Security Bulletin: Stored Cross-Site Scripting (XSS) in Langflow Markdown Rendering via rehypeRaw

Security Bulletin

Summary

A stored cross-site scripting (XSS) vulnerability in Langflow allows attackers to inject and execute arbitrary HTML/JavaScript through the Playground event-streaming and Markdown rendering pipeline due to unsafe use of rehypeRaw without sanitization, potentially leading to session theft, account takeover, and further exploitation depending on user privileges.

Vulnerability Details

CVEID: CVE-2026-3346 *(https://www.cve.org/CVERecord?id=CVE-2026-3346)*

DESCRIPTION: Lanflow is vulnerable to stored cross-site scripting. This vulnerability allows an authenticated user to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session.

CWE: CWE-89: Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') *(https://cwe.mitre.org/data/definitions/89.html)*

CVSS Source: IBM

CVSS Base score: 6.4

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

Affected Products and Versions

Affected Product(s)	Version(s)
IBM Langflow Desktop	1.6.0 - 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)*.

Workarounds and Mitigations

None

Get Notified about Future Security Bulletins

Subscribe to My Notifications *(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)*

IBM Product Security Incident Response Blog *(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

Document Information

More support for:

IBM Langflow Desktop

Software version:

1.6.0 - 1.8.4

Operating system(s):

Mac OS, Windows

Document number:

7271095

Modified date:

28 April 2026

Initial Publish date:

28 April 2026