NEW CRITICAL VULNERABILITY ADVISORY: CVE-2026-68771

Summary

CVE-2026-68771 is a newly disclosed Critical vulnerability. It is not yet on CISA's actively-exploited list; treat it as proactive patching before it is weaponised. ComfyUI v0.23.0 contains an unsafe deserialization vulnerability in the LoadTrainingDataset node that allows unauthenticated remote attackers to execute arbitrary Python code by uploading a crafted pickle file and triggering its deserialization. Attackers can upload a malicious shard_*.pkl file via the unauthenticated POST /upload/image endpoint and then queue a workflow graph via POST /prompt referencing the uploaded file, causing torch.load to deserialize the attacker-controlled pickle payload using **reduce** and execute arbitrary commands as the ComfyUI process user.

What we know

- **CVE:** CVE-2026-68771
- **Status:** Newly disclosed, not yet known-exploited (not on CISA KEV)
- **Severity:** CVSS 9.8 Critical, Network-exploitable, no privileges required, no user interaction (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H)
- **Exploitation likelihood (EPSS):** 1%

Recommended action

Patch as a fix becomes available, prioritised by the exposure and EPSS above. Until then, restrict network access to the affected service now (segment it, put it behind a VPN, or take it offline) until you can patch. This does not yet trigger CRA 24-hour reporting, which requires active exploitation, but patching ahead of exploitation is the whole point.

Sources: NIST NVD. Public data; an advisory of a newly disclosed vulnerability, not an incident report. Verify applicability to your estate before acting.