Critical Drupal flaw CVE-2026-132165 now exploited to take over sites



Drupal confirmed active exploitation of CVE-2026-132165, a critical flaw in the core installer that allows site takeover or remote code execution. CISA added it to its KEV Catalog. Upgrade, or block the installer file.

- CVE-2026-132165 lets anonymous users abuse the Drupal installer to take over a site or achieve remote code execution.
- Drupal says exploitation on live sites began as early as 2026-11-19 19:00 UTC.
- The fix is to upgrade to the latest Drupal version; Drupal Steward WAF customers are protected from known attack vectors.
- If upgrading is not possible, block access to /core/install.php in the web server configuration or .htaccess.

> - CISA added the flaw to its KEV Catalog and set a remediation deadline of November 27 for US federal agencies.

The Drupal security team has confirmed that a critical vulnerability in Drupal core is being exploited against unpatched sites. The flaw, tracked as CVE-2026-132165, was found by Anthropic's OSS Scanner.

What is affected

Drupal core includes an install.php file used to install the CMS. Under specific conditions, an attacker can use it to attempt a reinstallation, which can lead to site takeover or remote code execution. No authentication is needed. Drupal notes that some exploit paths are mitigated when the web server cannot write to or change permissions on settings.php.

The advisory was not initially marked as exploited, but Drupal later updated it to say attacks on live sites occurred as early as 2026-11-19 19:00 UTC. On Tuesday, CISA added the flaw to its Known Exploited Vulnerabilities (KEV) Catalog and required US federal agencies to remediate by Friday, November 27. CISA also encouraged all organizations to prioritise KEV-listed flaws within a risk-based vulnerability management approach.

Protection options

The primary remedy is to upgrade to the latest available Drupal version. Sites behind the paid Drupal Steward WAF service are protected from known attack vectors, though Drupal still advises upgrading in case other vectors emerge. Where an immediate upgrade is not possible, block access to /core/install.php in the web server configuration or in the .htaccess file in the web root.

Why it matters

Drupal is widely used by government bodies, universities, enterprises and media organisations. CISA has flagged five Drupal vulnerabilities as exploited since November 2021, two of them also used by ransomware groups. Institutions running public Drupal sites should treat this as an active, time-sensitive exposure.

What to do now

1. Inventory all Drupal sites, including public, intranet and third-party hosted ones, and confirm their versions.
2. Upgrade affected sites to the latest Drupal version as a priority.
3. Where upgrading is delayed, block /core/install.php in the web server configuration or .htaccess.
4. Check that the web server cannot write to or change permissions on settings.php.
5. Review web logs since 2026-11-19 for requests to the installer and for unexpected changes to site files or configuration.

6. Record the exposure and remediation in your vulnerability management process under NCA ECC and SAMA CSF requirements.