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

MITRE | NVD | CVE.ORG | JSON API | Print: PDF

Summary

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

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

ntegrity

High

vailability

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	www.ibm.com	Vendor Advisory
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	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.

Free CVE JSON API cve.report/api

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