Meter Security Audit Report

1. Executive Summary

On April 24, 2020, the SlowMist security team received the Meter team's security audit application for Meter, developed the audit plan according to the agreement of both parties and the characteristics of the project, and finally issued the security audit report.

The SlowMist security team adopts the strategy of “black, grey box lead, white box assists" to conduct a complete security test on the project in the way closest to the real attack.

SlowMist blockchain system test method:

Black box testing	Conduct security tests from an attacker's perspective externally.
Grey box testing	Conduct security testing on code module through the scripting tool, observing the internal running status, mining weaknesses.
White box testing	Based on the open source code, non-open source code, to detect wether there are vulnerabilities in programs suck as nodes, SDK, etc.

SlowMist blockchain risk level:

Critical vulnerabilities	Critical vulnerabilities will have a significant impact on the security of the blockchain, and it is strongly recommended to fix the critical vulnerabilities.
High-risk vulnerabilities	High-risk vulnerabilities will affect the normal operation of blockchain. It is strongly recommended to fix high-risk vulnerabilities.
Medium-risk vulnerablities	Medium vulnerability will affect the operation of blockchain. It is recommended to fix medium-risk vulnerabilities.

Low-risk vulnerabilities	Low-risk vulnerabilities may affect the operation of blockchain in certain scenarios. It is suggested that the project party should evaluate and consider whether these vulnerabilities need to be fixed.
Weaknesses	There are safety risks theoretically, but it is extremely difficult to reproduce in engineering.
Enhancement Suggestions	There are better practices for coding or architecture.

2. Project Background (Context)

2.1 Project Introduction

Meter is a decentralized finance (DeFi) infrastructure with a unique economic and consensus design. It uses proof of work mining algorithms to create a low-volatility global currency and a latest proof of stake consensus to protect the payment system.

Project website: https://www.meter.io/

Project source code:

https://github.com/dfinlab/meter-pov-consensus

https://github.com/dfinlab/btcpow

Audit version:

Meter - pov - consensus:

Branch: premainnet,

commit: 21c529eb1d0aa0e7fead8cd99ce398e0891de79a

Btcpow:

Branch: 0.17, commit: a3f66630d06e6ed3dc74596565525de3c48faf39

Review version:

Meter - pov - consensus:

Branch: premainnet,

commit: 4ba9554caafbcc5ca213c5d645493ef03d422754

2.2 Scope of Audit

The main types of security audit include:

No.	Audit category	Subclass	Audit result
1	Code static check	Built-in function security	Pass
		Standard library security audit	Pass
		Third party library security audit	Pass
		Injection audit	Pass
		Serialization algorithm audit	Pass
		Memory leak audit	Pass
		Arithmetic operation audit	Pass
		Resource consumption audit	Pass
		Exception handling audit	Pass
2	P2P security	Node connection number audit	Pass
		Node performance audit	Pass
		Communication encryption audit	Pass
		"Alien Attack" audit	Pass
3	RPC security	Remote call permission audit	Pass
		Malformed data request audit	Pass
		Communication encryption	Pass

		audit	
		Same-origin policy audit	Pass
4	Encrypted signature security	Random number generation algorithm audit	Pass
		Private key storage audit	Pass
		Cryptographic component call audit	Pass
		Hash intensity audit	Pass
		Transaction malleability attack audit	Pass
		Encryption and decryption fuzz testing	Pass
5	Account and transaction model security	Authority verification audit	Pass
		Transaction replay audit	Pass
		“False Top-up “ audit	Pass
6	Btcpow related module security	-	Pass
7	Token lockup security	-	Pass

(other unknown security vulnerabilities are not included in the scope of responsibility of this audit)

2.3 Conclusion

Audit result: Pass

Audit No. : BCA002005090001

Audit date: May 09, 2020

Audit team: SlowMist security team

Summary conclusion: After correction, all problems found have been fixed and the above risks have been eliminated by Meter. Comprehensive assessed, Meter has no risks above already.

3. Statement

SlowMist issues this report with reference to the facts that have occurred or existed before the issuance of this report, and only assumes corresponding responsibility base on these.

For the facts that occurred or existed after the issuance, SlowMist is not able to judge the security status of this project, and is not responsible for them. The security audit analysis and other contents of this report are based on the documents and materials provided to SlowMist by the information provider till the date of the insurance this report (referred to as "provided information"). SlowMist assumes: The information provided is not missing, tampered with, deleted or concealed. If the information provided is missing, tampered with, deleted, concealed, or inconsistent with the actual situation, the SlowMist shall not be liable for any loss or adverse effect resulting therefrom. SlowMist only conducts the agreed security audit on the security situation of the project and issues this report. SlowMist is not responsible for the background and other conditions of the project.

SLOWMIST

Official Website

www.slowmist.com

✉

E-mail

team@slowmist.com

Twitter

@SlowMist_Team

Github

https://github.com/slowmist