



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

## Security Bulletin

### Summary

IBM Langflow Desktop contains a Server-Side Request Forgery (SSRF) vulnerability in the URL data source component where user-supplied URLs are insufficiently validated before being used in backend HTTP requests, allowing authenticated attackers to force the Langflow server to make arbitrary requests to internal or restricted network resources such as localhost services, private IP ranges, and cloud metadata endpoints; this flaw enables unauthorized access to sensitive internal systems and data by relaying retrieved responses back through the Langflow execution flow.

### Vulnerability Details

**CVEID:** [CVE-2026-3340](https://www.cve.org/CVERecord?id=CVE-2026-3340) (<https://www.cve.org/CVERecord?id=CVE-2026-3340>)

**DESCRIPTION:** IBM Langflow is vulnerable to server-side request forgery (SSRF). This may allow an authenticated attacker to send unauthorized requests from the system, potentially leading to network enumeration or facilitating other attacks.

**CWE:** [CWE-918: Server-Side Request Forgery \(SSRF\)](https://cwe.mitre.org/data/definitions/918.html) (<https://cwe.mitre.org/data/definitions/918.html>)

**CVSS Source:** IBM

**CVSS Base score:** 6.5

**CVSS Vector:** (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:N)

### Affected Products and Versions

Affected Product(s)	Version(s)
IBM Langflow Desktop	1.0.0 - 1.8.4

### Remediation/Fixes

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> (<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) (<https://langflow.org/desktop>).

### Workarounds and Mitigations

None

## Get Notified about Future Security Bulletins

 Subscribe to [My Notifications](https://www.ibm.com/support/pages/node/718119) (<https://www.ibm.com/support/pages/node/718119>) to be notified of important product support alerts like this.

## References

[Complete CVSS v3 Guide](#) 

[On-line Calculator v3](#) 

## Related Information

[IBM Secure Engineering Web Portal](http://www.ibm.com/security/secure-engineering/bulletins.html) (<http://www.ibm.com/security/secure-engineering/bulletins.html>)

[IBM Product Security Incident Response Blog](http://www.ibm.com/blogs/psirt) (<http://www.ibm.com/blogs/psirt>)

## Acknowledgement

## Change History

28 Apr 2026: Initial Publication

\*The CVSS Environment Score is customer environment specific and will ultimately impact the Overall CVSS Score. Customers can evaluate the impact of this vulnerability in their environments by accessing the links in the Reference section of this Security Bulletin.

## Disclaimer

According to the Forum of Incident Response and Security Teams (FIRST), the Common Vulnerability Scoring System (CVSS) is an "industry open standard designed to convey vulnerability severity and help to determine urgency and priority of response." IBM PROVIDES THE CVSS SCORES ""AS IS"" WITHOUT WARRANTY OF ANY KIND, INCLUDING THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. CUSTOMERS ARE RESPONSIBLE FOR ASSESSING THE IMPACT OF ANY ACTUAL OR POTENTIAL SECURITY VULNERABILITY. In addition to other efforts to address potential vulnerabilities, IBM periodically updates the record of components contained in our product offerings. As part of that effort, if IBM identifies previously unidentified packages in a product/service inventory, we address relevant vulnerabilities regardless of CVE date. Inclusion of an older CVEID does not demonstrate that the referenced product has been used by IBM since that date, nor that IBM was aware of a vulnerability as of that date. We are making clients aware of relevant vulnerabilities as we become aware of them. "Affected Products and Versions" referenced in IBM Security Bulletins are intended to be only products and versions that are supported by IBM and have not passed their end-of-support or warranty date. Thus, failure to reference unsupported or extended-support products and versions in this Security Bulletin does not constitute a determination by IBM that they are unaffected by the vulnerability. Reference to one or more unsupported versions in this Security Bulletin shall not create an obligation for IBM to provide fixes for any unsupported or extended-support products or versions.

## Document Information

**More support for:**

IBM Langflow Desktop

**Software version:**

1.0.0 - 1.8.4

**Operating system(s):**

Windows, Mac OS

**Document number:**

7271096

**Modified date:**

28 April 2026

**Initial Publish date:**

28 April 2026