NEW CRITICAL VULNERABILITY ADVISORY: CVE-2026-73032

Summary

CVE-2026-73032 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. PapersGPT for Zotero 0.6.1 contains a remote code execution vulnerability that allows attackers to execute arbitrary JavaScript by returning malicious code from an LLM endpoint that is passed unsanitized to window.eval() in views.ts. Attackers can exploit this through prompt injection in PDFs, MITM interception of API requests, or a malicious custom LLM endpoint to execute arbitrary code in Zotero's chrome-privileged context, enabling file read/write, process execution, and access to all Zotero data.

What we know

- **CVE:** CVE-2026-73032
- **Status:** Newly disclosed, not yet known-exploited (not on CISA KEV)
- **Severity:** CVSS 9.6 Critical, Network-exploitable, no privileges required (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:H/I:H/A:H)
- **Exploitation likelihood (EPSS):** 0%

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.