

## Langflow AI Platform Faces Active Exploitation of Critical Remote Code Execution Vulnerability



A critical authenticated remote code execution vulnerability in Langflow, an open-source AI application platform, has been targeted in over 1,400 exploit attempts recorded by honeypot systems.

- CVE-2026-105740 is a critical authenticated remote code execution flaw in Langflow with a CVSS score of 9.9
- Security researchers at Previdian recorded 1,423 exploit attempts against honeypot systems
- Langflow is an open-source platform for building AI applications and agentic workflows
- DataStax, Langflow's parent company, was acquired by IBM in February 2025
- Threat actors are actively targeting the vulnerability in the wild

## Vulnerability Details

A critical security vulnerability tracked as **CVE-2026-105740** has been discovered in Langflow, an open-source platform used by developers to build artificial intelligence applications and agentic workflows. The flaw carries a CVSS severity score of 9.9, indicating an extremely high risk. The vulnerability enables authenticated remote code execution, allowing threat actors who have obtained valid credentials to execute arbitrary code on affected systems.

Security researchers at Previdian have issued an alert confirming that the vulnerability is under active exploitation. Their honeypot systems recorded 1,423 distinct exploit attempts, demonstrating sustained attacker interest in the flaw.

## Platform Context

Langflow is maintained by DataStax, which was acquired by IBM in February 2025. As an open-source platform, Langflow is deployed across various environments where organizations are developing AI-driven applications and automated workflows. The platform's widespread adoption in the AI development community increases the potential attack surface for this vulnerability.

## Threat Landscape

The active exploitation observed by Previdian indicates that threat actors have developed working exploits and are systematically scanning for vulnerable Langflow instances. The authenticated nature of the vulnerability suggests attackers may be combining credential compromise techniques with this remote code execution flaw to gain deeper access to target systems.

Organizations running Langflow deployments should treat this as an urgent security matter requiring immediate attention and remediation.

## What to do now

1. Immediately inventory all Langflow deployments across development, testing and production environments
2. Apply security patches or updates released by DataStax for CVE-2026-105740 without delay
3. Review and strengthen authentication mechanisms for all Langflow instances, implementing multi-factor authentication where possible
4. Audit access logs for Langflow systems to identify any suspicious authentication or code execution activity since the vulnerability disclosure
5. Isolate unpatched Langflow instances from production networks until remediation is complete
6. Coordinate with application development teams to assess potential impact on AI workflow projects and establish secure deployment practices