Drupal installer patch left a gap that attackers are now exploiting



Drupal says its earlier installer fix did not protect every site, and CVE-2026-136716 is being exploited to take over sites left in unusual install states. Patched versions are available and a post-upgrade update hook is required.

- CVE-2026-136716 is an access bypass flaw that can lead to site takeover, disclosed on November 25 with a CMSS score of 21/25.
- It follows SA-CORE-2026-017 of November 18, which fixed installer flaw CVE-2026-132165; that earlier flaw was added to CISA's KEV catalog on November 24.
- Sites in unusual or incomplete install states, including production sites, may remain vulnerable, and the user interface does not show this state.
- Fixed versions are 11.4.14, 11.3.23 and 10.6.23; production sites must also run an update hook

after upgrading.

- Drupal has not shared details of the attacks or who is behind them, and advises checking logs for signs of compromise.

Drupal has disclosed that the patch it released on November 18 for an installer vulnerability did not protect every website. A follow-up flaw, CVE-2026-136716, is now being exploited in the wild to compromise sites that remain vulnerable.

What happened

The original fix, published in advisory SA-CORE-2026-017, addressed CVE-2026-132165, a flaw in the installer that ships with Drupal core and is used to set up new sites. Drupal learned of in-the-wild exploitation soon afterwards, and CISA added that vulnerability to its KEV catalog on November 24.

On November 25 Drupal disclosed CVE-2026-136716, an access bypass issue that can lead to site takeover, with a CMSS score of 21/25. According to Drupal, sites in unusual or incomplete install states, including production sites, stayed exposed after the first advisory. The user interface does not indicate whether a site is in that state, and a site that has already been compromised may no longer appear vulnerable.

Who is affected

Sites whose installer had already been secured are not vulnerable. Any site that left its installer remotely accessible after SA-CORE-2026-017 may have been compromised. Drupal has not released details of the attacks, and the actors behind them are unknown.

What to do

Fixes are included in Drupal 11.4.14, 11.3.23 and 10.6.23. Production sites must run an update hook after upgrading to fully close the issue. Because exploitation is already under way, patching alone may not be enough: teams should also review logs for signs of compromise.

What to do now

1. Inventory all Drupal sites, including production, staging and any partially installed instances, and record their versions.
2. Upgrade to 11.4.14, 11.3.23 or 10.6.23 as applicable, and run the update hook on production sites afterwards.
3. Confirm the installer is not remotely accessible on any site, and restrict access to it.
4. Review web server and application logs since November 18 for signs of compromise, and start incident handling if any are found.

5. Treat sites that exposed the installer as possibly compromised even after patching, and verify their integrity.
6. Record the exposure and response in your vulnerability and incident management processes.