Drupal warns of second site-takeover flaw under active exploitation



Drupal says a second critical flaw, CVE-2026-136716, is being exploited to hijack unpatched sites. It covers install states left open after the earlier Fail2Install fix. Admins should upgrade or block the installer.

- CVE-2026-136716 was patched a week after CVE-2026-132165 (Fail2Install), and Drupal confirms it is being exploited in the wild.
- Sites in unusual or incomplete install states stayed vulnerable after SA-CORE-2026-017, including production sites.
- The vulnerable state is not visible in the user interface, and already-compromised sites may no longer show it.
- Fixed versions are Drupal 10.6.23, 11.3.23 and 11.4.14.

> - Where upgrading is not immediate, access to /core/install.php should be blocked.

The Drupal security team has warned that attackers are exploiting a second critical vulnerability that allows them to take over unpatched websites.

What happened

Last week Drupal fixed a remote code execution flaw, CVE-2026-132165, known as Fail2Install, which let anonymous users take over sites by abusing the installer. An update to that advisory later said exploitation began one day after patches were released.

The new issue, CVE-2026-136716, was patched a week afterwards. It addresses attack paths the first fix left open. Drupal states that sites in unusual or incomplete install states, including production sites, remained exposed after SA-CORE-2026-017. The condition is not visible in the user interface, and a site that is already compromised may no longer be in the vulnerable state. Drupal has not yet shared further details of the attacks.

Recommended steps from Drupal

Any site that left its installer remotely reachable may have been compromised. Administrators should confirm that the user 1 email address is one they control and consider resetting it. They should also review logs for unauthorized access, especially unexpected changes to or by the user 1 account, and follow Drupal's guidance if compromise is suspected.

Fixed releases are Drupal 10.6.23, 11.3.23 and 11.4.14. Teams that cannot upgrade immediately should block access to /core/install.php on all new and existing sites, either in the web server configuration or in the .htaccess file in the web root.

Why it matters

Because patching alone may not reveal a prior compromise, institutions running Drupal should pair the upgrade with a review for signs of intrusion.

What to do now

1. Inventory all Drupal sites, including development and staging, and identify those on versions below 10.6.23, 11.3.23 or 11.4.14.
2. Upgrade to a fixed release, or block /core/install.php in the web server configuration or .htaccess until you can.
3. Verify the user 1 email address is controlled by your team and consider resetting it.
4. Review logs for unexpected changes to or by the user 1 account and unauthorized access.

5. If compromise is suspected, follow Drupal's guidance and activate your incident response process, including reporting obligations to your regulator.