soken

SMART CONTRACT SECURITY AUDIT

Package Portal (PORT)

Scan and check this report
was posted at Soken Github

April, 2022

Website: soken.io

Table of Contents

Disclaimer

This is a comprehensive report based on our automated and manual examination of cybersecurity vulnerabilities and framework flaws. We took into consideration smart contract based algorithms, as well. Reading the full analysis report is essential to build your understanding of project's security level. It is crucial to take note, though we have done our best to perform this analysis and report, that you should not rely on the our research and cannot claim what it states or how we created it. Before making any judgments, you have to conduct your own independent research. We will discuss this in more depth in the following disclaimer - please read it fully.

DISCLAIMER: You agree to the terms of this disclaimer by reading this report or any portion thereof. Please stop reading this report and remove and delete any copies of this report that you download and/or print if you do not agree to these conditions. This report is for non-reliability information only and does not represent investment advice. No one shall be entitled to depend on the report or its contents, and Soken and its affiliates shall not be held responsible to you or anyone else, nor shall Soken provide any guarantee or representation to any person with regard to the accuracy or integrity of the report. Without any terms, warranties or other conditions other than as set forth in that exclusion and Soken excludes hereby all representations, warrants, conditions and other terms (including, without limitation, guarantees implied by the law of satisfactory quality, fitness for purposes and the use of reasonable care and skills). The report is provided as "as is" and does not contain any terms and conditions. Except as legally banned, Soken disclaims all responsibility and responsibilities and no claim against Soken is made to any amount or type of loss or damages (without limitation, direct, indirect, special, punitive, consequential or pure economic loses or losses) that may be caused by you or any other person, or any damages or damages, including without limitations (whether innocent or negligent).

Security analysis is based only on the smart contracts. No applications or operations were reviewed for security. No product code has been reviewed.

Procedure

Our analysis contains following steps:

1. Project Analysis;

2. Manual analysis of smart contracts:
- Deploying smart contracts on any of the network(Ropsten/Rinkeby) using Remix IDE
- Hashes of all transaction will be recorded
- Behaviour of functions and gas consumption is noted, as well.

3. Unit Testing:
- Smart contract functions will be unit tested on multiple parameters and under multiple conditions to ensure that all paths of functions are functioning as intended.
- In this phase intended behaviour of smart contract is verified.
- In this phase, we would also ensure that smart contract functions are not consuming unnecessary gas.
- Gas limits of functions will be verified in this stage.

4. Automated Testing:
- Mythril
- Oyente
- Manticore
- Solgraph

Terminology

We categorize the finding into 4 categories based on their vulnerability:

- Low-severity issue — less important, must be analyzed
- Medium-severity issue — important, needs to be analyzed and fixed
- High-severity issue —important, might cause vulnerabilities, must be analyzed and fixed
- Critical-severity issue —serious bug causes, must be analyzed and fixed.

Limitations

The security audit of Smart Contract cannot cover all vulnerabilities. Even if no vulnerabilities are detected in the audit, there is no guarantee that future smart contracts are safe. Smart contracts are in most cases safeguarded against specific sorts of attacks. In order to find as many flaws as possible, we carried out a comprehensive smart contract audit. Audit is a document that is not legally binding and guarantees nothing.

Token Contract Details for 19.04.2022

Deployed address: **zil1xlqwglrgr336rss9te4gwg2gy6frr4r2ymzwx8**

Total Supply: **10 000 000**

Token Tracker: **PORT**

Decimals: **4**

Token holders: **21 787**

Transactions count: **560 182**

Top 100 holders dominance: **97.68%**

Audit Details

Project Name: **Package Portal**

Language: **Scilla**

Blockchain: **Zilliqa**

Social Profiles

Project Website: **https://www.packageportal.com/**

Project Twitter: **https://twitter.com/packageportal**

Project Telegram: **https://t.me/polygamers**

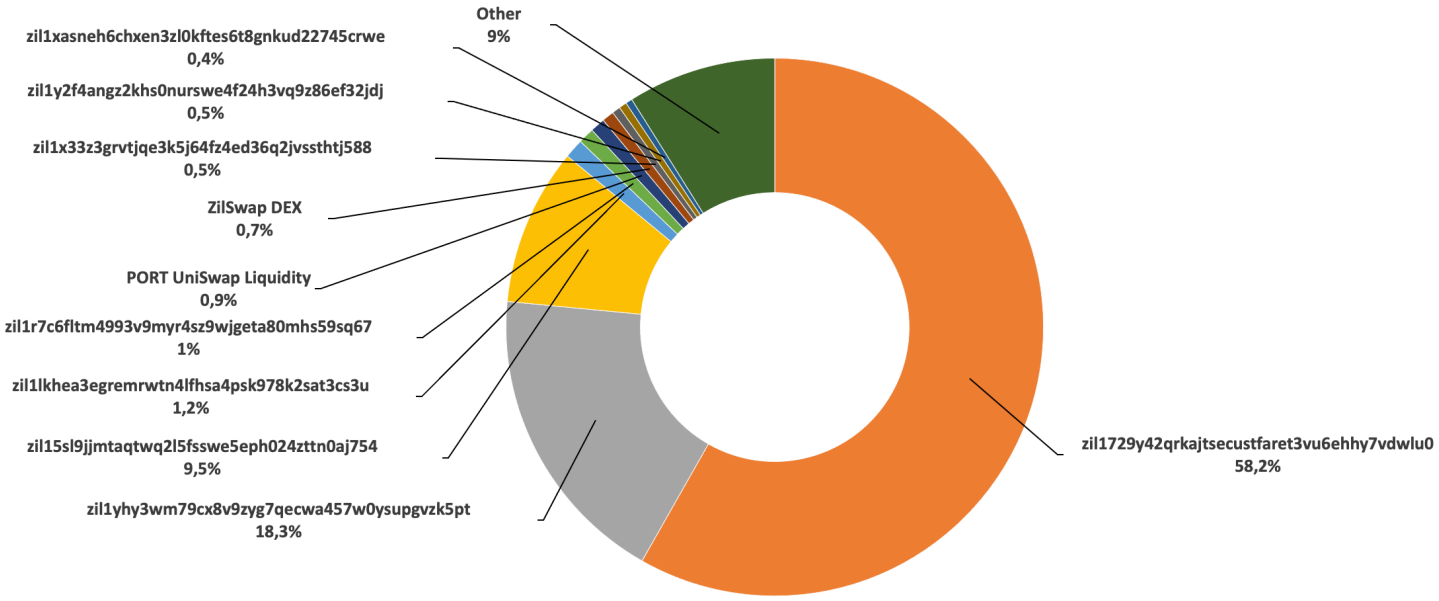
Project Facebook: **https://www.facebook.com/packageportal**

Project Medium: **https://medium.com/packageportal**

Project Instagram: **https://www.instagram.com/packageportal/**

Project YouTube: **https://www.youtube.com/channel/UCNSJKu3v0RV8nH2nLotqJfQ**

PORT Token Distribution



PORT Top Holders

RANK	ADDRESS	BALANCE	SHARE
1	zil1729y42qrkajtsecustfaret3vu6ehhy7vdwlu0	5 821 512,025	58.22%
2	zil1yhy3wm79cx8v9zyg7qecwa457w0ysupgvzk5pt	1 829 589,929	18.30%
3	zil15sl9jjmtaqtwq2l5fsswe5eph024zttn0aj754	945 253	9.45%
4	zil1lkhea3egremrwtn4lfhsa4psk978k2sat3cs3u	116 352,041	1.16%
5	zil1r7c6fltm4993v9myr4sz9wjgeta80mhs59sq67	95 801,065	0.96%
6	PORT UniSwap Liquidity	88 994,984	0.89%
7	ZilSwap DEX	72 494,129	0.72%
8	zil1x33z3grvtjqe3k5j64fz4ed36q2jvssthtj588	50 000	0.50%
9	zil1y2f4angz2khs0nurswe4f24h3vq9z86ef32jdj	46 891,424	0.47%
10	zil1xasneh6chxen3zl0kftes6t8gnkud22745crwe	40 164,312	0.40%

Whitepaper Review

The Whitepaper of PackagePortal team has been reviewed on behalf of Soken Team.

PackagePortal

Blockchain for E-commerce Delivery Data & Loyalty Rewards

An exhaustive introduction to the PackagePortal platform.

Abstract

The PackagePortal is a platform that incentivizes online shoppers to scan shipping labels with their mobile device. This enables real-time delivery confirmations & feedback about the delivery experience directly from consumer to shipper, circumventing carriers & their surcharges. The ecosystem leverages smart contracts for the tokenization of scan data, and the transferability of its value, rewarding users for scans in the form of tokens ascribed redemptive value within our platform. Online merchants and retailers are able to use PackagePortal to reconnect with their shoppers at the moment of delivery, and easily operate blockchain based loyalty campaigns, as they collect valuable consumer and delivery data, accompanied by driver ratings.

Whitepaper link: **https://docs.google.com/document/d/1-3qjW4bozTt72CzfGcwDGzcm8---opu0fN1pxs34RyE/edit**

Vulnerabilities checking

Issue Description	Checking Status
Compiler Errors	Completed
Delays in Data Delivery	Completed
Re-entrancy	Completed
Transaction-Ordering Dependence	Completed
Timestamp Dependence	Completed
Shadowing State Variables	Completed
DoS with Failed Call	Completed
DoS with Block Gas Limit	Completed
Outdated Complier Version	Completed
Assert Violation	Completed
Use of Deprecated Solidity Functions	Completed
Integer Overflow and Underflow	Completed
Function Default Visibility	Completed
Malicious Event Log	Completed
Math Accuracy	Completed
Design Logic	Completed
Fallback Function Security	Completed
Cross-function Race Conditions	Completed
Safe Zeppelin Module	Completed

Conclusion

Package Portal (PORT) token is free from any low, medium or high-severity issues.

NOTE: Please check the disclaimer above and note, that audit makes no statements or warranties on business model, investment attractiveness or code sustainability.

Soken Contact Info

Website: www.soken.io

Mob: (+1)416-875-4174

32 Britain Street, Toronto, Ontario, Canada

Telegram: @team_soken

GitHub: sokenteam

Twitter: @soken_team