مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Multiple Critical Vulnerabilities in Langflow

Tracking #:432319241

Date:04-07-2026

TLP: WHITE

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed IBM Security researchers have disclosed six Critical vulnerabilities affecting Langflow OSS, an open-source platform for building AI and LLM-powered applications.

TECHNICAL DETAILS:

IBM Security researchers have disclosed six Critical vulnerabilities affecting Langflow OSS, an open-source platform for building AI and LLM-powered applications. Collectively, these vulnerabilities could allow attackers to execute arbitrary code, bypass authorization controls, compromise application integrity, access sensitive data, perform cross-tenant attacks, and gain complete control of vulnerable Langflow deployments.
The vulnerabilities impact Langflow OSS versions 1.0.0 through 1.10.0 (depending on the CVE). Although there are no confirmed reports of active exploitation, proof-of-concept (PoC) exploits have been demonstrated for several vulnerabilities. Organizations should upgrade immediately and review their deployments for indicators of compromise.

Critical Vulnerability Details:

- CVE-2026-10134: Unauthenticated Remote Code Execution (RCE) – Severity: Critical – CVSS: 10.0
- CVE-2026-7803: Flow Validation Bypass – Severity: Critical – CVSS: 9.8
- CVE-2026-7871: Insecure Redis Deserialization – Severity: Critical – CVSS: 9.8
- CVE-2026-7873: Code Injection / OS Command Execution – Severity: Critical – CVSS: 9.9
- CVE-2026-10140: Cross-Tenant API Credential Reuse – Severity: Critical – CVSS: 9.6
- CVE-2026-7663: Streamable MCP Authorization Bypass – Severity: Critical – CVSS: 9.8 (NVD) / 9.1 (IBM CNA)

Fixed Version:

- Langflow OSS version 1.10.1 or later

RECOMMENDATIONS:

Immediate Actions:

- Update Langflow OSS version to fixed version or later immediately.

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://pypi.org/project/langflow/