PeriodicTokenVesting Audit Report

Date: 2022-12-02
Auditor: Xinghui Chen
Email: ChenXinghui@protonmail.com

Summary

Scope

PeriodicTokenVesting.sol
https://github.com/decentraland/vestings-builder/blob/ad906381b96f23c0b82a9ba89cf3466914448139/contracts/PeriodicTokenVesting.sol

Findings

	Critical	High	Middle	Low	Gas	Recommendation
PeriodicTokenVesting.sol	-	-	-	1	1	4

Audit revision

PeriodicTokenVesting.sol
https://github.com/decentraland/vestings-builder/blob/c80ee3e49e525ab6f541a84ab5e58cdf634a771a/contracts/PeriodicTokenVesting.sol

Details

Low risk

1. When `isPausable` and `isRevocable` are both true, if owner call `pause()` at stampA and later call `revoke()` at stampB, `stop` will be set to stampB. However, it should remain stampA as vesting has been paused already. So line 328 should be:

   ```
   if (!paused()) { // or if (stop == 0) {
         stop = block.timestamp;
   }
   ```

   Result: Changed.

Gas optimization

1. In `getTotal` funciton, as `vestedPerPeriod` will always contains multiple items, and array boundary check will access storage slot, it's better to copy into memory first. e.g.,

   ```
   uint256[] memory memVestedPerPeriod = vestedPerPeriod;
   for (uint256 i; i < memVestedPerPeriod.length; ) {
       total += memVestedPerPeriod[i];
   ```

   Result: Changed.

Recommendation

1. in `constructor` function, it's better to add `_transferOwnership(_msgSender());`. Then, if vesting tokens are tranferred to the implemention contract by mistake, deployer can call `releaseForeignToken` to rescue them.

   Result: Not change.

2. In `initialize` function, it's safer to check `start` param. e.g., `require(_start != 0, xx)` . Maybe better to check the upper limit(especially when `isRevocable` is false).

   Result: Changed.

3. In `initialize` function, it's safer to check the upper limit of `cliff` param(especially when `isRevocable` is false). For example, `cliff < _vestedPerPeriod.length * _period`.

   Result: Not change. It maybe a bit dangerous if `isRevocable` is false and `cliff` is set too big by mistake.

4. `pragma solidity ^0.8.17` could be changed to `pragma solidity 0.8.17`, for more detail please visit here.

   Result: Changed. And downgrade to 0.8.2.