Langflow CVE-2026-105740 ? 60-Minute Runbook

CVSS 9.9 ? exploited in the wild

Fixed by: Langflow 1.10.3 or newer

Any logged-in Langflow user can run OS commands on the server by adding an MCP server with the stdio transport ? the command field is passed straight to the shell with no validation.

Honeypots logged 1,423 exploit attempts from 27 attacker IPs since September 19, 2026, spiking to 333 in a single day on October 11.

Minutes 0-5 ? Confirm your version

1. Run: pip show langflow | grep -i version ? Docker users check the deployed image tag (e.g. langflowai/langflow:1.8.x).
2. Below 1.9.0 -> EXPOSED: any authenticated user can get RCE.
3. 1.9.0-1.10.2 -> AT-RISK: a second CVE record extends the flaw through 1.10.2. Upgrade to the latest anyway.
4. 1.10.3 or newer -> patched; skip to minutes 50-60.

Minutes 5-15 ? Cut the easiest doors first

1. Set LANGFLOW_AUTO_LOGIN=false ? attackers try /api/v1/auto_login right after checking your version, then fall back to common username/password combos.
2. Block the known campaign IPs at your firewall: 192.255.229.92 and the exfil host 146.70.211.112.
3. Enforce strong, unique passwords for every Langflow login ? this flaw turns every authenticated user into a potential root.

Minutes 15-30 ? Audit your MCP servers

1. List every configured MCP server and look for stdio-transport entries you did not authorize: curl -s -H "Authorization: Bearer $LF_API_KEY" http://localhost:7860/api/v2/mcp/servers | python3 -m json.tool | grep -A3 stdio
2. Malicious MCP configs live in project settings (invisible in the flow editor) and re-execute every time the server list loads ? deleting the flow does not remove them. Delete anything you did not authorize.

Minutes 30-45 ? Upgrade

1. Upgrade Langflow to 1.10.3 or newer. 1.9.0 is the absolute minimum ? do not stop there.

Minutes 45-55 ? Rotate secrets on the host

1. Rotate all secrets the host could read: Langflow secrets (LANGFLOW_SECRET_KEY, LANGFLOW_SUPERUSER_PASSWORD), API keys, database credentials, model tokens. Attackers exfiltrate environment variables and Langflow secrets ? patching does not un-read them.
2. Restrict who gets a Langflow login, starting today.

Minutes 50-60 ? Hunt and verify

1. Grep logs for auto-login hits ? any 200 there means someone walked straight in: grep "/api/v1/auto_login" your Langflow logs; and for MCP registrations: grep "POST /api/v2/mcp/servers" /var/log/langflow/*.log

2. Hunt for new processes, cron entries, or outbound connections you cannot explain ? RCE gives the attacker the whole host, not just Langflow.

3. Re-run the version check; record versions before/after, the MCP audit result, and the rotation list.

Source: Fleet checker: langflow-cve-2026-105740.html (disclosed Oct 5, 2026; active exploitation reported Oct 15, 2026)

Generated by BreachHunter (Ingenious AI) from the fleet’s published exposure checker for this CVE. Assessment guidance only ? verify eac