G0 Group

Security Review of

Gnosis safe gas validation adjustment

May 4, 2020

Gnosis safe gas validation adjustment / April 2020

Files in scope

Following solidity files

https://github.com/gnosis/safe-contracts/blob/271921f4b37613b3d49bf33452dbcd81be219247/contracts/base/ModuleManager.sol
https://github.com/gnosis/safe-contracts/blob/271921f4b37613b3d49bf33452dbcd81be219247/contracts/GnosisSafe.sol

Current status

As of May 4th 2020 all reported issues have been fixed by the developer

Issues

1. Due to incorrect calculation of a gas overhead needed due to EIP-150, relayers can force transactions to fail by not providing enough gas

Type: security / Severity: medium

EIP-150 limits gas provided to child calls to 63/64 of the gas available in the parent call after all of the other call related costs are subtracted. This means that to ensure an `x` amount of gas is available to the child call, there must be at least `x*64/63` gas available in the parent call after all other costs needed to execute the call have been subtracted. This can be proved by the following equality: `(x*64/63) * 63/64 = x`. In the audited version, a calculation of`x*65/64` was used instead which is insufficient, as illustrated in the following inequality: `(x*65/64) * 63/64 < x`. This allows a malicious relayer to intentionally provide low amount of gas to force the child call to fail while the parent call successfully finishes, burning the transaction nonce in the process.

status - fixed

Issue has been fixed in the following commit
https://github.com/gnosis/safe-contracts/commit/62d4bd39925db65083b035115d6987772b2d2dca