

NEW CRITICAL VULNERABILITY ADVISORY: CVE-2026-73532

Summary

CVE-2026-73532 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. Fluent Forms Pro 6.2.7 contains an embedded malicious code vulnerability introduced via a tampered plugin build served through a decommissioned update server. The tampered build introduced a rogue PHP file (libs/class-license-sync.php), loaded via a `require_once` directive added to `fluentformpro.php`, that established a backdoor REST API endpoint, dropped persistent PHP files in `mu-plugins` and `uploads` directories, installed a passwordless administrator account, and registered scheduled tasks that survived plugin removal.

What we know

- **CVE:** CVE-2026-73532
- **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)

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.