NEW CRITICAL VULNERABILITY ADVISORY: CVE-2026-8457

Summary

CVE-2026-8457 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 WooCommerce - Social Login plugin for WordPress is vulnerable to Authentication Bypass in all versions up to and including 2.8.7. This is due to the plugin's Apple login handler accepting the Apple id_token and decoding only its base64 payload without verifying the JWT signature against Apple's public keys or validating the issuer, audience, or expiry claims, combined with the security nonce required to invoke the login flow being publicly exposed to unauthenticated users via a localized JavaScript object on the login page. This makes it possible for unauthenticated attackers to log in as any existing WordPress user — including administrators — by supplying a forged id_token whose payload contains the target user's email address, as that email is used without any role exclusion to resolve a WordPress account and immediately issue an authenticated session for it.

What we know

- **CVE:** CVE-2026-8457
- **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):** 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.