SHPAUCO

WORLD CUP 22 TOKEN

Smart Contract Security Audit

SHP

March, 2022

This is security audit report document and which may contain information which is confidential. Which includes any potential vulnerabilities and malicious codes which can be used to exploit the software. This must be referred internally and only should be made available to the public after issues are resolved.

Background

SHPAUCO was contracted by the Influence team to perform the Security audit of the Influence protocol smart contract code. The audit has been performed using manual analysis as well as using automated software tools. This report presents all the findings regarding the audit Performed on DATA MONTH DAY 2022.

Project Background

Influence is a standard BEP20 token smart contract. This audit only considers Influence and ACT which are BEP20 tokens, Proxy admin and transparent upgradable proxies.

SHPAUCO was commissioned by World Cup 22 to perform an audit of smart contracts.

https://bscscan.com/token/0x44e1e671991c2507364f429247893f11ea481771

The purpose of this audit was to address the following:
Ensure that all claimed functions exist and function correctly. – Identify any security vulnerabilities that may be present in the smart contract.

Issues Checking Status

	Issue description	Checking Status
1	Contract Programming	Passed
2.	Solidity version not specified	Passed
3.	Solidity version too old	Passed
4.	Integer overflow/underflow	Passed
5.	Function input parameters lack of check	Passed
6.	Function input parameters check bypass	Passed
7.	Function access control lacks management	Passed
8.	Compiler errors.	Passed
9.	Possible delays in data delivery	Passed
10.	Oracle calls.	Passed
11.	Critical operation lacks event log	Passed
12.	Random number generation/use vulnerability	Passed
13.	Fallback function misuse	Passed
14.	Race condition Passed Logical vulnerability	Passed
15.	Front running.	Passed
16.	Features claimed	Passed
17.	Other programming issues	Passed
18.	Timestamp dependence	Passed
19.	Economy model of the contract.	Passed
20.	Private user data leaks	Passed
21.	Design Logic.	Passed
22.	Safe Open Zeppelin contracts implementation	Passed
23.	and usage.	Passed
24.	Function visibility not explicitly declared	Passed
25.	Var. storage location not explicitly declared	Passed
26.	Use keywords/functions to be deprecated	Passed
27.	Integer Overflow and Underflow.	Passed
28.	Methods execution permissions.	Passed

29.	Uninitialized storage pointers.	Passed
30.	"Out of Gas" Issue	Passed
31.	High consumption 'for/while' loop	Passed
32.	High consumption 'storage' storage	Passed
33.	Scoping and Declarations.	Passed
34.	Malicious Event log.	Passed
35.	Assert () misuse	Passed
36.	Business Risk The maximum limit for mintage	Passed
37.	not set	Passed
38.	The impact of the exchange rate on the logic	Passed
39.	Arithmetic accuracy	Passed
40.	DoS with block gas limit.	Passed
41.	DoS with Revert	Passed
42.	Cross-function race conditions.	Passed
43.	Fallback function security	Passed
44.	"Short Address" Attack	Passed
45.	"Double Spend" Attack	Passed

We used various tools like MythX, Slither and Remix IDE. At the same time this finding is based on critical analysis of the manual audit. All issues found during automated analysis were manually reviewed and applicable vulnerabilities are presented in the Audit overview section. General overview is presented in the AS-IS section and all identified issues can be found in the Audit overview section.

Security Issues

No high severity issues found.

No medium severity issues found.

No low severity issues found.

According to the standard audit assessment, Customer`s solidity smart contracts are "Secured". These contracts also have owner functions (described in the centralization section below), which does not make everything 100% decentralized. Thus, the owner must execute those smart contract functions as per the business plan.

Owner privileges (In the period when the owner is not renounced)

Owner can mint any amount of tokens (ownership renounced).

Security Issues

There is no high risky issues!

BscScan: https://bscscan.com/token/0x44e1e671991c2507364f429247893f11ea481771

Contract Address : 0x44e1E671991C2507364F429247893F11eA481771

PooCoin : https://poocoin.app/tokens/0x44e1e671991c2507364f429247893f11ea481771