



# IBM Langflow Desktop FAISS Vector Store Remote Code Execution via malicious Pickle file

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

## Summary

<b>CVE</b>	CVE-2026-3357
<b>State</b>	PUBLISHED
<b>Assigner</b>	ibm
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2026-04-08 01:16:41 UTC
<b>Updated</b>	2026-04-14 21:28:34 UTC
<b>Description</b>	IBM Langflow Desktop 1.6.0 through 1.8.2 Langflow could allow an authenticated user to execute arbitrary code on the system

## Risk And Classification

**Primary CVSS:** v3.1 8.8 HIGH from psirt@us.ibm.com

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

**EPSS:** 0.002610000 probability, percentile 0.495070000 (date 2026-04-15)

**Problem Types:** CWE-502 | CWE-502 CWE-502 Deserialization of Untrusted Data

Version	Source	Type	Score	Severity	Vector
3.1	psirt@us.ibm.com	Primary	8.8	HIGH	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H
3.1	CNA	CVSS	8.8	HIGH	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

## CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

Low

User Interaction

None

Scope

Unchanged

Confidentiality

High

Integrity

High

Availability

High

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

#### NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Langflow	Langflow	All	All	All	All

#### Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	IBM	Langflow Desktop	affected 1.6.0 1.8.2 semver	Not specified

#### References

Reference	Source	Link	Tags
www.ibm.com/support/pages/node/7268428	psirt@us.ibm.com	<a href="http://www.ibm.com">www.ibm.com</a>	Vendor Advisory
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

#### Vendor Comments And Credit

##### Discovery Credit

**CNA:** This vulnerability was reported to IBM by Weblover. (en)

#### Additional Advisory Data

##### Solutions

**CNA:** IBM recommends addressing the vulnerability now by upgrading to IBM Langflow Desktop 1.8.3 or newer <https://www.langflow.org/blog/langflow-1-8-desktop> If you are already using Langflow Desktop, upgrade in the application to version 1.8.3 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](#) 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](https://cve.report/api)

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