/zodiac-modifier-roles/tree/c824d7b2b71f3dece080686640e51754bc57a654/packages/evm/contracts