



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

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF](#)

## Summary

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

## 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	<a href="http://www.ibm.com">www.ibm.com</a>	
CVE Program record	CVE.ORG	<a href="http://www.cve.org">www.cve.org</a>	canonical
NVD vulnerability detail	NVD	<a href="http://nvd.nist.gov">nvd.nist.gov</a>	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.

© CVE.report 2026 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](https://www.mitre.org) and the authoritative source of CVE content is [MITRE's CVE web site](https://www.mitre.org/cve). This site includes MITRE data granted under the following [license](https://www.mitre.org/licenses).

Free CVE JSON API [cve.report/api](https://cve.report/api)

CVE.report and Source URL Uptime Status [status.cve.report](https://status.cve.report)