G₀ Group

Security Review of

Nexus Mutual: Distributor

March 2021

Overview

G0 Group was engaged to perform a security review of Nexus Mutual's distributor contracts and corresponding contract upgrade. This review is the product of a five person-day effort to that end. The primary subjects of this review were contracts which enable mutual members to launch and run cover distributors. This review was initially performed on
https://github.com/NexusMutual/distributor-contract/commit/98ec7fab659339fd0bf1b44d2362b3818dd1164c

https://github.com/NexusMutual/smart-contracts/commit/d0aeb546cbad7bc8f61e3d8b9737f105e90b0d48

https://github.com/NexusMutual/smart-contracts/commit/78796d76cd7cf43b8232f4c2ff6d839732ca9ed2

Scope

```
smart-contracts/
  contracts/
    modules/
      claims/
        Claims.sol
      cover/
        Quotation.sol
        Cover.sol
      governance/
        MemberRoles.sol
      token/
        TokenController.sol

distributor-contract/
  contracts/
    Distributor.sol
    DistributorFactory.sol
```

Result Summary

During the course of this review, 1 medium severity issue was discovered and addressed.

All fixes are present, and no further issues were discovered in:
https://github.com/NexusMutual/distributor-contract/commit/cf7cce7371af8ceec26a3136efa51facb4e303d3

https://github.com/NexusMutual/smart-contracts/commit/0cbc92c9b3abfa13848a78ed5b4d4388c25fc76f

Issues

1. Owner of distributor contract can steal from cover purchasers by front-running them with an exorbitant fee hike

Type: *security* / ***Severity:*** *medium*

This issue specifically pertains to cover purchases denominated in ERC20 tokens (i.e. not ETH). When interacting with contracts that “transferFrom” tokens, it is common for users to approve those contracts for the max value. This means the owner of the distributor contract could front-run a “buyToken” tx, with their own “setFeePercentage” tx crafted to set the fee to a such a high value that the “transferFrom” in “buyToken” would drain the entirety of the buyer’s balance.

Fix Description:

Add a parameter to “buyToken” for the maximum acceptable price for the cover + fee, revert if the calculated price exceeds this value.