NEW CRITICAL VULNERABILITY ADVISORY: CVE-2026-39932

Summary

CVE-2026-39932 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. OpenEMR through 8.2.0 contains a remote code execution vulnerability in the document category tree component (library/classes/Tree.class.php) that allows authenticated administrators to execute arbitrary operating system commands by injecting PHP payloads into the categories database table. Attackers can chain arbitrary SQL execution to alter the id column type to VARCHAR and insert a malicious PHP payload, which is then executed via an unsanitized eval() call whenever any page instantiates CategoryTree, including unauthenticated and low-privilege pages, resulting in command execution as the web server user.

What we know

- **CVE:** CVE-2026-39932
- **Status:** Newly disclosed, not yet known-exploited (not on CISA KEV)
- **Severity:** CVSS 9.1 Critical, Network-exploitable, no user interaction (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:C/C:H/I:H/A:H)

Recommended action

Patch as a fix becomes available, prioritised by the exposure and EPSS above. Until then, limit network exposure of the affected service and tighten access until patched. 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.