NEW CRITICAL VULNERABILITY ADVISORY: CVE-2026-15964

Summary

CVE-2026-15964 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 Single Sign On For TNG plugin for WordPress is vulnerable to Authentication Bypass via unauthenticated password reset in all versions up to, and including, 2.0.0. This is due to the `ssoprocess_ajax()` function — registered on `wp_ajax_nopriv_ssoprocess_ajax` and therefore reachable without authentication — accepting an attacker-supplied `email` parameter with the `setnewpassword` operation and calling `reset_password()` on the resolved account without any ownership token, email confirmation link, or capability check. The sole guard is a call to `check_ajax_referer()`, which provides no authorization barrier because the `ssoajaxnonce` nonce is publicly broadcast on every front-end page via `wp_localize_script()` into the `SSOPWDREQUIREMENT` JavaScript object; since WordPress computes nonces for logged-out visitors against a shared anonymous session context, any unauthenticated visitor can scrape a valid nonce from the homepage and use it to authenticate the request. This makes it possible for unauthenticated attackers to change the password of any WordPress account, including administrator accounts, enabling complete site takeover.

What we know

- **CVE:** CVE-2026-15964
- **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.