مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Critical Vulnerabilities in IBM Langflow OSS

Tracking #:432319197

Date:26-06-2026

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed IBM has disclosed two critical security vulnerabilities affecting IBM Langflow Open Source (OSS) that could allow unauthenticated attackers to gain access to protected functionality and execute arbitrary code on vulnerable servers.

TECHNICAL DETAILS:

IBM has disclosed two critical security vulnerabilities affecting IBM Langflow Open Source (OSS) that could allow unauthenticated attackers to gain access to protected functionality and execute arbitrary code on vulnerable servers.

Vulnerability Details

1. **CVE-2026-10561 – Unauthenticated Remote Code Execution**
   - **Severity:** Critical (CVSS v3.1: 10.0)
   - **CWE:** CWE-94 – Improper Control of Generation of Code
   - Langflow OSS has a vulnerability due to an improper isolation of Python execution combined with an authentication bypass that allows an unauthenticated attacker to execute arbitrary code on the host system, resulting in complete compromise

2. **CVE-2026-7664 – Authorization Bypass**
   - **Severity**: Critical (CVSS v3.1: 9.8)
   - **CWE**: CWE-287 – Improper Authentication
   - Langflow's MCP transport endpoint fails to properly validate authentication before processing requests. The endpoint implicitly trusts incoming requests and skips credential verification. This enables unauthenticated users to invoke protected functionality

Affected Versions & Fixed Version:

CVE	Affected Versions	Fixed Version
CVE-2026-10561	Langflow OSS 1.0.0 – 1.9.3	Langflow OSS version 1.9.4
CVE-2026-7664	Langflow OSS 1.0.0 – 1.8.4	Langflow OSS version 1.9.1

RECOMMENDATIONS:

Immediate Actions:

- Upgrade Langflow OSS to fixed version across all affected environments as soon as possible.

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://www.ibm.com/support/pages/node/7277243
- https://www.ibm.com/support/pages/node/7277242