



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

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

Summary

| | |
|------------------------|---|
| CVE | CVE-2026-3346 |
| 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 1.6.0 through 1.8.4 Lanflow is vulnerable to stored cross-site scripting. This vulnerability allows an a |

Risk And Classification

Primary CVSS: v3.1 6.4 MEDIUM from psirt@us.ibm.com

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

Problem Types: CWE-89 | CWE-89 CWE-89 Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')

| Version | Source | Type | Score | Severity | Vector |
|---------|------------------|---------|-------|----------|--|
| 3.1 | psirt@us.ibm.com | Primary | 6.4 | MEDIUM | CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:L/I:L/A:N |
| 3.1 | CNA | CVSS | 6.4 | MEDIUM | CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:L/I:L/A:N |

CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

Low

User Interaction

None

Scope

Changed

Confidentiality

Low

Integrity

Severity: **Low**

Availability: **None**

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

Vendor Declared Affected Products

| Source | Vendor | Product | Version | Platforms |
|--------|--------|------------------|-----------------------------|---------------|
| CNA | IBM | Langflow Desktop | affected 1.6.0 1.8.4 semver | Not specified |

References

| Reference | Source | Link | Tags |
|--|------------------|--|---------------------|
| www.ibm.com/support/pages/node/7271095 | 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 1.9.0To install Langflow Desktop for the first time, visit [Download Langflow 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](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

Free CVE JSON API cve.report/api

CVE.report and Source URL Uptime Status status.cve.report