QuillAudits

Audit Report
August, 2023

For

MXC

Table of Content

Executive Summary

Project Name	MXC Protocol
Timeline	17th July 2023 to August 1, 2023
Scope of Audit	The scope of this audit was to analyze and document the diff Go file codebase for quality, security, and correctness. QuillAudits reviewed the code with a focus on Denial-of-Service by abusing memory allocation and I/O usage.
Codebase	The code for the security review was taken from diff provided. *https://github.com/MXCzkEVM/mxc-geth/blob/audit/audit.diff*

1
Issue Found
🟥 High
🟨 Medium
🟩 Low
🟪 Informational

	High	Medium	Low	Informational
Open Issues	0	0	1	0
Acknowledged Issues	0	0	0	0
Partially Resolved Issues	0	0	0	0
Resolved Issues	0	0	0	0

Techniques and Methods

Throughout the audit of the code, care was taken to ensure

- The overall quality of code.
- Use of best practices.
- Code documentation and comments match logic and expected behavior.
- Efficient use of inbuilt functionality.
- Code is safe from known attack vectors.

Structural Analysis
In this step, we have analyzed the design patterns and structure of the code base. A thorough check was done to ensure that the code is structured in a way that will avoid future problems

Static Analysis
A static Analysis of the code base was done to identify vulnerabilities

Code Review / Manual Analysis
Manual Analysis or review of code was done to identify new vulnerabilities or verify the vulnerabilities found during the static analysis. Diff codes were completely manually analyzed, and their logic was checked and compared with the one used in the original Ethereum geth client.

Types of Issues

Open

Security vulnerabilities identified that must be resolved and are currently unresolved.

Resolved

These are the issues identified in the initial audit and have been successfully fixed.

Acknowledged

Vulnerabilities which have been acknowledged but are yet to be resolved.

Partially Resolved

Considerable efforts have been invested to reduce the risk/impact of the security issue, but are not completely resolved.

Types of Severities

High

A high severity issue or vulnerability means that your smart contract can be exploited. Issues on this level are critical to the smart contract's performance or functionality, and we recommend these issues be fixed before moving to a live environment.

Medium

The issues marked as medium severity usually arise because of errors and deficiencies in the smart contract code. Issues on this level could potentially bring problems, and they should still be fixed.

Low

Low-level severity issues can cause minor impact and or are just warnings that can remain unfixed for now. It would be better to fix these issues at some point in the future.

Informational

These are severity issues that indicate an improvement request, a general question, a cosmetic or documentation error, or a request for information. There is low-to-no impact.

Checked Vulnerabilities

- ✓ Peer-to-peer communication and networking, block downloading
- ✓ RPC interface, Javascript scripting engine
- ✓ Transaction and block processing, consensus rules implementation
- ✓ Virtual Machine (resource exhaustion/Denial-of-Service)
- ✓ Data shared between threads are properly protected
- ✓ Followed data flow from external inputs to see if invalid input leads to erroneous behaviour.
- ✓ Automatically searched for race conditions using Go’s built-in ”–race” build flag.
- ✓ Secure channel establishment - handshake and establishment of shared secrets.
- ✓ Secure channel properties - confidentiality and integrity.
- ✓ Message serialization
- ✓ Node discovery
- ✓ Protection against Denial-of-Service: timeouts and message size limits

Issues Found – Code Review/Manual Testing

High Severity Issues

No Issues Found

Medium Severity Issues

No Issues Found

Low Severity Issues

1. Remove Todo comments

Description

We recommend removing the todo comments from the code base. *REF1* and *REF2*.

Status

Resolved

Closing Summary

During the security review of the Go implementation of MEX. QuillAudits team found the code to be of high quality and developed with a security-focused mindset. No security vulnerabilities have been found.

Disclaimer

QuillAudits security audit provides services to help identify and mitigate potential security risks in Go implementation of MXC. However, it is important to understand that no security audit can guarantee complete protection against all possible security threats. QuillAudits audit reports are based on the information provided to us at the time of the audit, and we cannot guarantee the accuracy or completeness of this information. Additionally, the security landscape is constantly evolving, and new security threats may emerge after the audit has been completed.

Therefore, it is recommended that multiple audits and bug bounty programs be conducted to ensure the ongoing security of MXC Go implementation. One audit is not enough to guarantee complete protection against all possible security threats. It is important to implement proper risk management strategies and stay vigilant in monitoring your smart contracts for potential security risks.

QuillAudits cannot be held liable for any security breaches or losses that may occur subsequent to and despite using our audit services. It is the responsibility of the MXC to implement the recommendations provided in our audit reports and to take appropriate steps to mitigate potential security risks.

About QuillAudits

QuillAudits is a secure smart contracts audit platform designed by QuillHash Technologies. We are a team of dedicated blockchain security experts and smart contract auditors determined to ensure that Smart Contract-based Web3 projects can avail the latest and best security solutions to operate in a trustworthy and risk-free ecosystem.

850+
Audits Completed

$30B
Secured

800K
Lines of Code Audited

Follow Our Journey

Audit Report
August, 2023

For

MXC

QuillAudits

Canada, India, Singapore, UAE, UK

www.quillaudits.com

audits@quillhash.com