The State of MCP Security, 2026

AgentAuditKit 0.6.29 — offline, deterministic

Scan date: ? · 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	50.6%	1166	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	18.4%	424	MCP OAuth surface with no RFC 9728 Protected Resource Metadata discovery
AAK-SUPPLY-001	MEDIUM	12.3%	284	MCP server package not pinned to exact version
AAK-MCP-006	MEDIUM	7.8%	179	MCP server command uses relative path
AAK-MCP-STDIO-LAUNCHER-INJECTION	HIGH	2.1%	49	MCP stdio server launches a shell-style interpreter with an exec flag or interpolated a
AAK-TRANSPORT-003	MEDIUM	2.0%	47	Deprecated SSE transport in use
AAK-MCP-003	HIGH	1.3%	30	MCP server environment exposes secrets
AAK-MCP-SERENA-CVE-2026-49471-001	HIGH	0.8%	19	Serena MCP toolkit < 1.5.2 (unauthenticated dashboard → DNS-rebinding RCE)
AAK-MCP-004	HIGH	0.5%	12	Excessive number of MCP servers declared

Authentication posture (2026-07-28 profile)

No authentication: 1166 of 2,303 (50.6%). RFC 9728 PRM discovery: 0 of 2,303. Of inline-auth remotes, 424 of 424 hardcode a static credential.

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