Drupal Core CVE-2026-132165: Installer Flaw Could Allow Site Takeover or Code Execution



CISA lists CVE-2026-132165, a Drupal Core flaw that lets an unauthenticated attacker abuse install.php under specific conditions to take over a site or run arbitrary code. Apply vendor mitigations.

- CVE-2026-132165 affects Drupal Core and is described as a failure to fail securely.
- An unauthenticated attacker could take over an existing site or execute arbitrary code through the Drupal installer.
- Under specific conditions, the attacker can use install.php to attempt to reinstall Drupal on the site.
- CISA requires mitigations per vendor instructions, BOD 26-04 and its Forensics Triage Requirements; the federal due date is 2026-11-27.
- If mitigations are unavailable, CISA says to discontinue use of the product.

CISA has added CVE-2026-132165 to its catalogue of vulnerabilities. It concerns Drupal Core and is described as a failure to fail securely in the Drupal installer.

What the flaw allows

According to the entry, an unauthenticated attacker could take over an existing site or execute arbitrary code. Under specific conditions, the attacker can use install.php to attempt to reinstall Drupal on a site that is already running. The source does not state which versions are affected or what the specific conditions are, so organisations should consult the vendor's instructions for those details.

What CISA requires

CISA's required action is to apply mitigations in line with vendor instructions, while following its BOD 26-04 guidance on prioritising security updates based on risk and its Forensics Triage Requirements. For cloud services, the applicable BOD 26-04 guidance should be followed. Where mitigations are not available, CISA says use of the product should be discontinued. Stakeholders are responsible for assessing the internet exposure of each asset. The federal due date is 2026-11-27; this date binds US federal agencies, but it is a useful reference for planning.

Practical reading for Saudi institutions

Institutions running Drupal on public websites, portals or customer-facing services should treat this as a prompt to confirm exposure and apply the vendor's mitigations without waiting for the reference date.

What to do now

1. Inventory all Drupal Core instances, including test and forgotten sites, and record which are internet-facing.
2. Apply the vendor's mitigations for CVE-2026-132165 as instructed.
3. Check whether install.php is reachable from the internet on each instance and restrict access in line with vendor guidance.
4. Review web server and application logs for unexpected requests to the installer and for signs of unauthorised reinstallation or changes.
5. If mitigations are unavailable for an asset, plan to take it out of service as CISA advises.
6. Record the exposure assessment and remediation under your vulnerability management process.