NEW CRITICAL VULNERABILITY ADVISORY: CVE-2026-14526

Summary

CVE-2026-14526 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. The AI Copilot – Content Generator plugin for WordPress is vulnerable to authorization bypass in all versions up to, and including, 1.5.6. This is due to the plugin not properly verifying that a user is authorized to perform an action. This makes it possible for unauthenticated attackers to create a new administrator-level user account and achieve full site takeover by saving and executing a malicious workflow containing a wp_create_user action node specifying role=administrator. This vulnerability is exploitable by unauthenticated attackers on any site where the [aiwu-form] shortcode or public chatbot is rendered on a frontend page, as the waic-nonce value is emitted into publicly accessible JavaScript (WAIC_DATA.waicNonce) on those pages, rendering the nonce check a non-functional authorization barrier.

What we know

- **CVE:** CVE-2026-14526
- **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.