NEW CRITICAL VULNERABILITY ADVISORY: CVE-2026-64827

Summary

CVE-2026-64827 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. Telenia Software TVox 26.5.3 and prior 26.x versions, and 24.9.21 and prior 24.x versions, contain an authentication bypass vulnerability in set_env.php where the redirectToLoginAdminIRequestHaveAccessToken() function derives the current page name from PHP_SELF and skips authentication when the value matches 'login_admin.php'. Attackers can append '/login_admin.php' to the path of any target PHP script to cause the authentication check to pass and gain unauthenticated access to all PHP scripts under the manager HTML directory.

What we know

- **CVE:** CVE-2026-64827
- **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.