Cyberscope
A TAC Security Company

Audit Report
MCN Chain

December 2025

Repository	https://github.com/mcnchain/MCNBlockchain
Commit	770fcf367ffc32b1095fd2d84cac625bbf236f85
Audited by	© cyberscope

Table of Contents

Risk Classification

The criticality of findings in Cyberscope's smart contract audits is determined by evaluating multiple variables. The two primary variables are:

1. **Likelihood of Exploitation**: This considers how easily an attack can be executed, including the economic feasibility for an attacker.
2. **Impact of Exploitation**: This assesses the potential consequences of an attack, particularly in terms of the loss of funds or disruption to the contract's functionality.

Based on these variables, findings are categorized into the following severity levels:

1. **Critical**: Indicates a vulnerability that is both highly likely to be exploited and can result in significant fund loss or severe disruption. Immediate action is required to address these issues.
2. **Medium**: Refers to vulnerabilities that are either less likely to be exploited or would have a moderate impact if exploited. These issues should be addressed in due course to ensure overall contract security.
3. **Minor**: Involves vulnerabilities that are unlikely to be exploited and would have a minor impact. These findings should still be considered for resolution to maintain best practices in security.
4. **Informative**: Points out potential improvements or informational notes that do not pose an immediate risk. Addressing these can enhance the overall quality and robustness of the contract.

Severity	Likelihood / Impact of Exploitation
● Critical	Highly Likely / High Impact
● Medium	Less Likely / High Impact or Highly Likely/ Lower Impact
● Minor / Informative	Unlikely / Low to no Impact

Review

Repository	https://github.com/mcnchain/MCNBlockchain
Commit	770fcf367ffc32b1095fd2d84cac625bbf236f85

Audit Updates

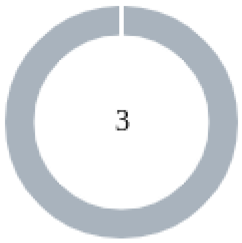
Initial Audit	29 Oct 2025
Corrected Phase 2	25 Nov 2025
Corrected Phase 3	19 Dec 2025

Diagnostics

🔴 Critical 🟠 Medium ⚪ Minor / Informative

Severity	Code	Description	Status
⚪	PECD	Potentially Exposed Coinbase Data	Unresolved
⚪	USA	Unconstrained System Access	Unresolved
⚪	UPPA	Unrestricted P2P Port Access	Unresolved

Findings Breakdown



●	Critical	0
●	Medium	0
●	Minor / Informative	3

Severity	Unresolved	Acknowledged	Resolved	Other
● Critical	0	0	0	0
● Medium	0	0	0	0
● Minor / Informative	3	0	0	0

PECD - Potentially Exposed Coinbase Data

Criticality	Minor / Informative
Location	geth-main.service geth-additional-nodes.service
Status	Unresolved

Description

The script uses a password file to unlock Ethereum accounts and their associated keystore. If an unauthorized party gains access to this file, they could potentially compromise the validator account and gain control over its operations.

Shell

```shell
--password /home/validator/node/password.txt \
```

Recommendation

It is recommended to restrict access to these sensitive files and directories using appropriate permissions. This ensures that only the owner can read the password file and access the validator data directory, improving security and preventing unauthorized access.

USA - Unconstrained System Access

Criticality	Minor / Informative
Location	geth-main.service geth-public.service geth-additional-nodes.service
Status	Unresolved

Description

The Geth node is configured to run under a non-privileged user using systemd. However, the associated systemd unit file lacks hardening directives, leaving the Geth process with broad read access to the host filesystem and unrestricted read/write access within the user's home directory.

This unrestricted access significantly increases the system's attack surface. In the event of a compromised execution an attacker could:

- Access sensitive files on the host system.
- Modify user-owned scripts or binaries to establish persistence.
- Deploy malware in shared directories.

Recommendation

It is recommended to apply standard systemd hardening flags to the Geth service unit such as:

Shell
```
- ProtectSystem=strict
- ProtectHome=true
- PrivateTmp=true
- NoNewPrivileges=yes
```

These directives limit the Geth process to a read-only view of system directories, restrict access to other users' home directories, isolate temporary files, and block privilege escalation. This reduces the attack surface and mitigates the risk of persistence or lateral movement in the event of a compromise.

UPPA - Unrestricted P2P Port Access

Criticality	Minor / Informative
Location	geth-main.service geth-public.service geth-additional-nodes.service
Status	Unresolved

Description

The Geth node is configured with default peer-to-peer (P2P) settings, leaving TCP and UDP ports open for public peer discovery. The P2P service listens on all network interfaces, allowing any external Ethereum client with knowledge of the node's enode URL to initiate a handshake, maintain connections, and send traffic.

If the HTTP and WebSocket APIs are exposed to the network (as in the current configuration), they could allow unauthorized access to blockchain data. The node is thus exposed to unsolicited connections from the public internet. Malicious actors could exploit this by sending malformed blocks, oversized transaction pools, or other resource-intensive requests, potentially degrading performance or causing denial-of-service conditions.

Recommendation

For private chains, disable public peer discovery and restrict P2P connections by using one of the following startup options:

- `--nodiscover` along with `--bootnodes <trusted-enodes>` to connect only to known peers (preferred).
- `--maxpeers 0` if the node is intended to operate as a solo validator.
- `--netrestrict <CIDR>` to limit peer connections to a specific LAN or VPN range. Additionally, firewall or externally close port 30303 to block unwanted access.

Summary

MCN implements an EVM-compatible network based on Geth. Systemd scripts automate genesis initialization, network configuration, and validator setup. This audit investigates security issues, business logic, and potential improvements.

Disclaimer

The information provided in this report does not constitute investment, financial or trading advice and you should not treat any of the document's content as such. This report may not be transmitted, disclosed, referred to or relied upon by any person for any purposes nor may copies be delivered to any other person other than the Company without Cyberscope's prior written consent. This report is not nor should be considered an "endorsement" or "disapproval" of any particular project or team. This report is not nor should be regarded as an indication of the economics or value of any "product" or "asset" created by any team or project that contracts Cyberscope to perform a security assessment. This document does not provide any warranty or guarantee regarding the absolute bug-free nature of the technology analyzed, nor do they provide any indication of the technologies proprietors' business, business model or legal compliance. This report should not be used in any way to make decisions around investment or involvement with any particular project. This report represents an extensive assessment process intending to help 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 Cyberscope's position is that each company and individual are responsible for their own due diligence and continuous security Cyberscope's goal is to help reduce the attack vectors and the high level of variance associated with utilizing new and consistently changing technologies and in no way claims any guarantee of security or functionality of the technology we agree to analyze. The assessment services provided by Cyberscope are subject to dependencies and are under continuing development. You agree that your access and/or use including but not limited to any services reports and materials will be at your sole risk on an as-is where-is and as-available basis Cryptographic tokens are emergent technologies and carry with them high levels of technical risk and uncertainty. The assessment reports could include false positives false negatives and other unpredictable results. The services may access and depend upon multiple layers of third parties.

About Cyberscope

Cyberscope is a TAC blockchain cybersecurity company that was founded with the vision to make web3.0 a safer place for investors and developers. Since its launch, it has worked with thousands of projects and is estimated to have secured tens of millions of investors' funds.

Cyberscope is one of the leading smart contract audit firms in the crypto space and has built a high-profile network of clients and partners.

A ***TAC Security*** *Company*

The Cyberscope team

cyberscope.io