NereusShapeshiftersMarket Contract Code Audit by Ambisafe Inc.

August, 2022

Artem Martiukhin, Oleksii Matiiasevych

1. **Introduction.** Nereus Finance requested Ambisafe to perform a code audit of the contracts implementing NereusShapeshiftersMarket. The contracts in question can be identified by the following git commit hash:

   `e0aecc7960f737cb0bad3a1eacd4114fcca8fe63`

   The scope of the audit is NereusShapeshiftersMarket contract.

2. **Disclaimer.** The code audit makes no statements or warranties about utility of the code, safety of the code, suitability of the business model, regulatory regime for the business model, or any other statements about fitness of the contracts for any specific purpose, or their bugfree status.

3. **Executive Summary.** There are **no** known compiler bugs for the specified compiler version (0.8.7), that might affect the contracts' logic. There were 0 critical, 0 major, 1 minor, 2 informational and optimizational issues identified in the initial version of the contract.

4. **Critical Bugs and Vulnerabilities.** No critical bugs or vulnerabilities were found.

5. **Line By Line Review. Remaining and Acknowledged Issues.**

   5.1. NereusShapeshiftersMarket, line 166. Minor, there is no check that provided wave prices length is equal to claim allowance in **addWhitelistableSaleWave()**. This might result in some of them being free. Either add a check as in addSaleWave() or use the prices length instead of allowance.

   5.2. NereusShapeshiftersMarket, lines 266-281. Optimization, this functionality repeats the functionality of **getWavePriceForAddress()** function, so the copy of code could be replaced with public function call

5.3. NereusShapeshiftersMarket, line 347. Optimization, “transfer” usage is not recommended to use as legacy functionality, it might stop working in the future, especially for contract receivers. Use a helper like Address.sendValue() from OpenZeppelin.

Oleksii Matiiasevych

Artem Martiukhin