Drupal core installer access bypass allows site takeover (CVE-2026-136716)

Status: Recovering / monitoring

Started Nov 28, 2026, 11:36 AM PST · Drupal's estimate: Fixed versions are available

CVE-2026-136716 · Being exploited: yes · Fix available: yes

WHAT'S HAPPENING

Drupal is a widely used website platform. Its core software includes an installer file (install.php) that is used to set up a new site. On November 18, Drupal fixed a serious installer flaw (CVE-2026-132165, advisory SA-CORE-2026-017). On November 25, Drupal said that some sites in an 'unusual or incomplete install state' could still be taken over by anonymous visitors, including production sites. Drupal says this state is not visible in the admin interface. Sites that are already compromised may no longer look vulnerable. Sites whose installer was already secured are not affected. Drupal rates the issue 'Highly critical' (21 out of 25 on its own scale). We found no CVSS score.

WHO IS AFFECTED

- Drupal core sites where the installer is reachable from the internet and the site is in an unusual or incomplete install state, even if the November 18 update (SA-CORE-2026-017) was applied
- Branches reported as fixed in 10.6.x, 11.3.x and 11.4.x: sites running versions older than 10.6.23, 11.3.23 or 11.4.14 should be treated as exposed. One outlet lists the affected ranges as up to and including those versions, so confirm the exact ranges in Drupal's advisory.
- Older, end-of-life Drupal branches: no fix is reported for them, so blocking the installer is the only protection

IS IT BEING EXPLOITED?

Drupal's security team says in its advisory SA-CORE-2026-019 (published November 25, 2026) that this is being exploited in the wild. Reports differ on when attacks began. One outlet says November 19, but other coverage says the start date is not stated, so we treat it as unconfirmed. We did not find it in CISA's Known Exploited Vulnerabilities list at the time of writing (one outlet reported it was not listed). We did not open CISA's catalog ourselves, so please check it directly.

WHAT YOU SHOULD DO NOW

Home users

- If you only visit Drupal-based websites, you do not need to do anything. The fix has to be applied by the site's owner or host.
- If you run your own Drupal site (for example a hobby or club site), update it now to the fixed version and run the database update step (update.php, or 'drush updb').
- Ask your web host or developer whether the site has been updated and whether access to /core/install.php is blocked.
- If your site might have been exposed, change all administrator passwords and look for unknown admin accounts.

Businesses

- Update Drupal core to 10.6.23, 11.3.23 or 11.4.14 (or later), then run the database update (update.php or drush updb). Drupal says the update includes a step that marks the installation as finished.
- Block public access to /core/install.php at the web server, firewall or CDN level. This removes the exposure right away and is the only protection for end-of-life Drupal branches.
- Assume sites that were reachable between November 18 and your update may have been compromised.

Questions? Contact BIS Computer Solutions, Inc.
5500 Alta Canyada Rd., La Canada, CA 91011 USA · Phone: +1-818-248-5023 · Fax: +1-818-249-1169 · Email: support@biscomputer.com · Web: www.biscomputer.com

Check for unknown admin users, unexpected files or code changes, new scheduled tasks and unusual logs for requests to install.php.

- If you find signs of compromise, restore from a clean backup taken before the incident, rotate all passwords, API keys and database credentials, and consider bringing in an incident responder.
- Plan an upgrade for any site on an unsupported Drupal branch.

HOW TO CHECK IF YOU'RE AFFECTED

- Log in to Drupal as an administrator and go to Reports > Status report (/admin/reports/status). The Drupal core version is listed at the top.
- On the command line, run 'drush status' or 'composer show drupal/core' in the site folder.
- Test whether the installer is reachable: visit yoursite.example/core/install.php. A properly protected site should not show an installation screen. If you are unsure, ask your developer.
- Remember that the vulnerable state is not visible in the admin interface, so updating and blocking the file are safer than trying to judge by looking.

FIXED VERSIONS AND WORKAROUNDS

- Drupal 10.6.x: 10.6.23
- Drupal 11.3.x: 11.3.23
- Drupal 11.4.x: 11.4.14

Until you can update:

- Block access to /core/install.php (web server rules, firewall or CDN). Coverage describes this as the only protection for end-of-life branches.
- Run the database update after upgrading so the installation is marked as finished.

OTHER COVERAGE

Drupal Installer Patch Left a Gap Attackers Are Already Exploiting (SecurityWeek) — https://www.securityweek.com/drupal-installer-patch-left-a-gap-attackers-are-already-exploiting/

Drupal Warns of New Critical Flaw Exploited in the Wild (Security Affairs) — https://securityaffairs.com/204085/security/drupal-warns-of-new-critical-flaw-exploited-in-the-wild.html

Drupal Core Access Bypass Allows Site Takeover via the Installer (Kudelski Security) — https://kudelskisecurity.com/research/drupal-core-access-bypass-allows-site-takeover-via-the-installer

ABOUT THIS BRIEF

Last updated November 28, 2026. Researched with AI help from public sources and checked against the official advisories above. Details can change; follow your vendor's guidance.

Questions? Contact BIS Computer Solutions, Inc.

5500 Alta Canyada Rd., La Canada, CA 91011 USA · Phone: +1-818-248-5023 · Fax: +1-818-249-1169 · Email: support@biscomputer.com · Web: www.biscomputer.com