G0 Group

Security Review of

Argent RecoveryManager vulnerability fix

June 19, 2020

Argent RecoveryManager vulnerability fix / June 2020

Files in scope

This is a review of a fix to a vulnerability present in `RecoveryManager.sol` that has been added in this commit:

https://github.com/argentlabs/argent-contracts/commit/268b7ddcd2945e22970b96a8ed7497dc239ea22a

Summary of the vulnerability

The original issue was caused by `getRequiredSignatures` returning `0` for metatransaction calls to `executeRecovery` function when the number of guardians was `0` as a result of this calculation: `SafeMath.ceil(guardianStorage.guardianCount(_wallet), 2)`. This is interpreted by the system to mean that anybody can call the `executeRecovery` when no guardians are present.

Summary of the fix

The issue was fixed by throwing an exception when a call to `executeRecovery` is attempted with `0` guardians. We confirm the fix is sufficient and doesn't introduce any new issues.