G_0 Group

Security Review of

Gnosis Protocol Token

December 2021

Gnosis Protocol Token / December 2021

Files in scope

The Solidity files whose content match the following sha256 hashes:

```
a3066be820b433d1fc47e854c806a0d82d9fbb1d2362ea81e9f497893756ab08
src/contracts/CowSwapVirtualToken.sol
7dd3764ed525f1e0a34769bd1d58f9da6a1f80e23eefabb068c81ace573ca02e
src/contracts/vendored/libraries/Strings.sol
fbc417655bec31de8c2d08926cdd533a11c1188f773d6153161f3c7a451f06ad
src/contracts/vendored/libraries/ECDSA.sol
5a726b4159a6fa207fcaf5dbcb25498fadf4c6de2cccf538a7e233b261f4ae78
src/contracts/vendored/libraries/Counters.sol
c8a9310200fec6294ed6c23fa651de55dd86a63139601e56b57f1c1cbb679a51
src/contracts/vendored/libraries/SafeERC20.sol
f1dc5e6badaac071d8c3292b19db8c132d51b9ad32b10894b9fc997fdbb8b298
src/contracts/vendored/libraries/MerkleProof.sol
e6c036cb3b1b6b17e64f2d4d80fb5496c7e6e9b5d2fefb6ccbc99a7eaed0830e
src/contracts/vendored/libraries/Math.sol
ea852d8d1cacd25a952a1d5f960efad7862a7bd93f60caea75d6f0f0e68a21ec
src/contracts/vendored/readme.md
02f466d516b35ddae0770db78b651ef446ae0bef31ba279cb32cbb97a85ce3d0
src/contracts/vendored/interfaces/draft-IERC20Permit.sol
293709d531f367b1499f3cb4d5271f36002f92ada3ddd04d9d2ebc8bf2e9cdb0
src/contracts/vendored/interfaces/IERC20Metadata.sol
11403ec779ea104b7dd27ac27758abbad98043204b912d1241dbaee6126bd09d
src/contracts/vendored/interfaces/IERC20.sol
5d9c7c593c71f5e3474384ad5d5efddbf2b168542cc29c0363ebfe86163eba94
src/contracts/vendored/interfaces/Context.sol
84925045d19fb29dc2c87e9d723cca125956681de87e9bf31e9ab7b0cc6929e6
src/contracts/vendored/mixins/ERC20.sol
480548df0b26d1c59ed07ce3729bf6afa3c7db5d6a9318872dae84048ed494fc
src/contracts/vendored/mixins/draft-ERC20Permit.sol
55add03449b6442b86c0d05c47129726335dd8406b8ad8525f3424c92e97be7f
src/contracts/vendored/mixins/StorageAccessible.sol
4604a59049751095c28df693134a82bcbb84f53947e505e0d69f3e1635291125
src/contracts/vendored/mixins/draft-EIP712.sol
b365918eea1ea4bd9dc074e07a5cba4e07f5ed6cb7d2463258c3917e8a368173
src/contracts/interfaces/ClaimingInterface.sol
f4f4a08e48574dfcbe8cd7db37033ff42ef26feda98a3a88bb023081b53a3639
src/contracts/interfaces/VestingInterface.sol
60a009dd7b58e312d08f105edb08d0c93bac3bf1dbba5f8a9dfe1247c331510e
src/contracts/CowSwapToken.sol
fc70059775f429383aed29ab0c425b4e4ab79a55c27e968101e9b69f4a96bd48
src/contracts/mixins/NonTransferrableErc20.sol
b702cc7ba08240822f7aca3d5f03df19322e44919e3fc5d15ece7a6bae286c92
src/contracts/mixins/Claiming.sol
85b8a23fa15831725dd3fd5d721fd0cc9603b7a9af9d39e860402fb6c29b37f1
src/contracts/mixins/InflationaryToken.sol
1d1e9aa8d2a0b65756b54cc284a8a9750554059a850064e43d6d6dfaa9092980
src/contracts/mixins/Vesting.sol
d4a1f8c563bcb12ce0cf68a726bd340af1f10d2c39e11a41a71ba2bf6af06c80
src/contracts/mixins/MerkleDistributor.sol
```

Current status

All found issues have been fixed or addressed. Following files have been updated in result of this audit:

```
c2f0ab92cc1ae9027d9cfbc5ad327d856050fea56c489e136b082bb3fa553272
src/contracts/mixins/Vesting.sol
f6c1585d1bac70e5858c0c8d57610fd46d1b515fb5f23562e45c86676c7b0fa6
src/contracts/mixins/MerkleDistributor.sol
```

Issues

1. Possible loss of funds in Vesting.shiftVesting

Severity: minor

In `Vesting.shiftVesting` there's a hypothetical possibility of `user == freedVestingBeneficiary` in which case the allocation will be lost.

status - fixed

The issue is no longer present in

```
c2f0ab92cc1ae9027d9cfbc5ad327d856050fea56c489e136b082bb3fa553272
src/contracts/mixins/Vesting.sol
```

2. All allocations of an address with one cancellable allocation will end up cancellable

Severity: minor

In `Vesting.addVesting` in case an address has an allocation `ClaimType.Team` all other allocations of the address will end up cancellable regardless of their `ClaimType`.

status - addressed

The issue will be worked around by never including other types of allocation for an address that has `ClaimType.Team`.

Notes

- `Vesting.cumulativeVestedBalance` can be optimized by modifying the included statement to: `Math.min(block.timestamp - vestingStart, VESTING_PERIOD_IN_SECONDS) * fullAllocation[user] / VESTING_PERIOD_IN_SECONDS`
- Two for loops in `MerkleDistributor.claimMany` can be merged into one