مجلس الأمن السيبراني

CYBER SECURITY COUNCIL

United Arab Emirates

Critical Remote Code Execution Vulnerability in Langflow

Tracking #:432318490

Date:02-03-2026

THE INFORMATION CONTAINED WITHIN IS THE PROPERTY OF THE CYBER SECURITY COUNCIL OF THE UNITED ARAB EMIRATES GOVERNMENT AND IS TO BE USED EXCLUSIVELY FOR INTELLGIENCE PURPOSES. IT MAY NOT BE USED IN ANY LEGAL OR PUBLIC MATTER WITHOUT THE EXPLICIT APPROVAL OF THE CYBER SECURITY COUNCIL

TLP: WHITE

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed a critical vulnerability in Langflow that could be exploited to execute arbitrary commands on affected systems.

TECHNICAL DETAILS:

A critical Remote Code Execution (RCE) vulnerability has been identified in Langflow, a widely adopted visual platform used to design and deploy AI-powered agents and workflows.
Successful exploitation allows remote attackers to execute arbitrary system commands on the server hosting Langflow, potentially leading to full system compromise.

Vulnerability Details

- **CVE ID:** CVE-2026-27966
- **CVSS Score:** 9.8 Critical
- **Vulnerability Type:** Remote Code Execution (RCE)
- The vulnerability exists in Langflow's CSV Agent component, which processes spreadsheet data using the backend framework LangChain.
- In affected versions, a backend setting (allow_dangerous_code) was hardcoded to True, automatically enabling execution of arbitrary Python code on the host system. This unsafe configuration allows attackers to exploit the system through prompt injection, causing the AI agent to run malicious operating system commands.
- Because this behavior could not be disabled via configuration or the user interface, exposed instances are at risk of remote code execution.

Affected Products

- Langflow versions prior to 1.6.9

Fixed Versions

- Langflow 1.8.0 and later

RECOMMENDATIONS:

The UAE Cyber Security Council recommends updating the affected versions to the fixed or latest versions released by Langflow.

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://nvd.nist.gov/vuln/detail/CVE-2026-27966