

NEW CRITICAL VULNERABILITY ADVISORY: CVE-2026-41452

Summary

CVE-2026-41452 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. Krayin CRM 2.2.4 contains a missing authentication vulnerability in the installer middleware that allows unauthenticated remote attackers to overwrite the primary administrator account by sending a crafted HTTP POST request with the X-Requested-With: XMLHttpRequest header to bypass the CanInstall middleware redirect check. Attackers can supply arbitrary name, email, and password values to the admin-config-setup endpoint, which performs an unauthenticated updateOrCreate targeting the hardcoded administrator user ID, enabling full administrative access to all CRM data.

What we know

- **CVE:** CVE-2026-41452
- **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.