Langflow - Stored XSS via Malicious SVG Upload

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2026-5026
State	PUBLISHED
Assigner	tenable
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-03-27 15:17:04 UTC
Updated	2026-03-30 13:26:29 UTC
Description	The '/api/v1/files/images/{flow_id}/{file_name}' endpoint serves SVG files with the 'image/svg+xml' content type without sani

Risk And Classification

Primary CVSS: v4.0 7 HIGH from vulnreport@tenable.com

CVSS:4.0/AV:N/AC:L/AT:N/PR:L/UI:P/VC:H/VI:L/VA:N/SC:N/SI:N/SA:N/E:X/CR:X/IR:X/AR:X/MAV:X/MAC:X/MAT:X/MPR:X/MUI:X/MVC:X/MVI:X/MVA:X/MSC:X/MSI:X/MSA:X/S:X/AU:X/R:X/V:X/RE:X/U:X

EPSS: 0.000720000 probability, percentile 0.220630000 (date 2026-04-04)

Problem Types: CWE-79 | CWE-79 CWE-79 Improper neutralization of input during web page generation ('cross-site scripting')

Version	Source	Type	Score	Severity	Vector
4.0	vulnreport@tenable.com	Secondary	7	HIGH	CVSS:4.0/AV:N/AC:L/AT:N/PR:L/UI:P/VC:H/VI:L/VA:N/SC:N/SI:N/SA:N/I
4.0	CNA	CVSS	7	HIGH	CVSS:4.0/AV:N/AC:L/AT:N/PR:L/UI:P/VC:H/VI:L/VA:N/SC:N/SI:N/SA:N

CVSS v4.0 Breakdown

Attack Vector

Network

Attack Complexity

Low

Attack Requirements

None

Privileges Required

Low

User Interaction

Passive

Confidentiality

High

ntegrity

Low

Availability

None

Sub Conf.

None

Sub Integrity

None

Sub Availability

None

CVSS:4.0/AV:N/AC:L/AT:N/PR:L/UI:P/VC:H/VI:L/VA:N/SC:N/SI:N/SA:N/E:X/CR:X/IR:X/AR:X/MAV:X/MAC:X/MAT:X/MPR:X/MUI:X/MVC:X/MVI:X/MVA:X/MSC:X/MSI:X/MSA:X/S:X/AU:X/R:X/V:X/RE:X/U:X

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Langflow-ai	Langflow	affected custom	Not specified

References

Reference	Source	Link	Tags
www.tenable.com/security/research/tra-2026-25	vulnreport@tenable.com	www.tenable.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.

There are currently no legacy QID mappings associated with this CVE.