TRUST REPORT

serenialabs.space

https://serenialabs.space/api/mcp

Scanned May 3, 2026 · 06:08 UTC

B

VERDICT

REVIEW

Score	**87** / 100
Risk	**MEDIUM**
Tier	Perimeter

TOOLS	RISK SURFACE	RULES PASSED	AUTH
0	0R · 0W · 0D	15/16	Required

WHY THIS VERDICT

01 Insufficient probe coverage to evaluate the server

02 Authorization server metadata does not advertise a jwks_uri

CATEGORY BREAKDOWN

Trust dimensions

Each dimension shows percent of contributing rule weight earned.

Transport and endpoint hygiene — 100%

8/8 checks passed (4 n/a) ? 100%.

MCP protocol hygiene — n/a

No applicable signals for this scan.

Auth discovery posture — 94%

7/8 checks passed, 1 failed ? 94%.

Capability risk — n/a

No applicable signals for this scan.

Transparency and operability — n/a

No applicable signals for this scan.

Coverage and confidence — n/a

Coverage: none. Confidence: low. Perimeter-only scan: the MCP JSON-RPC handshake did not comple?

RULE FINDINGS

All rules evaluated

Failing rules are listed first, ordered by severity. Weight reflects the rule's contribution to the score.

FAIL	**Authorization server advertises a JWKS URI**	LOW · w2
PASS	No code-execution tools in the public surface	CRITICAL · w14
PASS	No credential-access tools in the public surface	CRITICAL · w12
PASS	No admin-control tools in the public surface	CRITICAL · w10
PASS	No filesystem-write tools in the public surface	CRITICAL · w10
PASS	Server uses HTTPS	HIGH · w10
PASS	No unconstrained prompt-injection vectors	HIGH · w8
PASS	Server validates the Origin header	HIGH · w8
PASS	TLS handshake completes with a trusted certificate	HIGH · w8
PASS	No destructive tools in the public surface	HIGH · w8
PASS	No financial-action tools in the public surface	HIGH · w6
PASS	No credentials in the endpoint URL	HIGH · w6
PASS	Authorization server issuers are HTTPS	HIGH · w6
PASS	No insecure grant types advertised	HIGH · w6
PASS	Authorization server advertises PKCE with S256	HIGH · w6
PASS	Auth-discovery metadata URLs are HTTPS and publicly routable	HIGH · w6
PASS	No prompt-manipulation patterns in tool descriptions	HIGH · w6
PASS	Tool annotations are consistent with the surface	HIGH · w6
PASS	No outbound network-access tools in the public surface	HIGH · w4
PASS	No outbound-messaging tools in the public surface	HIGH · w4

RULE FINDINGS (continued)

PASS	All tools declare an input schema	MEDIUM · w6
PASS	Tool surface unchanged since the previous scan	MEDIUM · w5
PASS	Tool surface does not mention PII	MEDIUM · w5
PASS	TLS 1.2 or newer is negotiated	MEDIUM · w5
PASS	No secret material leaked in observed metadata	MEDIUM · w5
PASS	No injection vectors in resource or prompt entries	MEDIUM · w5
PASS	Auth-required server advertises discovery metadata	MEDIUM · w5
PASS	No injection vectors in initialize.instructions	MEDIUM · w5
PASS	No description-borne injection vectors	MEDIUM · w5
PASS	Server identity claim matches transport identity	MEDIUM · w4
PASS	Endpoint hostname is reachable from the public internet	MEDIUM · w4
PASS	All tools have descriptions	LOW · w4
PASS	Server advertises HTTP Strict-Transport-Security	LOW · w3
PASS	Authorization server metadata is parseable	LOW · w3
PASS	Server advertises an MCP protocol version	LOW · w3
PASS	TLS certificate has at least 14 days until expiry	LOW · w2
PASS	Authorization server advertises a token endpoint	LOW · w2
PASS	Tool names are ASCII identifier-shaped	LOW · w2
PASS	Tool count is reasonable	LOW · w2
PASS	Tool input schemas have bounded shape	LOW · w2
PASS	Server identifies itself	INFO · w2
PASS	Probe response size is within the safe bound	INFO · w1

RULE FINDINGS (continued)

PASS	Probe redirects are within the safe bound	INFO · w1
PASS	tools/list returned a tool array	INFO · w1
PASS	Server advertises a version string	INFO · w1
PASS	Probe response content-type was acceptable	INFO · w1