G0 Group

Security Review of

Zodiac Exit Module

January 2022

Zodiac Exit Module / January 2022

Files in scope

The following solidity files in: https://github.com/gnosis/zodiac-module-exit/tree/c13f1e9f4bdccf6616cebd7b8e4be6134d54247f/packages/contracts/contracts

- CirculatingSupply.sol
- CirculatingSupplyERC721.sol
- ExitBase.sol
- ExitERC20Module.sol
- ExitERC721Module.sol

Current status

All found issues have been fixed or addressed.

Issues

1. CirculatingSupplyERC721 is missing functionality to exclude returned tokens

Severity: critical

The purpose of `CirculatingSupply` contract is specifically to exclude tokens held by the avatar, so that when someone returns tokens, circulating supply decreases along with the balance of funds that have been withdrawn, in the absence of that people who withdraw later will receive less funds. CirculatingSupplyERC721 needs to implement the same functionality.

status - fixed

The issue is no longer present in: https://github.com/gnosis/zodiac-module-exit/tree/2341cf0375b8f78b0dc3bd4d0d7ee864e1a6f804/packages/contracts/contracts

2. Exit function should have a re-entrancy guard

Severity: medium

There should be a reentrancy guard on the exit functions, since during exit, it’s possible to reenter the contract with another exit, which will affect payouts.

status - fixed

The issue is no longer present in: https://github.com/gnosis/zodiac-module-exit/tree/2341cf0375b8f78b0dc3bd4d0d7ee864e1a6f804/packages/contracts/contracts