Past paid bounties

This list includes valid submissions from past and current contract versions for which a bounty has been paid.

Potential suicide of MultiSend library

We use aMultiSend(opens in a new tab) library to batch multiple transactions together. A transaction could be created that would self-destruct the contract. While this would not have put any funds at risk, user experience would have been seriously impacted.

We've updated the library as well as our interfaces. Details about the fix can be found onGitHub(opens in a new tab) .

This bug was submitted byMicah Zoltu(opens in a new tab) . It was regarded as a "Low Threat," and a bounty of 1,000 USD has been paid out.

Transaction failure when receiving funds viatransfer

orsend

Since the beginning of the bug bounty period, the contract update has been live on the Ethereum Mainnet. We performed extensive internal testing and discovered an edge case where a Safe couldn't receive funds from another contract viasend ortransfer . This was due to additional gas costs caused by theemission of additional events(opens in a new tab)andgas price changes(opens in a new tab) in the latest hard fork. This issue has been fixed, and more details can be found onGitHub(opens in a new tab) .

Duplicate owners during setup could render Safe unusable

A bug in thesetupOwners function onOwnerManager.sol allows duplicate owners to be set when the duplicated address is next to itself in the_owners array. This could cause unexpected behavior. While stealing funds from existing Safes is impossible, it's unexpected, and user funds might be locked. During Safe creation, the threshold of a Safe could be set to something unreachable, making it impossible to execute a transaction afterward.

The Safe interfaces prevent this by checking for duplicates, but if users directly interact with the contracts, this can still happen. The issue is tracked onGitHub(opens in a new tab) .

This bug was submitted byDavid Nicholas(opens in a new tab) . It was regarded as a "Medium Threat," and a bounty of 2,500 USD has been paid out.

Setting a Safe as an owner of itself essentially reduces the threshold by 1

The contracts allow to set a Safe as an owner of itself. This has the same effect as lowering the threshold by 1, as it's possible for anyone to generate a valid signature for the Safe itself when triggeringexecTransaction . This is especially an issue for Safes with a threshold of 1. Anyone can execute transactions if a Safe with threshold 1 adds itself as an owner.

To our knowledge, there is no actual use case where it would make sense to set a Safe as an owner of itself. Hence, only a few number of Safes used themselves as owners. Most of these Safes could be contacted, and the Safe has been removed as an owner. The Safes still affected are Safes used for testing by us or Safes owned by a single owner with a threshold > 1 (so no immediate risk).

To fix this, the next contract update will prevent the Safe as its owner viarequire(owner != address(this), "Safe can't be an owner") . This check can be performed when adding owners and/or when checking signatures.

Details about this issue can be found onGitHub(opens in a new tab) .

The bug was submitted byKevin Foesenek(opens in a new tab) . It was regarded as a "Medium Threat," and a bounty of 5,000 USD has been paid out.

The functiongetModulesPaginated

doesn't return all modules

The methodgetModuledPaginated(opens in a new tab) is used to return enabled modules page by page. For this, astart and apageSize need to be specified, and the method will return an array of Safe Module addresses andnext . This next can be used as thestart to load the next page. When another page exists, thennext is a module address. This module address, however, won't be present in any of the returned arrays. While this doesn't put any user assets at risk directly, it could lead to a wrong perception of the enabled modules of a Safe and, thereby, its state.

The workaround is to append thenext to the returned array of module addresses if it's not the zero or sentinel address. Alternatively, the last element of the returned array can be used as thestart for the next page.

This bug was submitted byRenan Souza(opens in a new tab). It was regarded as a "Low Threat," and a bounty of 2,000 USD has been paid out.

Bug Bounty Service Architecture

Was this page helpful?

Report issue