Server-Side Request Forgery (SSRF) in Langflow URL Component

MITRE | NVD | CVE.ORG | JSON API | Print: PDF

Summary

CVE	CVE-2026-3340
State	PUBLISHED
Assigner	ibm
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-04-30 21:16:32 UTC
Updated	2026-04-30 21:16:32 UTC
Description	IBM Langflow Desktop 1.0.0 through 1.8.4 IBM Langflow is vulnerable to server-side request forgery (SSRF). This may allo

Risk And Classification

Primary CVSS: v3.1 6.5 MEDIUM from psirt@us.ibm.com

CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:N

Problem Types: CWE-918 | CWE-918 CWE-918 Server-Side Request Forgery (SSRF)

Version	Source	Type	Score	Severity	Vector
3.1	psirt@us.ibm.com	Primary	6.5	MEDIUM	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:N
3.1	CNA	CVSS	6.5	MEDIUM	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:N

CVSS v3.1 Breakdown

Attack Vector
Network

Attack Complexity
Low

Privileges Required
None

User Interaction
None

Scope
Unchanged

Confidentiality
Low

Integrity
Low

Availability

None

CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:N

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	IBM	Langflow Desktop	affected 1.0.0 1.8.4 semver	Not specified

References

Reference	Source	Link	Tags
www.ibm.com/support/pages/node/7271096	psirt@us.ibm.com	www.ibm.com	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analysis

No vendor comments have been submitted for this CVE.

Additional Advisory Data

Solutions

CNA: IBM recommends addressing the vulnerability now by upgrading to IBM Langflow Desktop 1.9.0 or newer https://www.langflow.org/blog/langflow-1-8-desktop If you are already using Langflow Desktop, upgrade in the application to version 1.9.0 To install Langflow Desktop for the first time, visit Download Langflow Desktop https://langflow.org/desktop .

There are currently no legacy QID mappings associated with this CVE.