G$_0$ Group

Security Review of

Zodiac Exit Module

September 2021

Zodiac Exit Module / September 2021

Files in scope

https://github.com/gnosis/zodiac-module-exit/blob/6ba501d62f307b63d829d70392a850967d1d27ca/contracts/ExitModule.sol
https://github.com/gnosis/zodiac-module-exit/blob/6ba501d62f307b63d829d70392a850967d1d27ca/contracts/CirculatingSupply.sol

Current status

All issues have been fixed by the developer. There are no known issues in
https://github.com/gnosis/zodiac-module-exit/tree/4e7029acf8c71727f484ca0b1873de021964d3c7

Issues

1. tokens array argument of the exit function can contain duplicates

type: security / severity: critical

If `tokens` array in `exit` function contains the same token address multiple times, the exiting user will be paid out multiple shares of the tokens in the DAO's custody instead of just one.

status - fixed

Issue has been fixed and is no longer present in

https://github.com/gnosis/zodiac-module-exit/tree/4e7029acf8c71727f484ca0b1873de021964d3c7

2. Circulating supply should be reduced on exit

type: incorrect implementation / severity: major

Circulating supply should be reduced on`exit`, otherwise withdrawed amounts won't be consistent between `exit` calls.

status - fixed

Issue has been fixed and is no longer present in

https://github.com/gnosis/zodiac-module-exit/tree/4e7029acf8c71727f484ca0b1873de021964d3c7

Notes

It’s important to make sure there is no situation where there’s temporary token imbalance in the avatar contract with possibility of external call to an untrusted address. For example if there was some token exchange functionality in the avatar that first takes `tokenA` from the buyer, then makes an external call and then transfers proportional amount of `tokenB` to the buyer. Between `tokenA` inflow and `tokenB` outflow there’s an imbalance where the contract has higher total value in custody than in the final state, if attacker would be able to exit at this moment and withdraw both `tokenA` and `tokenB` they will receive more tokens than they should. This is only a hypothetical issue, but it’s something to keep in mind.