OWASP MCP Top 10

Compliance assessment — 2025

Server: dodopayments-mcp

Slug: dodopayments-mcp-20260921080358-1874fd
Scan id: ae3bc3a7-38f5-47f0-8cc4-1a3361b66c17

Assessed at: 2026-09-21 08:04:02 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.

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 dodopayments-mcp against OWASP MCP Top 10: overall status non compliant. Of 10 controls, 2 met, 5 unmet, 0 partial, 3 not assessed, 0 not applicable. 7 control(s) had complete mapped-assessor execution evidence; 3 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: high

Coverage ratio: 88%

Rules version: 2026-04-23

Analysis techniques applied:

- ast-taint
- capability-graph
- composite
- cross-module
- dependency-audit
- linguistic
- schema-inference
- similarity
- structural
- stub
- unicode

3. Controls summary

ControlName

	Status	Evidence
MCP01	Prompt Injection?	Not assessed	0
MCP02	Tool Poisoning'	Unmet	1
MCP03	Command Injection'	Met	0
MCP04	Data Exfiltration?	Not assessed	0
MCP05	Privilege Escalation'	Unmet	2
MCP06	Excessive Permissions'	Unmet	1
MCP07	Insecure Configuration'	Unmet	4
MCP08	Dependency Vulnerabilities'	Unmet	15
MCP09	Logging & Monitoring Failures'	Met	0
MCP10	Supply Chain Compromise?	Not assessed	0

4. Control details

MCP01 — Prompt Injection

? Not assessed

22/24 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: I3 (resource_templates, resources); I6 (prompts).

MCP02 — Tool Poisoning

' Unmet

12/15 mapped assessor rule(s) are proven to have executed; 1 finding(s) observed (1 high); at least one finding is at or above the high threshold (status: unmet). 3 mapped assessor(s) did not execute, so this finding-backed result does not imply complete control coverage.

Evidence:

[High] Excessive Scope Claims in Description (finding 5f148b3d-59d4-4ad5-983f-fcdbbbf2ea86, confidence 80%)

SOURCE: external-content at tool execute — Tool description for "execute" advertises excessive scope via 1 claim pattern(s). Strongest: "all-data-scope". AI clients use the description to shape permis

Required mitigations:

- Rewrite the description so it accurately reflects the tool's scope. Replace sweeping claims ("full access", "unrestricted", "admin mode") with the specific operations the tool actually performs and the specific subset of resources it touches. The AI client uses the description as its mental model of acceptable privilege — overclaims directly undermine least-privilege review.

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

14/15 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: I13 (multi_server_tools).

MCP05 — Privilege Escalation

' Unmet

6/7 mapped assessor rule(s) are proven to have executed; 2 finding(s) observed (2 high); at least one finding is at or above the high threshold (status: unmet). 1 mapped assessor(s) did not execute, so this finding-backed result does not imply complete control coverage.

Evidence:

[High] No Authentication on Network-Exposed Server (finding 02a80d24-a021-4949-b00e-83fe2f832e78, confidence 85%)

SOURCE: file-content at http.js:176:20 — Bare `listen(port)` call with no host argument — defaults to 0.0.0.0 on most Node stacks, and no middleware registration naming an authentication construct was

[High] No Authentication on Network-Exposed Server (finding 2663bb12-269b-474a-90f9-bcfbb2bf010e, confidence 85%)

SOURCE: file-content at src/http.ts:215:18 — Bare `listen(port)` call with no host argument — defaults to 0.0.0.0 on most Node stacks, and no middleware registration naming an authentication construct

Required mitigations:

• Register an authentication middleware before exposing the server on a network interface. For express: `app.use(authMiddleware)` BEFORE any route registration; for fastify: `fastify.addHook('preHandler', authHook)`; for FastAPI: `Depends(get_current_user)` on every router. Acceptable auth strategies: JWT bearer (validated against an issuer + audience), OAuth 2.1, API key (rotated, expirable, validated with constant-time comparison), or mutual TLS. NEVER rely on a query-string token alone — query strings leak via reverse-proxy logs and browser history. If the MCP server is meant to be workstation-local, bind to 127.0.0.1 / localhost instead of 0.0.0.0 — most listen() / uvicorn.run() calls default to 0.0.0.0 if the host argument is omitted, so set the host EXPLICITLY.

MCP06 — Excessive Permissions

' Unmet

4/7 mapped assessor rule(s) are proven to have executed; 1 finding(s) observed (1 high); at least one finding is at or above the medium threshold (status: unmet). 3 mapped assessor(s) did not execute, so this finding-backed result does not imply complete control coverage.

Evidence:

[High] Excessive Scope Claims in Description (finding 5f148b3d-59d4-4ad5-983f-fcdbbbf2ea86, confidence 80%)

SOURCE: external-content at tool execute — Tool description for "execute" advertises excessive scope via 1 claim pattern(s). Strongest: "all-data-scope". AI clients use the description to shape permis

Required mitigations:

• Rewrite the description so it accurately reflects the tool's scope. Replace sweeping claims ("full access", "unrestricted", "admin mode") with the specific operations the tool actually performs and the specific subset of resources it touches. The AI client uses the description as its mental model of acceptable privilege — overclaims directly undermine least-privilege review.

MCP07 — Insecure Configuration

' Unmet

11/11 mapped assessor rule(s) are proven to have executed; 4 finding(s) observed (2 low, 2 high); at least one finding is at or above the high threshold (status: unmet).

Evidence:

[Low] Schema Allows Unconstrained Additional Properties (finding 9b9c2db8-f1e1-4274-824a-650c47f47743, confidence 75%)

SOURCE: user-parameter at tool execute — Tool "execute" accepts arbitrary extra keys at 1 point(s) in its input contract. The declared properties are validated; the handler may still read undeclared k

[Low] Schema Allows Unconstrained Additional Properties (finding d2169aef-c097-4622-adfa-f9b996b1094e, confidence 75%)

SOURCE: user-parameter at tool search_docs — Tool "search_docs" accepts arbitrary extra keys at 1 point(s)

in its input contract. The declared properties are validated; the handler may still read unde

[High] No Authentication on Network-Exposed Server (finding 02a80d24-a021-4949-b00e-83fe2f832e78, confidence 85%)

SOURCE: file-content at http.js:176:20 — Bare `listen(port)` call with no host argument — defaults to 0.0.0.0 on most Node stacks, and no middleware registration naming an authentication construct was

[High] No Authentication on Network-Exposed Server (finding 2663bb12-269b-474a-90f9-bcfbb2bf010e, confidence 85%)

SOURCE: file-content at src/http.ts:215:18 — Bare `listen(port)` call with no host argument — defaults to 0.0.0.0 on most Node stacks, and no middleware registration naming an authentication construct

Required mitigations:

- Set additionalProperties: false on every object schema. This rejects any key outside the declared properties, closing the side-channel smuggling path and enforcing the schema's stated contract.
- Register an authentication middleware before exposing the server on a network interface. For express: `app.use(authMiddleware)` BEFORE any route registration; for fastify: `fastify.addHook('preHandler', authHook)`; for FastAPI: `Depends(get_current_user)` on every router. Acceptable auth strategies: JWT bearer (validated against an issuer + audience), OAuth 2.1, API key (rotated, expirable, validated with constant-time comparison), or mutual TLS. NEVER rely on a query-string token alone — query strings leak via reverse-proxy logs and browser history. If the MCP server is meant to be workstation-local, bind to 127.0.0.1 / localhost instead of 0.0.0.0 — most listen() / uvicorn.run() calls default to 0.0.0.0 if the host argument is omitted, so set the host EXPLICITLY.

MCP08 — Dependency Vulnerabilities

' Unmet

7/7 mapped assessor rule(s) are proven to have executed; 15 finding(s) observed (3 high, 12 medium); at least one finding is at or above the high threshold (status: unmet).

Evidence:

[High] Known CVEs in Dependencies (finding 6a8f2b39-b87d-4150-9a7f-5eebdfebd915, confidence 92%)

SOURCE: external-content at npm:qs@6.14.1 — Third-party package dependencies are external content resolved from public registries. A version with a published CVE ships the vulnerable code path as-is;

[High] Known CVEs in Dependencies (finding 4ff249a2-d4c8-4242-b717-c65a98671943, confidence 78%)

SOURCE: external-content at npm:@hono/node-server@1.19.10 — Third-party package dependencies are external content resolved from public registries. A version with a published CVE ships the vulnerable c

[High] Known

CVEs in Dependencies (finding 40d1a446-3075-4c90-b4c9-3245a41a892b, confidence 92%)

SOURCE: external-content at npm:hono@4.12.4 — Third-party package dependencies are external content resolved from public registries. A version with a published CVE ships the vulnerable code path as-is

[Medium] Abandoned Dependencies (finding f814e72b-9a41-4b83-bd73-a18e75df1bd6, confidence 70%)

SOURCE: external-content at npm:zod@3.25.20 — 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 fd457992-35da-49d4-89bb-280b2fb9be7c, confidence 70%)

SOURCE: external-content at npm:zod-to-json-schema@3.24.5 — An unmaintained dependency receives no patches for newly disclosed vulnerabilities. Every published CVE in the package after its last releas

[Medium] Abandoned Dependencies (finding 4f6701ae-b83e-4bf6-8468-2fcc1a816882, confidence 70%)

SOURCE: external-content at npm:zod-validation-error@4.0.1 — An unmaintained dependency receives no patches for newly disclosed vulnerabilities. Every published CVE in the package after its last relea

[Medium] Abandoned Dependencies (finding 9189b613-655e-4cd6-a9ea-c0ab8433d49f, confidence 70%)

SOURCE: external-content at npm:@cloudflare/cabidela@0.2.4 — An unmaintained dependency receives no patches for newly disclosed vulnerabilities. Every published CVE in the package after its last relea

[Medium] Abandoned Dependencies (finding 90cf551b-ef44-4c18-8beb-c5208bbacf3f, confidence 70%)

SOURCE: external-content at npm:@valtown/deno-http-worker@0.0.21 — An unmaintained dependency receives no patches for newly disclosed vulnerabilities. Every published CVE in the package after its last

[Medium] Abandoned Dependencies

(finding
2aa38ffd-c1e3-4
87c-8cb0-79526
2049bce,
confidence 70%)
SOURCE: external-content at npm:cookie-parser@1.4.6 — 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
b8bdb990-
b13f-464b-99b3-
d20e5577dec0,
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 1f5b31b6
-5f6a-47f0-9136-
12d563a7e4df,
confidence 70%)
SOURCE: external-content at npm:express@5.1.0 — An unmaintained dependency receives no patches for newly disclosed vulnerabilities. Every published CVE in the package after its last release date remai

[Medium]
Abandoned
Dependencies
(finding bec8b39
4-2c91-4f0a-90a
6-
cc771396368e,
confidence 70%)
SOURCE: external-content at npm:fuse.js@7.1.0 — An unmaintained dependency receives no patches for newly disclosed vulnerabilities. Every published CVE in the package after its last release date remai

[Medium]
Abandoned
Dependencies
(finding 34dde0c
a-675f-4e97-923
e-2f508dfab390,
confidence 70%)
SOURCE: external-content at npm:minisearch@7.2.0 — An unmaintained dependency receives no patches for newly disclosed vulnerabilities. Every published CVE in the package after its last release date re

[Medium]
Abandoned
Dependencies
(finding
2913030b-a6c5-
415e-9f76-18117
4c1f867,
confidence 70%)
SOURCE: external-content at npm:typescript@5.8.3 — An unmaintained dependency receives no patches for newly disclosed vulnerabilities. Every published CVE in the package after its last release date re

[Medium]
Abandoned
Dependencies
(finding 219c431
9-7fca-4b8f-94b9
-2f8481152228,

confidence 70%)
SOURCE: external-content at npm:yargs@17.7.2 — An unmaintained dependency receives no patches for newly disclosed vulnerabilities. Every published CVE in the package after its last release date remain

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.

MCP09 — Logging & Monitoring Failures

' Met

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

MCP10 — Supply Chain Compromise

? Not assessed

24/27 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: I5 (resource_templates, resources); 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: `2026-09-21T08:04:02.860Z`
Canonicalization: `RFC8785`

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


```
ZvvQp7cDYzv8J+Cb2zv0+OKZEYJ/lHg5vIBVW7r0XRU=
```


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.
```