Drupal Warns of Actively Exploited, Highly Critical Core Vulnerability



Drupal has disclosed a highly critical flaw in Drupal core, CVE-2026-136716, that it says is being exploited in the wild. It relates to the earlier Fail2Install issue and covers installation states that remained vulnerable.

- Drupal rates the new core flaw as highly critical and reports exploitation in the wild.
- It is tracked as CVE-2026-136716; no CVSS score is given in the source.
- The weakness is described as improper checking for unusual or exceptional conditions.
- It is linked to CVE-2026-132165 (Fail2Install) and addresses installation states that stayed vulnerable.

Drupal has issued a warning about a new security flaw in Drupal core that it classifies as "highly critical".

According to the report, the vulnerability is already being exploited in the wild, and the headline describes it as a site takeover risk.

What is known

The flaw is tracked as **CVE-2026-136716**. The source lists its CVSS score as not available. It is described as a case of improper checking for unusual or exceptional conditions.

The issue is connected to **CVE-2026-132165**, also known as Fail2Install. The new vulnerability addresses installation states that remained vulnerable after that earlier problem. The source does not provide further technical detail, affected version ranges or patch information, so those points should be confirmed directly with Drupal's official advisory.

What to do next

Because exploitation has been reported, organisations that run Drupal should treat this as a priority rather than waiting for a routine maintenance window. The first step is to establish where Drupal is used, including public portals, customer-facing services and any forgotten or test instances. The next is to read the official Drupal security advisory and apply the fixed release it specifies.

Teams should also review whether any installation or setup routines are reachable from the internet, given the link to installation states, and check logs for unusual activity. Findings that suggest compromise should follow the institution's incident response process.

What to do now

1. Inventory all Drupal instances, including public, test and legacy sites.
2. Read the official Drupal advisory for CVE-2026-136716 and apply the specified fixed release as an emergency change.
3. Confirm that installation or setup routines are not reachable from the internet.
4. Review web server and application logs for unusual requests or unexpected changes since the exploitation was reported.
5. Escalate any sign of compromise through the incident response process and notify the relevant regulator where required.