GOVERNMENT OF THE REPUBLIC OF VANUATU

PRIME MINISTER'S OFFICE

CERTVU
DEPARTMENT OF COMMUNICATIONS & DIGITAL TRANSFORMATION

PM B 9108 Port Vila, Vanuatu
Tel: (678) 33380

GOUVERNEMENT DE LA REPUBLIQUE DU VANUATU

BUREAU DU PREMIER MINISTRE

CERTVU

DEPARTMENT DE COMMUNICATION ET DE TRANSFORMATION NUMERIQUE

SPP 9108 Port Vila, Vanuatu
Tel: (678) 33380

8 July 2026

Advisory 161: CVE-2026-55255 — Langflow Cross-Tenant IDOR (Unauthorized Flow Execution)

Release Date: 07th July 2026
Impact: HIGH / CRITICAL
TLP: CLEAR

The Department of Communications and Digital Transformation (DCDT) through CERT Vanuatu (CERTVU), provides the following advisory.

This alert is relevant to Organizations and System/Network administrators that utilize the above products. This alert is intended to be understood by technical users and systems administrators.

What is it?

An Insecure Direct Object Reference (IDOR) in Langflow's `/api/v1/responses` endpoint — an OpenAI-Responses-compatible API where the `model` field is actually a flow UUID (Langflow exposes each user's flow as a callable "model"). The vulnerable helper function, `get_flow_by_id_or_endpoint_name()`, resolves a flow by UUID without checking that the flow belongs to the requesting user. A separate resolution path (by endpoint name) does enforce ownership correctly — only the UUID lookup path is broken. The result: any authenticated user can execute any other user's flow simply by supplying that flow's UUID, with no authorization check in between.

What are the systems affected?

Any Langflow deployment prior to 1.9.2, particularly:

- Multi-tenant or managed/SaaS Langflow deployments where multiple distinct users or organizations share one instance — this is where the vulnerability has real teeth, since it breaks the tenant isolation boundary.
- Single-tenant self-hosted instances are technically affected too, but the practical impact is much smaller there, since anyone with valid credentials on a single-tenant instance may already have broad access.

What does this mean?

How it's exploited:

• Attacker needs only a **low-privilege, valid, authenticated account** on the target Langflow instance — no special role required.
• Attacker sends a request to `/api/v1/responses`, setting the `model` field to another user's flow UUID (flow IDs can potentially be discovered, guessed, or obtained through other means).
• Because the UUID lookup path skips the ownership check, Langflow executes the victim's flow on the attacker's behalf.
• Depending on what that flow does, this can expose the victim's data, credentials embedded in the flow (e.g., API keys for connected LLM providers or data sources), or let the attacker manipulate/trigger workflows they have no right to invoke — a straightforward cross-tenant confidentiality and integrity breach.

Mitigation process

CERTVU recommends the following:

• **Patch:** Upgrade Langflow to **1.9.2 or later**. The fix normalizes `user_id` once and enforces ownership on both the UUID and endpoint-name lookup branches, makes cross-user lookups return a uniform 404 (avoiding a 403-vs-404 existence oracle), and hardens the `/api/v1/run*` routes with auth-aware dependency wrappers as defense in depth.
• **If immediate patching isn't possible:**

- Restrict Langflow instance access to trusted networks/VPN, especially for any multi-tenant or shared deployment.
- Review flow UUIDs for predictability/enumerability in your deployment and rotate any that may have been exposed in logs, URLs, or shared links.
- Audit for any credentials or secrets embedded directly inside flows (API keys, connection strings); move these to a secrets manager instead where the flow orchestration supports it.

Reference

1. https://www.cisa.gov/news-events/alerts/2026/07/07/cisa-adds-three-known-exploited-vulnerabilities-catalog
2. https://www.cve.org/CVERecord?id=CVE-2026-55255