CISA flags Drupal Core installer flaw (CVE-2026-136716) that allows remote site takeover



CISA lists CVE-2026-136716, a Drupal Core flaw that lets an unauthenticated remote attacker take over a site through the exposed installer when the installation is in an unusual or incomplete state.

- The flaw is an improper check for unusual or exceptional conditions in Drupal Core.
- An unauthenticated remote attacker can take over a site through the exposed Drupal installer.
- It applies only when a site is in one of the affected unusual or incomplete installation states.
- CISA requires mitigations per vendor instructions, under BOD 26-04 and its Forensics Triage Requirements.
- The federal due date is 2026-11-30.

CISA has listed CVE-2026-136716, a vulnerability in Drupal Core described as an improper check for unusual or exceptional conditions. According to the entry, an unauthenticated remote attacker can take over a site through the Drupal installer when it is exposed and the site is in one of the affected unusual or incomplete installation states.

What the advisory says

The issue is tied to the installer rather than to normal site operation. The conditions that make a site vulnerable are specific installation states, which the source describes only in general terms. The consequence, however, is full site takeover without any credentials.

CISA's required action is to apply mitigations in line with the vendor's instructions, while following its BOD 26-04 guidance on prioritizing security updates based on risk and its Forensics Triage Requirements. Where cloud services are involved, the applicable BOD 26-04 guidance should be followed. If mitigations are not available, the product should no longer be used. The federal due date is 2026-11-30, and each stakeholder is responsible for assessing the internet exposure of its own assets.

What this means for Saudi institutions

BOD 26-04 binds US federal agencies, not Saudi entities, but the logic is a sound benchmark. Institutions running Drupal for public portals, customer sites or intranets should confirm whether any instance is internet-facing and whether its installer remains reachable or an installation was left unfinished. Start with the vendor's guidance, and treat any site that could have been exposed as a candidate for a forensic check.

What to do now

1. Inventory all Drupal Core instances and identify which are internet-facing.
2. Check for sites with incomplete or unusual installation states and confirm the installer is not reachable externally.
3. Apply the vendor's mitigations for CVE-2026-136716 as soon as possible.
4. Review affected sites for signs of compromise, using a forensic triage approach such as the one CISA describes.
5. If mitigations are unavailable for a site, restrict or retire it until a fix exists.
6. Record the work in your vulnerability management process for ECC-aligned reporting.