Security Update: CVE-2026-30623 — Command Injection via Anthropic's MCP SDK

Blog

April 21, 2026

Krrish Dholakia
CEO, LiteLLM

Ishaan Jaffer
CTO, LiteLLM

On April 15, 2026, OX Security published an advisory covering **command-injection in Anthropic's MCP SDK's stdio transport** (`StdioServerParameters` runs whatever `command` it's handed). This has been fixed on LiteLLM since `v1.83.6-nightly`.

The fix landed in commit `7b7f304` (PR #25343) and has been in every release from `v1.83.6-nightly` onward. `v1.83.7-stable` includes it.

TLDR;

- **This was not exploitable by unauthenticated users.** The affected endpoints (MCP server creation and the `/mcp-rest/test/*` preview endpoints) all sit behind LiteLLM's auth. An attacker needed a valid LiteLLM API key — and, with the patch, the `PROXY_ADMIN` role — before they could reach this code path.
- **The fix has been live since `v1.83.6-nightly`.** The first stable release with the fix is `v1.83.7-stable`. Full list of patched versions below.
- **If you find other vulnerabilities, please send them our way.** We run a bug bounty program and pay out for P0 (supply chain) and P1 (unauthenticated proxy access) issues. See our previous security update for the current bounty table.

What was the issue

Per OX Security's advisory:

> LiteLLM contains an authenticated remote command execution vulnerability in its MCP server creation functionality. The application allows users to add MCP servers via a JSON configuration specifying arbitrary command and args values. LiteLLM [illegible] values on the host without validation, enabling attackers to run arbitrary operating system commands.

Ask AI

Concretely: when adding an MCP server with `transport: stdio`, the `command` field was passed straight through to `StdioServerParameters` and executed as a subprocess on the proxy host. An authenticated user with permission to create MCP servers could run arbitrary commands as the LiteLLM process.

← Blog

- **CVE:** CVE-2026-30623
- **Severity:** Critical
- **Auth required:** Yes (authenticated RCE, not unauthenticated)
- **Affected surfaces:**
  - MCP server creation/update (`NewMCPServerRequest`, `UpdateMCPServerRequest`)
  - `/mcp-rest/test/connection` and `/mcp-rest/test/tools/list` preview endpoints
  - Servers rehydrated from config or the DB at runtime

What the fix does

Commit `7b7f304` lands four changes:

1. **Command allowlist for stdio transport.** A new constant `MCP_STDIO_ALLOWED_COMMANDS` restricts stdio `command` values to a small set of known MCP launchers:

   ```
   MCP_STDIO_ALLOWED_COMMANDS = frozenset(
       {"npx", "uvx", "python", "python3", "node", "docker", "deno"}
   )
   ```

   The list is extensible at deploy time via the `LITELLM_MCP_STDIO_EXTRA_COMMANDS` env var (comma-separated) if you need to allow additional binaries.

2. **Pydantic-level validation.** Both `NewMCPServerRequest` and `UpdateMCPServerRequest` now reject configs whose `command` basename is not in the allowlist — so the bad input never makes it past request parsing.

3. **Defense-in-depth at runtime.** `_create_mcp_client` re-validates the command when instantiating the stdio client, so any `MCPServer` reconstructed from an older DB row or config file (predating the allowlist) is also blocked at spawn time.

4. **Locked down the preview endpoints.** `/mcp-rest/test/connection` and `/mcp-rest/test/tools/list` now require the `PROXY_ADMIN` role. These "try before you add" endpoints were the easiest way to trigger command execution without persisting anything.

Versions with the fix

The patch is present in every LiteLLM release tagged from `v1.83.6-nightly` onward. Confirmed tags at the time of publishing:

← Blog

Version	Type
`v1.83.6-nightly`	First release with the fix
`v1.83.7.rc.1`	Release candidate
`v1.83.7-stable`	Stable
`v1.83.8-nightly`	Nightly
`v1.83.9-nightly`	Nightly
`v1.83.10-nightly`	Nightly

Any LiteLLM release newer than these also includes the fix.

What you should do

- **Upgrade.** Move to `v1.83.7-stable` or later. If you track nightlies, anything `>= v1.83.6-nightly` is patched.
- **Audit existing MCP servers.** If you have stdio MCP servers configured from before the upgrade, any row whose `command` basename isn't in the allowlist will now fail to start. Either update the config to use an allowed launcher (e.g. `npx`, `uvx`, `python`) or add the binary to `LITELLM_MCP_STDIO_EXTRA_COMMANDS`.
- **Review who has `PROXY_ADMIN`.** The stdio test endpoints are now admin-only. If you'd previously delegated MCP testing to non-admin users, they'll now hit a 403.

Credit

Thanks to the OX Security research team — **Moshe Siman Tov Bustan**, **Mustafa Naamnih**, and **Nir Zadok** — for the disclosure. Their full cross-ecosystem writeup is here.

If you find a security issue in LiteLLM, please report it through our bug bounty program.

Tags: security

← Blog