

CVE-2025-34291

Langflow Origin Validation Error Vulnerability

Exigent

CISA KEV since May 21, 2026

Actively exploited

Langflow versions up to and including 1.6.9 contain a chained vulnerability that enables account takeover and remote code execution. An overly permissive CORS configuration (allow_origins="*" with allow_credentials=True) combined with a refresh token cookie configured as SameSite=None allows a malicious webpage to perform cross-origin requests that include credentials and successfully call the refresh endpoint.

EVRS 87 / 100 Immediate priority	CVSS V4.0 9.4 Critical · NVD	EPSS 0.928 99.83rd percentile · FIRST	CISA DEADLINE Jun 4, 2026 CISA federal deadline · Overdue by 5 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	0.928 probability	☐ Pre-patch disclosure	Disclosure status unavailable
☒ CVSS	Base score 9.4	☐ Microsoft Exploitability Index	Not a Microsoft CVE

Remediation

Out-of-band / urgent Patch or fixed version identified

CISA required action: Apply mitigations per vendor instructions, follow applicable BOD 22-01 guidance for cloud services, or discontinue use of the product if mitigations are unavailable. **CISA note:** This vulnerability could affect an open-source component, third-party library, protocol, or proprietary implementation that could be used by different products.

Basis: CISA KEV required action

An attacker-controlled origin can therefore obtain fresh access_token / refresh_token pairs for a victim session. Obtained tokens permit access to authenticated endpoints — including built-in code-execution functionality — allowing the attacker to execute arbitrary code and achieve full system compromise.

Affected and fixed versions

PACKAGE	AFFECTED	FIXED IN	SOURCE
langflow	≤ 1.6.9	1.7.0	GitHub

Sources

Vendor guidance	github.com/advisories/GHSA-577h-p2hh-v4mv	github.com	github.com/langflow-ai/langflow
github.com	github.com/langflow-ai/langflow/releases/tag/v1.9.3	github.com	github.com/langflow-ai/langflow/issues/11465#event-25774545848
NVD	nvd.nist.gov/vuln/detail/CVE-2025-34291	CISA KEV	cisa.gov/known-exploited-vulnerabilities-catalog
ENISA EUVD	euvd.enisa.europa.eu/vulnerability/EUVD-2025-201507	Current data	evulnable.com/vulnerability-management/cve/CVE-2025-34291

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