TANZANITE Audit

Client	Omari Kitula
Audit By	Scrutify.io
Created On	@January 15, 2023
Network	BSC
Source Code	https://bit.ly/scrutify-0x1B014B9B81f245
Tools	Mythril Slither
Methods	Automated Analysis Confidence Check Static Analysis
Type	DApp DEX Token
Compiler	v0.8.15
# Lines of Code	384
# Vulnerabilities	23
# Score	4.27
Standard	Basic

Disclaimer

This audit report contains sensitive information about the IT systems and intellectual property of our valued client, as well as details about any vulnerabilities that were identified and the potential ways in which they could be exploited. It is intended for

internal use by the client to address and fix any vulnerabilities, but may also be publicly disclosed once all issues have been resolved.

Introduction

The client did not provide an introduction for the project. This basic audit is offered at no cost and is a quick way to identify vulnerabilities in a contract. It includes (but not all) a basic vulnerability check for code quality, access and visibility, gas optimizations, integer overflow and underflow, compiler version. It also includes an EVM bytecode analysis. However, it is important to note that this basic audit may not detect all vulnerabilities and a more comprehensive, manual audit may be necessary for a thorough analysis.

Vulnerability Indicators

#Critical

Identifies critical vulnerabilities that are usually easy to exploit and can lead to asset loss or data manipulation.

#High

Identifies vulnerabilities that are difficult to exploit, but also have a significant impact on smart contract execution, e.g., public access to crucial functions.

#Medium

Identifies vulnerabilities that must be addressed, but cannot result in asset loss or data manipulation.

#Low

Identifies vulnerabilities that are mostly related to outdated, unused, etc. code snippets that cannot have a significant impact on execution.

#Informational

Identifies vulnerabilities that are good to look at and be addressed, but can have a significant impact on execution of the smart contract, but cannot lead to any loss of fund.

#Gas

Identifies vulnerabilities that are good to look at and be addressed, but can have a significant impact on execution of the smart contract, but cannot lead to any loss of fund.

Score

Red = Poor, **Brown** = Low, **Yellow** = Average, **Green** = Good

Audit Score	**4.27** | Lines of Code: 384

> *The Scrutify score is calculated based on various factors, including the number of lines of code and the severity and confidence levels of identified vulnerabilities.*

Vulnerabilities Detected

We analyzed 5 contracts using 78 detectors resulting in a total of 23 vulnerabilities listed below. To view detailed report and comprehensive results about the vulnerabilities, we recommend purchasing our pro audit service.

▼ **#Critical - 0**

No Vulnerabilities Were Detected

▼ **#High - 0**

No Vulnerabilities Were Detected

▼ **#Medium - 0**

No Vulnerabilities Were Detected

▼ **#Low - 17**

Pragma Warning - 1 on line 6
Solidity Compiler Version - 1 on line 6
Function Shadowing - 2 on lines 271 and 439
Function visibility - 13 on lines 417-523

▼ **#Informational - 4**

Code Quality - 1 on line 6
Redundant Code - 2 on lines 126 and 197
Literals with many digits - 1 on line 211

▼ **#Gas - 2**

Gas optimisations detected for project dependencies(**unlock with pro version**)

> Upgrade to our **Pro Audit** for in-depth analysis and comprehensive results of your smart contract. Simply click here or send us an email at audits@scrutify.io to request your Pro Audit.

About Us

Scrutify is a smart contract audit platform that was founded to help businesses and individuals ensure the security and integrity of their smart contracts. Our team of experienced blockchain developers and security experts has completed over **100+ audits** and secured over **$2B+ total amount**. We conduct more than **100+ vulnerability checks**, making us one of the most trusted and reliable platforms in the industry.

At Scrutify, we are committed to providing fast and accurate results to our clients. Our proprietary algorithms and in-depth analysis techniques allow us to identify vulnerabilities and potential issues quickly and effectively. And, to further demonstrate our confidence in our services, we offer a **100% money back guarantee**.

Whether you are a business owner looking to secure your smart contracts, or an individual looking to ensure the safety of your assets, Scrutify is here to help. Contact us today to learn more about how we can protect your smart contracts and give you peace of mind.

Disclaimer

The smart contracts provided for audit have been analyzed using common industry tools. The findings of this basic audit are intended to identify vulnerabilities in the contracts, but do not guarantee the security of the code. This report should not be considered a comprehensive assessment of the code's utility, safety, or bug-free status, and no warranties are made regarding the security of the code. A more thorough analysis, including manual review and functional testing, may be necessary to fully assess the safety and functionality of the contracts.