Security Bulletin: IBM Langflow Desktop FAISS Vector Store Remote Code Execution via malicious Pickle file

Security Bulletin

Summary

IBM Langflow Desktop supports retrieval-augmented generation (RAG) workflows through its FAISS Vector Store component, which loads persisted vector indexes and associated metadata from disk. A vulnerability in the FAISS component arises from unsafe deserialization of Python Pickle files, where dangerous deserialization is enabled by default and untrusted data is loaded without restriction. An authenticated attacker could exploit this vulnerability by uploading a specially crafted Pickle file and configuring the component to load it, leading to arbitrary code execution with the privileges of the backend service and resulting in a remote code execution condition in IBM Langflow Desktop.

Vulnerability Details

CVEID: CVE-2026-3357 *(https://www.cve.org/CVERecord?id=CVE-2026-3357)*

DESCRIPTION: Langflow could allow an authenticated user to execute arbitrary code on the system, caused by an insecure default setting which permits the deserialization of untrusted data in the FAISS component.

CWE: CWE-502: Deserialization of Untrusted Data *(https://cwe.mitre.org/data/definitions/502.html)*

CVSS Source: IBM

CVSS Base score: 8.8

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

Affected Products and Versions

Affected Product(s)	Version(s)
IBM Langflow Desktop	1.6.0 - 1.8.2

Remediation/Fixes

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 *(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)*.

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

This vulnerability was reported to IBM by Weblover.

Change History

02 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:
1.6.0 - 1.8.2

Operating system(s):
Windows, Mac OS

Document number:
7268428

Modified date:
03 April 2026

Initial Publish date:
02 April 2026