SOLIDProof

Bring trust into your projects

Blockchain Security | Smart Contract Audits | KYC Development | Marketing

MADE IN GERMANY

AUDIT

SECURITY ASSESSMENT

15. March, 2024

FOR

Webchain Offline Wallet

QCAT
Smart CAT, Inc.

Contents

Disclaimer 2
Project Overview 4
Summary 4
Social Medias 4
Audit Summary 5
File Overview 5
Imported packages 5
Audit Information 7
Vulnerability & Risk Level 7
Auditing Strategy and Techniques Applied 8
Methodology 8
Overall Security 9
Medium or higher issues 9
Components 10
Audit Results 11
#1 | Code Review 11

Introduction

SolidProof.io is a brand of the officially registered company MAKE Network GmbH, based in Germany. We're mainly focused on Blockchain Security such as Smart Contract Audits and KYC verification for project teams.
Solidproof.io assess potential security issues in the smart contracts implementations, review for potential inconsistencies between the codebase and the whitepaper/documentation, and provide suggestions for improvement.

Disclaimer

SolidProof.io reports are not, nor should be considered, an

"endorsement"or "disapproval" of any particular project or team. These reports are not, nor should be considered, an indication of the economics or value of any"product" or "asset" created by any team. SolidProof.io do not cover testing or auditing the integration with external contract or services (such as Unicrypt, Uniswap, PancakeSwap etc'...)

SolidProof.io Audits do not provide any warranty or guarantee regarding the absolute bug- free nature of the technology analyzed, nor do they provide any indication of the technology proprietors. SolidProof Audits should not be used in any way to make decisions around investment or involvement with any particular project. These reports in no way provide investment advice, nor should be leveragedas investment advice of any sort.

SolidProof.io Reports represent an extensive auditing process intending tohelp our customers increase the quality of their code while reducing the high level of risk presented by cryptographic tokens and blockchain technology. Blockchain technology and cryptographic assets present a high level of ongoing risk. SolidProof's position is that each company and individual are responsible for their own due diligence and continuous security. SolidProof in no way claims any guarantee of security or functionality of the technology we agree to analyze.

Project Overview

Summary

Project Name	Webchain Offline Wallet
Website	1. https://www.unhackablecloud.com 2. https://www.smartcat.tech
About the project	TBA
Whitepaper	https://sg.docworkspace.com/d/sIOeGjo0wxezYrwY
Chain	Other EVM-based
Language	C/C++
Codebase	Provided as Files
Commit	N/A
Unit Tests	Not Provided

Social Medias

Telegram	N/A
Twitter	N/A
Facebook	N/A
Instagram	N/A
GitHub	N/A
Reddit	N/A
Medium	N/A
Discord	N/A
YouTube	N/A
TikTok	N/A
LinkedIn	N/A

Audit Summary

Version	Delivery Date	Change Log
v1.0	16. March 2024	· Manual Functionality Review · Summary

Note - The following audit report presents a comprehensive security analysis of the smart contract utilized in the project. This analysis did not include functional testing (or unit testing) of the contract's logic. We cannot guarantee 100% logical correctness of the contract as it was not functionally tested by us.

File Overview

The Team provided us with the files that should be tested in the securityassessment. This audit covered the following files listed below with a SHA-1 Hash.

1. build_offline_tools.sh
2. build_ubunut22_libethc.sh
3. build_ubuntu22_libsecp156k1.sh
4. new_ubuntu22_dependency_check.sh
5. generator_util.h
6. offlinetransaction5e.c
7. walletgenerator3e.c

Please note: Files with a different hash value than in this table have been modified after the security check, either intentionally or unintentionally. A different hash valuemay (but need not) be an indication of a changed state or potential vulnerability thatwas not the subject of this scan.

Imported packages

Used code from other Frameworks.

1. libethc

2. libsecp156k1
3. libqrencode
4. libjson-c-dev
5. libcrypto++-dev
6. libssl
7. libssl-dev
8. openssl
9. libgmp-dev

Audit Information

Vulnerability & Risk Level

Risk represents the probability that a certain source-threat will exploit vulnerability, and the impact of that event on the organization or system. Risk Level is computed based on CVSS version 3.0.

Level	Value	Vulnerability	Risk (Required Action)
Critical	9 - 10	A vulnerability that can disrupt the contract functioning in a number of scenarios, or creates a risk that the contract may be broken.	Immediate action to reduce risk level.
High	7 – 8.9	A vulnerability that affects the desired outcome when using a contract, or provides the opportunity to use a contract in an unintended way.	Implementation of corrective actions as soon aspossible.
Medium	4 – 6.9	A vulnerability that could affect the desired outcome of executingthe contract in a specific scenario.	Implementation of corrective actions in a certain period.
Low	2 – 3.9	A vulnerability that does not have a significant impact on possible scenarios for the use of the contract and is probably subjective.	Implementation of certain corrective actions or accepting the risk.
Informational	0 – 1.9	A vulnerability that have informational character but is not effecting any of the code.	An observation that does not determine a level of risk

Auditing Strategy and Techniques Applied

Throughout the review process, care was taken to check the repository for security- related issues, code quality, and compliance with specifications and best practices. To this end, our team of experienced pen-testers and smart contract developers reviewed the code line by line and documented any issues discovered.

We check every file manually. We use automated tools only so that theyhelp us achieve faster and better results.

Methodology

The auditing process follows a routine series of steps:

1. Code review that includes the following:
    a. Reviewing the specifications, sources, and instructions providedto SolidProof to ensure we understand the size, scope, and functionality of the program.
    b. Manual review of the code, i.e., reading the source code line by line to identify potential vulnerabilities.
    c. Comparison to the specification, i.e., verifying that the code does what is described in the specifications, sources, and instructions provided to SolidProof.

Overall Security

Medium or higher issues

No critical Issues found	✅ Program is safe to use
Description	The program does not contain issues of high or medium criticality. This means that no known vulnerabilities were found in the sourcecode.
Comment	N/A

Components

Programs	Libraries	Interfaces	Abstract
2	7	0	0

Audit Results

#1 | Code Review

File	Severity	Location	Status
Main	Informational		none

Description

1. Walletgenerator3e

a. The reviewed code generates a valid Ethereum key pair and address. The keys are generated from not guessable randomness and can not be regenerate by accident.

File	Severity	Location	Status
Main	Informational		none

2. Offlinetransaction5e

a. **The reviewed code generates a signed “offlinesend” transaction. Because of lacking informations, there was no possibility to do a real send, but the transaction is signed valid and could be sent to a network.**

File	Severity	Location	Status
Main	Informational		none

3. Build_offline_tools.sh

a. **The given shell script compiles both C-Code files. The script works as expected and creates working executables.**

File	Severity	Location	Status
Main	Informational		none

4. Build_ubuntu22_libethc.sh

a. **The given shell script downloads and compiles the libethc library. The script works as expected.**

File	Severity	Location	Status
Main	Informational		none

5. Build_ubuntu22_libsecp256k1

a. **The given shell script downloads and compiles the libsecp256k1 library. The script works as expected.**

b.

File	Severity	Location	Status
Main	Not working	L174	open

6. New_ubuntu22_dependency_check.sh

a. The given shell script checks for all dependencies needed to compile the given codebase. The script also downloads and installs all missing dependencies, if needed. The script ends with an error.

Note:

b. None of the given code files contains any new or breaking technology.

Legend For the Issue Status

Attribute or Symbol	Meaning
Open	The issue is not fixed by the project team.
Fixed	The issue is fixed by the project team.
Acknowledged(ACK)	The issue has been acknowledged or declared as part of business logic.

Blockchain Security | Smart Contract Audits | KYC Development | Marketing

MADE IN GERMANY