مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Actively Exploited Critical Vulnerability in Langflow

Tracking #:432317216

Date:06-05-2025

TLP: WHITE

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed a critical security vulnerability in Langflow is being actively exploited in the wild.

TECHNICAL DETAILS:

A critical security vulnerability—**CVE-2025-3248**—affecting **Langflow versions prior to 1.3.0** is being **actively exploited in the wild**. This unauthenticated remote code execution (RCE) vulnerability allows attackers to execute arbitrary code through the /api/v1/validate/code endpoint, due to missing authentication for a critical function.

With a **CVSS v3.1 score of 9.8 (Critical)**, this flaw represents an immediate and severe risk to any system running an affected version of Langflow. Exploitation may result in full system compromise, unauthorized data access, malware deployment, or lateral movement within networks. Organizations are urged to treat this as a top-priority issue and implement mitigations or upgrades without delay.

Vulnerability Details

- **CVE ID:** CVE-2025-3248
- **Vendor:** Langflow-AI
- **Product Affected:** Langflow
- **Affected Versions:** 0.0.0 through 1.2.0
- **Fixed Version:** 1.3.0
- **User Interaction:** None
- **CWE:** CWE-306 – Missing Authentication for Critical Function
- **CVSS v3.1 Base Score:** 9.8 (CRITICAL)
  Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

Description:
Langflow's /api/v1/validate/code endpoint fails to implement authentication, enabling unauthenticated attackers to send crafted HTTP requests and execute arbitrary code. If exploited, an attacker could:

- Take full control of the affected system,
- Exfiltrate sensitive data,
- Establish persistence,
- Use the compromised host for further attacks.

RECOMMENDATIONS:

- Upgrade to Langflow version 1.3.0 or later to eliminate the vulnerability.
- Review logs for suspicious HTTP POST requests to the vulnerable endpoint.

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/1.3.0