G₀ Group

Security Review of

Nexus Mutual: Claim Payout Upgrade

November 2020

Overview

G0 Group was engaged to perform a security review of Nexus Mutual's claim payout address update in collaboration with Daniel Luca (https://cleanunicorn.xyz/). This review is the product of a six person-day effort to that end. The primary subjects of this review were contract upgrades which enable members to specify a claim payout address different than their member address. This review was initially performed on https://github.com/NexusMutual/smart-contracts/commit/a3fa29c70143f9ed749621971df9cbd6684eb8ad.

Scope

```
contracts/
  modules/
    claims/
      ClaimsReward.sol
    governance/
      MemberRoles.sol
```

Result Summary

During the course of this review, 1 medium, 1 minor, and 1 informational issue were addressed. Issues marked with an asterisk were previously disclosed, and were included for fix validation.

All fixes are present, and no further issues were discovered in: https://github.com/NexusMutual/smart-contracts/commit/a7f8f7077a688c4a08a7a49396b18c408bea4e2f

Issues

1. User can misconfigure claim payout address

Type: *security* / ***Severity:*** *low*

Claim payouts are sent to the member's address by default. This default is recorded as the member's claim address set to 0x0.

Misconfiguration Scenario:
1. User changes their claim payout address

2. User intends to change their claim payout address back to their member address, and does so "manually": setting it to their literal address instead of setting to 0x0

3. User switches membership to a 3rd address

4. Their claim payout address is still their old membership address, when the user likely expects it to be set to their new membership address

Fix Description:

This issue was addressed by:
1. Not allowing claim payout address to be set to the current member address
2. If a user sets their member address to their current claim payout address, set their claim payout address to 0x0
3. If a user withdraws membership and their claim payout address is not set to 0x0, set it to 0x0

*2. Accepted claims not updated to terminal status can lead to repeated payouts

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

Claims were not being updated from accepted statuses to terminal status on payout. This allows a claimant to resubmit a claim which has already been paid. Claims assessors/members would need to accept those resubmitted claims for a repeated payout to occur, however it's still a griefing vector until governance can intervene.

Fix Description:

This issue was addressed by adding the missing code path to update accepted claims to terminal status on pay out. Three paid claims' statuses were stuck in the manner described above, and were migrated to terminal status by this upgrade.

3. Recommendation: Emit an event when a claim payout address is changed

Type: *informational*

Emitting an event would allow for easier access of historical data/event listening for the front-end/monitoring services.

Fix Description:

The event was added.