مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Actively Exploited Remote Code Execution Vulnerability in Langflow

Tracking #:432318662

Date:26-03-2026

TLP: WHITE

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed that a critical security vulnerability has been identified in Langflow that enables unauthenticated remote code execution (RCE) and is being widely exploited.

TECHNICAL DETAILS:

A critical security vulnerability has been identified in Langflow, tracked as CVE-2026-33017, enabling unauthenticated remote code execution (RCE).
The flaw exists in the /api/v1/build_public_tmp/{flow_id}/flow endpoint, which improperly allows attacker-controlled input to be executed via Python's exec() function without authentication or sandboxing.
An attacker can exploit this vulnerability remotely with no credentials or user interaction, leading to full system compromise, including command execution, data exfiltration, and lateral movement. This is distinct from CVE-2025-3248, which fixed /api/v1/validate/code by adding authentication.

Vulnerability Details

- CVE ID: CVE-2026-33017
- Severity: Critical (CVSS v4: 9.3)
- CWE:
  - CWE-94: Code Injection
  - CWE-95: Improper Neutralization of Directives in Dynamically Evaluated Code
  - CWE-306: Missing Authentication
- Affected Versions: ≤ 1.8.1
- Patched Version: ≥ 1.9.0
- Attack Vector: Network (Remote)
- Privileges Required: None
- User Interaction: None

RECOMMENDATIONS:

- Organizations using Langflow should treat this as an urgent patching priority and apply compensating controls immediately if patching is not feasible.

Kindly circulate this information to your subsidiaries and partners as well as share with us any relevant information and findings.

The UAE Cyber Security Council extends its appreciation for the continued collaboration.

REFERENCES:

- https://github.com/langflow-ai/langflow/security/advisories/GHSA-vwmf-pq79-vjvx