G_0 Group

Security Review of

Gnosis Safe 1.3.0

April 2021

Gnosis Safe 1.3.0 / April 2021

Files in scope

All solidity files in:

https://github.com/gnosis/safe-contracts/tree/4bfc0c8519f1893015d7edfd2c2780fca163c364

Current status

No serious issues have been discovered.

Report

Issues

No issues have been discovered.

Notes

1. `GnosisSafe.signMessage` could be optimized by providing a hash instead of data
2. `GnosisSafeProxyFactory.calculateCreateProxyWithNonceAddress` has unused return value
3. In `SecuredTokenTransfer` the boolean return value of the call could be directly written to scratch space by the call function instead of using returndatacopy to retrieve it
4. Some contracts implement a check that detects whether a code is being delegatecalled, there's a possible cheaper alternative to the current implementation based on storing the contract's address in an immutable in the contract's constructor and then comparing it with `address(this)` when the call is being called
5. Uniqueness check on the `_owners` array in `OwnerManager.setupOwners` could be implemented in a cheaper way if the array of owners was required to be sorted. Checking that `currentOwner < owner` in the for loop would ensure there are no duplicates.

Suggestions in notes 3. and 4. have been implemented in:https://github.com/gnosis/safe-contracts/commit/9b305a0f80da7f1107d1181f52c844f089557d05