Drupal Core Flaw Fail2Install (CVE-2026-132165) Added to CISA KEV Catalog



CISA has added the critical Drupal core remote code execution flaw CVE-2026-132165, known as Fail2Install (CVSS 9.8), to its KEV catalog. US federal agencies must apply fixes by November 27, 2026.

- CISA added the Drupal flaw to its Known Exploited Vulnerabilities catalog.
- The flaw is tracked as CVE-2026-132165 and nicknamed Fail2Install.
- It carries a CVSS score of 9.8 and allows remote code execution in Drupal core.
- US federal agencies must apply fixes by November 27, 2026.
- The KEV listing indicates the flaw is being actively exploited.

The U.S. Cybersecurity and Infrastructure Security Agency (CISA) has added a critical vulnerability in Drupal to its Known Exploited Vulnerabilities (KEV) catalog. The flaw is tracked as **CVE-2026-132165** and is also referred to as **Fail2Install**.

What is known

The vulnerability is a remote code execution (RCE) issue affecting Drupal core and has a CVSS score of 9.8. Federal agencies in the United States have been required to apply the fixes by November 27, 2026. Inclusion in the KEV catalog reflects that the flaw is under active exploitation, and technical details of the exploit have begun to emerge.

The source excerpt does not list affected versions, patch versions or the exact conditions needed to exploit the flaw, so those should be confirmed from the official Drupal security advisory.

Why it matters for Saudi institutions

Drupal is a common content management platform, and any organisation running it on public-facing sites should treat a core RCE under active exploitation as urgent. Priority should go to internet-exposed instances, including those run by third-party web agencies or hosting providers on the institution's behalf.

A calm, ordered response is best: establish where Drupal is used, confirm the version, apply the vendor fix, and check for signs of compromise on systems that were exposed before patching.

What to do now

1. Inventory all Drupal instances, including those managed by third parties, and record their versions.
2. Check the official Drupal security advisory and apply the fix for CVE-2026-132165 starting with internet-facing sites.
3. Review web server and application logs on exposed instances for unusual activity before patching.
4. Ask web agencies and hosting providers to confirm in writing their patching status.
5. Add CVE-2026-132165 to vulnerability tracking and report remediation status to the CISO.