مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Critical Vulnerability in Langflow

Tracking #:432319061

Date:03-06-2026

TLP: WHITE

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed a critical Remote Code Execution (RCE) vulnerability has been identified in the AI workflow orchestration platform Langflow.

TECHNICAL DETAILS:

A critical Remote Code Execution (RCE) vulnerability has been identified in the AI workflow orchestration platform Langflow and tracked as CVE-2026-48519 with a CVSS score of 9.6 (Critical).

Vulnerability Details:

- Vulnerability: Remote Code Execution (RCE)
- CVE ID: CVE-2026-48519
- Severity: Critical
- CVSS Score: 9.6
- Affected Product: Langflow
- Affected Versions: Langflow 1.9.1 and earlier
- Fixed Version: Langflow 1.9.2 and later
- Exploitation Method: Crafted JSON payload containing malicious Python code

RECOMMENDATIONS:

- Upgrade Langflow immediately to fixed version.

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/releases/tag/1.9.5