Drupal core flaw CVE-2026-132165 exploited in the wild; patches available



A patched Drupal core flaw, CVE-2026-132165, allows remote code execution via the installer and is being exploited. CISA added it to its KEV catalog. Fixed versions exist; end-of-life branches get no patch.

- CVE-2026-132165 affects the installer shipped with Drupal core and can lead to site hijack or remote code execution by an unauthenticated attacker under certain conditions.
- The flaw was patched on November 18; Drupal reports exploitation on live sites as early as November 19.
- Fixed versions are Drupal 11.4.13, 11.3.22 and 10.6.22; end-of-life branches will not receive a fix.
- CISA added the flaw to its KEV catalog on November 24, and Drupal raised its rating to highly critical.

> - Some exploit paths are mitigated if the web server cannot write to or change permissions on settings.php.

A recently patched vulnerability in Drupal core, tracked as CVE-2026-132165, is being exploited in the wild, according to CISA and the Drupal developers. The flaw can lead to remote code execution.

What happened

The issue sits in the installer that ships with Drupal core and is used to set up a new site. Under certain conditions, an unauthenticated attacker can abuse it to reinstall Drupal, which may allow them to hijack the website or run arbitrary code.

The fix was released on November 18. Drupal's Security Team says it received a report of exploitation on live sites as early as 19:00 UTC on November 19, and it then raised the rating to highly critical. CISA added the flaw to its Known Exploited Vulnerabilities catalog on November 24. The discovery is credited to Anthropic's OSS Scanner, a free opt-in service that scans enrolled open source projects.

No public details on the attacks appear to be available, and it is unclear how many sites are affected.

Who should act

Any organisation running Drupal 10 or 11 should treat this as urgent. Patches are in Drupal 11.4.13, 11.3.22 and 10.6.22. End-of-life branches will not be fixed, so sites on them need migration or compensating controls.

Drupal notes that some, but not all, exploit paths are mitigated when the web server cannot write to or change permissions on settings.php. It recommends upgrading and also securing the installer after installation.

This is the third Drupal vulnerability reported as exploited this year, following a Commerce Core access bypass flaw in October and another flaw in May.

What to do now

1. Inventory all Drupal sites, including internet-facing and third-party-hosted ones, and record their versions.
2. Upgrade to Drupal 11.4.13, 11.3.22 or 10.6.22 as applicable, prioritising public-facing sites.
3. Plan migration or compensating controls for sites on end-of-life Drupal branches, which will not be patched.
4. Secure the installer after installation and prevent the web server from writing to or changing permissions on settings.php.
5. Review web server and application logs since November 18 for unexpected reinstall activity or changes, and escalate through incident response if found.