CYBER ADVISORY

Wednesday, July 22, 2026 **CAL-CSIC-202607-A-012**

Remote Code Execution Vulnerability Identifed in LangFlow

Proof-of Concept Available	Full System Compromise	Remote Code Execution	Patch Available

The California Cybersecurity Integration Center (Cal-CSIC) has become aware of a critical vulnerability that impacts LangFlow and has been added to CISA's Known Exploited Vulnerability catalog. LangFlow is typically deployed as a service or application stack used for building and running LLM/flow-based workload often on developer workstations, internal app servers, containers, or cloud instances that may be accessible from broader networks. CVE-2026-0770 carries a CVSS 3.1 score of 9.8.[1]

CVE-2026-0770 is a remote code execution vulnerability that exists within the handling of the exec_globals parameter provided to the validate endpoint. The issue results from the inclusion of a resource from an untrusted control sphere. The vulnerability allows an attacker to remotely execute arbitrary commands without requiring authentication, potentially as the system's root user. Successful exploitation would lead to full system compromise, data exfiltration, installation of malicious payloads, and pivoting towards internal networks.[2]

LangFlow has acknowledged the exploit and have issued release notes recommending upgrading to the latest version of LangFlow. A public proof-of-concept is available.[3]

The Cal-CSIC recommends following the LangFlow update guidance as soon as possible. If patching cannot be immediately accomplished utilized one of the following workarounds until the vendor patch can be completed:

1. Segment and remove from internet exposure; allowlist management networks at the firewall or security group.
2. Access control; require stronger authentication – deploy a reverse proxy or zero-trust broker in front of the UI and APIs.
3. Virtual Patching/WAF; block request patterns that attempt to inject external references or suspicious inclusion parameters tuned from the vendor's description once available.

4. Monitoring and Log Retention; alerts on new child processes form the Langflow service, unexpected outbound connections, authentication anomalies.[4]

For additional details regarding CVE-2026-0770, please use this link:

PoC: https://github.com/affix/CVE-2026-0770-PoC

Affected Product and Version

Product	Affected Version
LangFlow	All versions up to 1.7.3

Cal-CSIC services are provided at no cost to assist organizations in strengthening their cybersecurity defenses. If you need assistance or wish to verify this communication, please contact us at (833) REPORT-1, or (916) 636-2997. Visit our website for more details: California Cybersecurity Integration Center | California Governor's Office of Emergency Services

References

[1] NVD; "CVE-2026-0770 Detail"; https://nvd.nist.gov/vuln/detail/CVE-2026-0770; accessed 22 July 2026
[2] Pentest Tools; "Langflow < 1.3.0 - Remote Code Execution via validate_code exec() (CVE-2026-0770)"; https://pentest-tools.com/vulnerabilities-exploits/langflow-130-remote-code-execution-via-validate-code-exec_28889; accessed 22 July 2026
[3] Github; "CVE-2026-0770 PoC"; https://github.com/affix/CVE-2026-0770-PoC; accessed 22 July 2026
[4] RecentBreaches; "CVE-2026-0770: Langflow Inclusion of Functionality from Untrusted Control Sphere Vulnerability; https://recentbreaches.com/vulnerability/CVE-2026-0770; accessed 22 July 2026