OWASP MCP Top 10

Compliance assessment — 2025

Server: 00-renjing-mcp-server-pypi

Slug: 00-renjing-mcp-server-pypi-20260921084418-17033a
Scan id: 00000000-0000-0000-0000-000000000000

Assessed at: 2026-09-21 08:44:20 UTC
Sentinel version: 0.4.0
Rules version: 2026-04-23

? Insufficient evidence

DRAFT for review — not legal advice. See attestation block for verification instructions.

DRAFT

Table of contents

1. Executive summary
2. Coverage & transparency
3. Controls summary
4. Control details
5. Multi-step attack chains
6. Cryptographic attestation

1. Executive summary

Assessment of 00-renjing-mcp-server-pypi against OWASP MCP Top 10: overall status insufficient evidence. Of 10 controls, 2 met, 0 unmet, 0 partial, 8 not assessed, 0 not applicable. 2 control(s) had complete mapped-assessor execution evidence; 8 lacked sufficient execution evidence and 0 were outside the current assessor mapping. No definitive compliance conclusion is possible because one or more mapped assessor sets did not execute completely. All claims are traceable to individual finding rows via finding_id and to the governing rule via rule_id; the enclosing signed envelope commits MCP Sentinel to the exact bytes of this report.

2. Coverage & transparency

Coverage band: low

Coverage ratio: 58%

Rules version: 2026-04-23

Analysis techniques applied:

- ast-taint
- composite
- cross-module
- dependency-audit
- similarity
- structural
- stub

3. Controls summary

ControlName	Status	Evidence
MCP01Prompt Injection?	Not assessed	0
MCP02Tool		

Poisoning?
Not assessed0
MCP03
Command
Injection' Met0
MCP04Data
Exfiltration?
Not assessed0
MCP05
Privilege
Escalation?
Not assessed0
MCP06
Excessive
Permissions?
Not assessed0
MCP07
Insecure
Configuration
? Not
assessed0
MCP08
Dependency
Vulnerabilities'
Met0
MCP09
Logging &
Monitoring
Failures? Not
assessed0
MCP10Supply
Chain
Compromise?
Not assessed0

4. Control details

MCP01 — Prompt Injection

? Not assessed

4/24 mapped assessor rule(s) are proven to have executed; no adverse findings were observed, but the control is not assessed because execution evidence is incomplete. Unexecuted assessors: A1 (tools); A5 (tools); A7 (tools); A8 (tools); A9 (tools); B5 (tools); F1 (tools); F6 (tools); G1 (tools); G2 (tools); G3 (tools); G4 (tools); G5 (tools); H2 (initialize_metadata); H3 (tools); I3 (resource_templates, resources); I6 (prompts); I7 (tools); J3 (tools); J6 (tools).

MCP02 — Tool Poisoning

? Not assessed

5/15 mapped assessor rule(s) are proven to have executed; no adverse findings were observed, but the control is not assessed because execution evidence is incomplete. Unexecuted assessors: A2 (tools); A4 (tools); A6 (tools); F2 (tools); G6 (scan_history); I1 (tool_attributes(annotations), tools); I2 (tool_attributes(annotations), tools); I5 (resource_templates, resources, tools); I16 (min_tools(10), tools); J6 (tools).

MCP03 — Command Injection

' Met

6/6 mapped assessor rule(s) are proven to have executed; no adverse findings were observed on the mapped detector surface.

MCP04 — Data Exfiltration

? Not assessed

9/15 mapped assessor rule(s) are proven to have executed; no adverse findings were observed, but the control is not assessed because execution evidence is incomplete. Unexecuted assessors: A3 (tools); F1 (tools); F3 (tools); F7 (min_tools(2), tools); I9 (tools); I13 (multi_server_tools, tools).

MCP05 — Privilege Escalation

? Not assessed

5/7 mapped assessor rule(s) are proven to have executed; no adverse findings were observed, but the control is not assessed because execution evidence is incomplete. Unexecuted assessors: I4 (resource_templates, resources); I12 (declared_capabilities).

MCP06 — Excessive Permissions

? Not assessed

0/7 mapped assessor rule(s) are proven to have executed; no adverse findings were observed, but the control is not assessed because execution evidence is incomplete. Unexecuted assessors: A2 (tools); B3 (tools); B7 (tools); E4 (min_tools(51), tools); F2 (tools); I11 (roots); I16 (min_tools(10), tools).

MCP07 — Insecure Configuration

? Not assessed

8/11 mapped assessor rule(s) are proven to have executed; no adverse findings were observed, but the control is not assessed because execution evidence is incomplete. Unexecuted assessors: B6 (tools); E1 (connection_metadata); E2 (connection_metadata).

MCP08 — Dependency Vulnerabilities

' Met

7/7 mapped assessor rule(s) are proven to have executed; no adverse findings were observed on the mapped detector surface.

MCP09 — Logging & Monitoring Failures

? Not assessed

5/6 mapped assessor rule(s) are proven to have executed; no adverse findings were observed, but the control is not assessed because execution evidence is incomplete. Unexecuted assessors: E3 (connection_metadata).

MCP10 — Supply Chain Compromise

? Not assessed

23/27 mapped assessor rule(s) are proven to have executed; no adverse findings were observed, but the control is not assessed because execution evidence is incomplete. Unexecuted assessors: A4 (tools); I5 (resource_templates, resources, tools); L1 (source_files(ci-config)); L3 (source_files(container-config)).

5. Multi-step attack chains

No multi-step attack chains were synthesized for this server.

6. Cryptographic attestation

Algorithm: `HMAC-SHA256`
Key ID: `mcps-hkdf-e8990a4e1526`
Signer: `mcp-sentinel/v1`
Signed at: `2026-09-21T08:44:20.188Z`

Canonicalization:

RFC8785

HMAC-SHA256 signature (base64, wrapped at 64 chars):

```
9SnH4ya+KH77LRGn6N+PqVlEX2gNtrEKUOZeCkdch14=
```

Verification instructions:

```
To verify this report:
  1. Extract the report body (everything except the .attestation field).
  2. Canonicalize the body via RFC 8785 (JCS).
  3. Compute HMAC-SHA256 with the signing key for key_id "mcps-hkdf-e8990a4e1526".
  4. Base64-encode the result and compare with the signature above.
```