

CVE-2026-55255

Langflow Authorization Bypass Through User-Controlled Key Vulnerability

CISA KEV since Jul 7, 2026

Actively exploited

Langflow is a tool for building and deploying AI-powered agents and workflows. Prior to 1.9.1, an Insecure Direct Object Reference (IDOR) vulnerability in /api/v1/responses endpoint allows an authenticated attacker to execute any flow belonging to another user by specifying the victim's flow ID in the request. This vulnerability is fixed in 1.9.1.

EVRS 75/₁₀₀ Urgent priority	CVSS V3.1 8.4 High · NVD	EPSS 0.009 58.9th percentile · FIRST	CISA DEADLINE Jul 10, 2026 CISA federal deadline · Overdue by 3 months
---	--	--	--

Signals behind the score

☒ counted in the score ☐ not counted

evidence for 6 of 8 signals

☒ CISA KEV	Listed in the catalog	☐ Vendor exploitation	Confirmed exploitation in the wild
☐ Ransomware	No known ransomware campaign association	☐ KEV recency	Added to CISA KEV within the last year
☒ EPSS	0.009 probability	☐ Pre-patch disclosure	Disclosure status unavailable
☒ CVSS	Base score 8.4	☐ Microsoft Exploitability Index	Not a Microsoft CVE

Remediation

Patch This Cycle Patch or fixed version identified

CISA required action: Apply mitigations in accordance with vendor instructions, ensuring compliance with CISA's BOD 26-04 Prioritizing Security Updates Based on Risk (see URL in Notes) guidance and CISA's "Forensics Triage Requirements" (see URL in Notes). Follow applicable BOD 26-04 guidance for cloud services or discontinue use of the product if mitigations are unavailable. Stakeholders are responsible for evaluating each asset's internet exposure and ensuring adherence to BOD 26-04 patching guidelines.
Basis: CISA KEV required action

Affected and fixed versions

PACKAGE	AFFECTED	FIXED IN	SOURCE
langflow	< 1.9.1	1.9.1	GitHub

Sources

Vendor guidance	github.com/langflow-ai/langflow/commit/2c9f498d664a3c32698b57d7c5e752625291060e	Additional guidance	github.com/langflow-ai/langflow/security/advisories/GHSA-qrpv-q767-xqq2
BOD 26-04	cisa.gov/news-events/directives/bod-26-04-prioritizing-security-updates-based-risk	Forensics Triage Requirements	cisa.gov/news-events/directives/bod-26-04-implementation-guidance-prioritizing-security-updates-based-risk
NVD	nvd.nist.gov/vuln/detail/CVE-2026-55255	CISA KEV	cisa.gov/known-exploited-vulnerabilities-catalog
GitHub advisory	github.com/advisories/GHSA-qrpv-q767-xqq2	ENISA EUVD	euvd.enisa.europa.eu/vulnerability/EUVD-2026-38517
Current data	evulnable.com/vulnerability-management/cve/CVE-2026-55255		

Snapshot at generation time. EPSS can move quickly. A public exploit module is not evidence of active exploitation.