G₀ Group

Security Review of

Zodiac Delay Module

September 2021

Zodiac Delay Module / September 2021

Files in scope

https://github.com/gnosis/zodiac-modifier-delay/blob/bde282125ebbe119df4bfd6374e097007a13fb8a/contracts/Delay.sol

Current status

All issues have been fixed by the developer. There are no known issues in https://github.com/gnosis/zodiac-modifier-delay/blob/808dfda6fd0ea144bbbe83e419e14045a029ca5d/contracts/Delay.sol

Issues

1. Reentrancy attack allows one transaction to be executed multiple times

type: security / severity: critical

In `executeNextTx` `txNonce` is incremented after `exec` is called, this allows a reentrant subcall of `exec` to call `executeNextTx` again with the same arguments and execute the same transaction again.

status - fixed

Issue has been fixed and is no longer present in

https://github.com/gnosis/zodiac-modifier-delay/blob/808dfda6fd0ea144bbbe83e419e14045a029ca5d/contracts/Delay.sol

2. In skipExpired, txNonce can be incremented to be higher than queueNonce

type: security / severity: major

Since the while loop in `skipExpired` keeps iterating until `txNonce <= queueNonce` and every iteration will increase `txNonce` by none, the last iteration will result in `txNonce > queueNonce`, this will lead to next qued transaction being skipped.

status - fixed

Issue has been fixed and is no longer present in

https://github.com/gnosis/zodiac-modifier-delay/blob/808dfda6fd0ea144bbbe83e419e14045a029ca5d/contracts/Delay.sol

3. Deactivation of transaction expiration is not respected in executeNextTx

type: incorrect implementation / severity: major

In `executeNextTx` require on `line 150` doesn't reflect that `txExpiration == 0` is a special state that should lead to the skipping of expiration check.

status - fixed

Issue has been fixed and is no longer present in

https://github.com/gnosis/zodiac-modifier-delay/blob/808dfda6fd0ea144bbbe83e419e14045a029ca5d/contracts/Delay.sol

4. Inconsistently defined expiration periods between functions

type: inconsistency / severity: minor

Executable period defined in `executeNextTx` and expired period defined in `skipExpired` are not continuous.

status - fixed

Issue has been fixed and is no longer present in

https://github.com/gnosis/zodiac-modifier-delay/blob/808dfda6fd0ea144bbbe83e419e14045a029ca5d/contracts/Delay.sol

Note

It should be kept in mind that if all DAO calls are routed through the Delay module, including calls to the Delay module itself, there's a threat of a broken transaction blocking calls that would normally be used to skip it. This is especially problematic if transactions have no expiration.