PowerPool Vesting v2 Security Analysis

by Pessimistic

This report is public.

Published: November 2, 2020

Abstract

In this report, we consider the security of CVP token vesting v2 contract of the PowerPool project. Our task is to find and describe security issues in smart contracts of the platform.

Disclaimer

The audit does not give any warranties on the security of the code. One audit cannot be considered enough. We always recommend proceeding with several independent audits and a public bug bounty program to ensure the security of smart contracts. Besides, security audit is not an investment advice.

Summary

In this report, we considered the security of CVP token vesting v2 contract of PowerPool project. We performed our audit according to the procedure described below.

The analysis showed no vulnerabilities. The code is of good quality.

General recommendations

We do not have any further recommendations.

Procedure

In our audit, we consider the following crucial features of the code:

1. Whether code logic corresponds to the specification.
2. Whether the code is secure.
3. Whether the code meets best practices.

We perform our audit according to the following procedure:

- Manual audit
  - We inspect the specification and check whether the logic of smart contracts is consistent with it.
  - We manually analyze code base for security vulnerabilities.
  - We assess overall project structure and quality.
- Report
  - We reflect all the gathered information in the report.

Project overview

Project description

In our analysis we consider CVP vesting v2 contract of PowerPool project on GitHub repository, commit 782ed8373eeb39d648a7bc7469c6d48eda4643aa, and the specification, commit 78ec735fe386c9a980d1cbafb7fd600f03bad796.

The total LOC of audited sources is 376.

Manual analysis

The contracts were completely manually analyzed, their logic was checked. Besides, the results of the automated analysis were manually verified. All the confirmed issues are described below.

Critical issues

Critical issues seriously endanger smart contracts security. We highly recommend fixing them.

The audit showed no critical issues.

Medium severity issues

Medium issues can influence project operation in current implementation. We highly recommend addressing them.

The audit showed no medium severity issues.

Low severity issues

Low severity issues can influence project operation in future versions of code. We recommend taking them into account.

The audit showed no low severity issues.

This analysis was performed by Pessimistic:

Evgeny Marchenko, Senior Security Engineer

Igor Sobolev, Security Engineer

Boris Nikashin, Analyst

Alexander Seleznev, Founder

November 2, 2020