



DeXe Platform StakingProposal Update Code Audit And Verification by Ambisafe Inc.

December 2024

Oleksii Matiasevych

1. **INTRODUCTION.** DeXe Network requested Ambisafe to perform a code audit of the DeXe Platform StakingProposal contract along with the updates to their other contracts that interact with it. The code in question can be identified by the following git commit hash diff:

```
c0291bcc1fbf0db794f3299da5887e08446e753c
...
f7ef4b290c949f16a5770b5f1259b581f4841017
```

All changes are in scope and include a number of updates that the DeXe Network team applied during the audit.

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 (0.8.20), that might affect the contracts' logic. There were 0 critical, 0 major, 2 minor, 2 informational and optimizational findings identified in the initial version of the contracts. All the findings were addressed and were not found in the final version of the code, they are listed below for historical purposes.
4. **CRITICAL BUGS AND VULNERABILITIES.** No critical issues were identified.
5. **LINE BY LINE REVIEW. FIXED FINDINGS.**
 - 5.1. StakingProposal. Minor, the **claim()** function could be called by anyone on a valid finished tier to emit a RewardClaimed event multiple times.

- 5.2. StakingProposal. Minor, the **reclaim()** function could be called by anyone on a valid finished tier to emit a RewardClaimed event multiple times.
- 5.3. StakingProposal. Note, the **StakingCreated** event doesn't have a tier **id** parameter.
- 5.4. StakingProposal. Note, the **createStaking()** function does not emit a **StakingCreated** event in case of the already finished staking creation.



Oleksii Matiasevych