GGMT Token Security Analysis

by Pessimistic

This report is public

April 28, 2023

Abstract

In this report, we consider the security of smart contracts of GGMT ERC20 project. Our task is to find and describe security issues in the smart contracts of the platform.

Disclaimer

The audit does not give any warranties on the security of the code. A single 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, a security audit is not investment advice.

Summary

In this report, we considered the security of GGMT ERC20 smart contracts. We described the audit process in the section below.

The audit showed one issue of medium severity: Discrepancy with the documentation, and the developers promptly addressed it.

General recommendations

We have no further recommendations.

Project overview

Project description

For the audit, we were provided with GGMT ERC20 project on a public GitHub repository, commit c972845dba28f1d18de73368711c8ccf926f0eb7, and a deployed contract address 0x76aAb5FD2243d99EAc92d4d9EBF23525d3ACe4Ec.

The scope of the audit includes the whole repository.

The documentation for the project is available at https://docs.ggmt.io/tokenomics/ggmt-metrics.

The total LOC of audited sources is 151.

Token details:

Name:	Green Grey MetaGame Token
Symbol:	GGMT
Decimals:	18
Total Supply:	10 000 000 000

Audit process

We started the audit on April 13, 2023, and finished on April 14, 2023.

We inspected the materials provided for the audit.

We manually analyzed all the contracts within the scope of the audit and checked their logic. Among other, we verified the following properties of the contracts:

- Conformance with the ERC20 standard;
- The provided contract address 0x76aAb5FD2243d99EAc92d4d9EBF23525d3ACe4Ec source code is equivalent to the audited code;
- The token's name, symbol, and decimal parameters are the same as provided in the documentation (see M01).

We ran tests and calculated the code coverage.

We combined in a private report all the verified issues we found during the manual audit.

Later the developers updated the documentation to match the source code and the deployed contract. They also provided a comment for the low-severity issue. We reflected this update in the report.

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 project security. They can lead to loss of funds or other catastrophic consequences. The contracts should not be deployed before these issues are fixed.

The audit showed no critical issues.

Medium severity issues

Medium severity issues can influence project operation in the current implementation. Bugs, loss of potential income, and other non-critical failures fall into this category, as well as potential problems related to incorrect system management. We highly recommend addressing them.

M01. Discrepancy with the documentation (fixed)

The project documentation says that the token supply is one billion. However, according to the code and deployed contract, the token supply is 10 billion.

> *The developers have updated documentation, now it is in line with the code and deployed contract.*

Low severity issues

Low severity issues do not directly affect project operation. However, they might lead to various problems in future versions of the code. We recommend fixing them or explaining why the team has chosen a particular option.

L01. Sources (commented)

Standard code from the OpenZeppelin library is copied into the project. We recommend using it as a project dependency to follow the best practices.

> *Comment from the developers: This issue does not pose any threat to the security of the smart contract and is not meant to be addressed.*

This analysis was performed by Pessimistic:

Evgeny Marchenko, Senior Security Engineer
Yhtyyar Sahatov, Junior Security Engineer
Irina Vikhareva, Project Manager
Alexander Seleznev, Founder

April 28, 2023