

The State of MCP Security, 2026

AgentAuditKit 0.3.59 — offline, deterministic

Scan date: 2026-07-26 · Corpus: 2,303 distinct public MCP server configs ({'crawl': 664, 'registry': 1639})

Headline findings — % of public MCP servers

Rule	Severity	% of corpus	Configs	Finding
AAK-MCP-001	CRITICAL	52.3%	1205	Remote MCP server without authentication
AAK-MCP-005	MEDIUM	19.5%	450	MCP server uses npx/uvx to fetch and execute remote packages
AAK-OAUTH-008	LOW	18.3%	421	MCP OAuth surface with no RFC 9728 Protected Resource Metadata discovery
AAK-MCP-006	MEDIUM	7.8%	179	MCP server command uses relative path
AAK-MCP-003	HIGH	3.0%	70	MCP server environment exposes secrets
AAK-SECRET-007	MEDIUM	3.0%	70	Secret in MCP server environment block
AAK-MCP-STDIO-LAUNCHER-INJECTION-001	HIGH	2.1%	49	MCP stdio server launches a shell-style interpreter with an exec flag or interpolated command
AAK-MCP-009	HIGH	1.9%	44	MCP server URL points to localhost/internal network
AAK-TRANSPORT-003	MEDIUM	1.6%	36	Deprecated SSE transport in use
AAK-MCP-004	HIGH	0.5%	12	Excessive number of MCP servers declared

Authentication posture (2026-07-28 profile)

No authentication: 1205 of 2,303 (52.3%). RFC 9728 PRM discovery: 0 of 2,303. Of inline-auth remotes, 421 of 421 hardcode a static credential.

Reproduce (offline, deterministic): `make report`. Full narrative + method: `research/state-of-mcp-2026/REPORT.md`.