Quantstamp Security Assessment Certificate

April 26th 2021 — Quantstamp Verified

Tera Stake Finance

This smart contract audit was prepared by Quantstamp, the protocol for securing smart contracts.

Executive Summary

Type	Token Yield Aggregator
Auditors	Ed Zulkoski, Senior Security Engineer Kacper Bąk, Senior Research Engineer Poming Lee, Research Engineer Sebastian Banescu, Senior Research Engineer
Timeline	2019-12-02 through 2021-04-23
EVM	Muir Glacier
Languages	Solidity, Javascript
Methods	Architecture Review, Unit Testing, Functional Testing, Computer-Aided Verification, Manual Review
Specification	README.md
Documentation Quality	Medium
Test Quality	Medium
Source Code	

Repository	Commit
tera-stake-contracts	937f989 (initial audit)
tera-stake-contracts	b5fb299 (latest audit)

Goals

- Do functions have proper access control logic?
- Are there centralized components of the system which users should be aware?
- Do the contracts adhere to best practices?

Total Issues	**39** (25 Resolved)
High Risk Issues	0 (0 Resolved)
Medium Risk Issues	**4** (4 Resolved)
Low Risk Issues	**11** (9 Resolved)
Informational Risk Issues	**18** (8 Resolved)
Undetermined Risk Issues	**6** (4 Resolved)

High Risk	The issue puts a large number of users' sensitive information at risk, or is reasonably likely to lead to catastrophic impact for client's reputation or serious financial implications for client and users.
Medium Risk	The issue puts a subset of users' sensitive information at risk, would be detrimental for the client's reputation if exploited, or is reasonably likely to lead to moderate financial impact.
Low Risk	The risk is relatively small and could not be exploited on a recurring basis, or is a risk that the client has indicated is low-impact in view of the client's business circumstances.
Informational	The issue does not post an immediate risk, but is relevant to security best practices or Defence in Depth.
Undetermined	The impact of the issue is uncertain.
Unresolved	Acknowledged the existence of the risk, and decided to accept it without engaging in special efforts to control it.
Acknowledged	The issue remains in the code but is a result of an intentional business or design decision. As such, it is supposed to be addressed outside the programmatic means, such as: 1) comments, documentation, README, FAQ; 2) business processes; 3) analyses showing that the issue shall have no negative consequences in practice (e.g., gas analysis, deployment settings).
Resolved	Adjusted program implementation, requirements or constraints to eliminate the risk.
Mitigated	Implemented actions to minimize the impact or likelihood of the risk.