EU AI Act

Compliance assessment — 2024/1689

Server: @modelcontextprotocol/server-everything

Slug: modelcontextprotocol-server-everything-20260910032240-1bff92
Scan id: 0d011be5-d736-4391-a1ac-11f6c141492b

Assessed at: 2026-09-10 03:22:40 UTC
Sentinel version: 0.4.0
Rules version: 2026-04-23

' Non-compliant

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

Table of contents

1. Executive summary

Assessment of @modelcontextprotocol/server-everything against EU AI Act: overall status non compliant. Of 5 controls, 0 met, 1 unmet, 0 partial, 4 not assessed, 0 not applicable. 1 control(s) had complete mapped-assessor execution evidence; 4 lacked sufficient execution evidence and 0 were outside the current assessor mapping. Unmet controls have findings at or above the framework's mandatory severity threshold and should be remediated before relying on this server in a regulated deployment. 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
Art.9Risk Management System'	Unmet	

8	
Art.12Record-Keeping? Not assessed0	
Art.13 Transparency & Provision of Information to Deployers? Not assessed0	
Art.14Human Oversight? Not assessed0	
Art.15 Accuracy, Robustness, and Cybersecurity ? Not assessed0	

4. Control details

Art.9 — Risk Management System

' Unmet

20/22 mapped assessor rule(s) are proven to have executed; 8 finding(s) observed (1 high, 7 medium); at least one finding is at or above the high threshold (status: unmet). 2 mapped assessor(s) did not execute, so this finding-backed result does not imply complete control coverage.

Evidence:

[High] Known CVEs in Dependencies (finding ef3ea7db-2b79-45f3-9e84-072f5e948dfd, confidence 78%)

SOURCE: external-content at npm:vitest@4.1.8 — Third-party package dependencies are external content resolved from public registries. A version with a published CVE ships the vulnerable code path as-i

[Medium] Abandoned Dependencies (finding 2208fdb2-04e4-41bb-91ca-a79db3875719, confidence 70%)

SOURCE: external-content at npm:cors@2.8.5 — An unmaintained dependency receives no patches for newly disclosed vulnerabilities. Every published CVE in the package after its last release date remains

[Medium] Abandoned Dependencies (finding f8718f42-5981-4f9b-92b3-1fd3e6d0127d, confidence 70%)

SOURCE: external-content at npm:jszip@3.10.1 — An unmaintained dependency receives no patches for newly disclosed vulnerabilities. Every published CVE in the package after its last release date remain

[Medium]

Abandoned Dependencies (finding cdec920e-ce2d-4d01-8561-98d9d5b34a14, confidence 70%)
SOURCE: external-content at npm:zod@4.0.0 — An unmaintained dependency receives no patches for newly disclosed vulnerabilities. Every published CVE in the package after its last release date remains p

[Medium]
Abandoned Dependencies (finding 8f381261-1338-4c72-8f5a-9b2d618369a0, confidence 70%)
SOURCE: external-content at npm:@types/cors@2.8.19 — An unmaintained dependency receives no patches for newly disclosed vulnerabilities. Every published CVE in the package after its last release date

[Medium]
Abandoned Dependencies (finding 39e1f19a-53c6-4b73-9b9e-b4f792e816eb, confidence 70%)
SOURCE: external-content at npm:prettier@2.8.8 — An unmaintained dependency receives no patches for newly disclosed vulnerabilities. Every published CVE in the package after its last release date rema

[Medium]
Abandoned Dependencies (finding 9ca53a83-ef21-4bc0-84d8-db69ab2bdc1a, confidence 70%)
SOURCE: external-content at npm:shx@0.4.0 — An unmaintained dependency receives no patches for newly disclosed vulnerabilities. Every published CVE in the package after its last release date remains p

[Medium]
Abandoned Dependencies (finding 0c358727-409f-44af-85a8-38c8fd5102ce, confidence 70%)
SOURCE: external-content at npm:typescript@5.6.2 — An unmaintained dependency receives no patches for newly disclosed vulnerabilities. Every published CVE in the package after its last release date re

Required mitigations:

- Update the flagged dependency to a version that resolves every listed CVE. Consult the NVD or OSV advisory linked in the finding for the minimum safe version. Re-run `npm audit` / `pip-audit` / `osv-scanner` after the bump to confirm no residual advisories remain. Where a patched version is not yet released, apply an override (npm `overrides`, `resolutions`, `pnpm.overrides`, or a Python constraints file) to pin a compatible fix, and file a tracking issue so the override is removed when the upstream fix lands.
- Replace the abandoned dependency with an actively maintained alternative. Where no alternative exists, vendor the minimal code the project uses and delete the dependency. If the package is internal/private and legitimately stable, mark it as such in a repository-local allowlist so the scanner can skip it on future runs. Track the abandonment risk in the project's SBOM per ISO 27001 A.8.8.

Art.12 — Record-Keeping

? Not assessed

4/5 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).

Art.13 — Transparency & Provision of Information to Deployers

? Not assessed

4/14 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); A8 (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).

Art.14 — Human Oversight

? Not assessed

5/13 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: K4 (tools); I12 (declared_capabilities); M5 (tools); H3 (tools); F1 (tools); F6 (tools); K15 (min_tools(2), tools); Q10 (tools).

Art.15 — Accuracy, Robustness, and Cybersecurity

? Not assessed

66/111 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); A3 (tools); A5 (tools); A7 (tools); A9 (tools); B1 (tools); B2 (tools); B3 (tools); B4 (tools); B5 (tools); B6 (tools); B7 (tools); E1 (connection_metadata); E2 (connection_metadata); E4 (min_tools(51), tools); F3 (tools); F4 (tools); F7 (min_tools(2), tools); G1 (tools); G2 (tools); G3 (tools); G4 (tools); G5 (tools); H2 (initialize_metadata); I3 (resource_templates, resources); I4 (resource_templates, resources); I6 (prompts); I7 (tools); I9 (tools); I10 (tools); I11 (roots); I13 (multi_server_tools, tools); J3 (tools); J6 (tools); K19 (source_files(container-config)); M1 (tools); M4 (tools); P1 (source_files(container-config)); P2 (source_files(container-config)); P5 (source_files(container-config)); P7 (source_files(container-config)); P9 (source_files(container-config)); P10 (source_files(container-config)); Q6 (tools); Q10 (tools).

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: `2026-09-11T05:31:18.842Z`
Canonicalization: `RFC8785`

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


```
1+qqJqmteWyPhR713D4fbx8U3ShsyHy/coBe4xngvYI=
```


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.
```