

Drupal patches critical remote code execution vulnerability exploitable via contributed modules



Drupal released security updates on 14 October addressing a critical remote code execution flaw in the Field UI module, with at least one known exploit path requiring no authentication.

- Drupal released patches on 14 October 2024 for versions 11.4.10, 11.3.19, and 10.6.19 addressing a critical flaw in the Field UI module
- The vulnerability permits remote code execution on the server hosting the Drupal site
- The flaw cannot be exploited through Drupal core alone but requires contributed modules to create exploit paths
- At least one known exploit path exists that does not require attacker authentication
- Multiple exploit paths have been identified through various contributed modules

Vulnerability details

Drupal released security patches on 14 October 2024 to address a critical vulnerability in the **Field UI module**, a component of Drupal core. The flaw enables remote code execution on the server hosting the affected Drupal installation. The patched versions are 11.4.10, 11.3.19, and 10.6.19.

According to the Drupal Security Team advisory, the vulnerability cannot be exploited through Drupal core functionality alone. Instead, attackers must leverage contributed modules—third-party extensions developed by the Drupal community—to create viable exploit paths. The security team confirmed that multiple such paths exist across different contributed modules.

Authentication not required for exploitation

A particularly concerning aspect of this vulnerability is that at least one known exploit path does not require the attacker to authenticate to the system. This significantly lowers the barrier to exploitation and increases the risk profile for public-facing Drupal installations that use vulnerable contributed modules alongside the affected core versions.

The combination of critical severity, remote code execution capability, and unauthenticated access makes this vulnerability a priority for immediate remediation. Organizations running Drupal sites should verify their core version and review installed contributed modules to assess exposure.

Patch availability

Drupal has released fixes across three supported release branches. Organizations should apply the appropriate patch based on their current major version: 11.4.10 for the latest 11.4.x branch, 11.3.19 for the 11.3.x branch, and 10.6.19 for sites still running Drupal 10. The security team has not disclosed specific details about vulnerable contributed modules or exploit techniques to prevent widespread exploitation before patching is complete.

What to do now

1. Identify all Drupal installations across your organisation's web infrastructure and document their current versions
2. Apply security patches immediately to upgrade to Drupal 11.4.10, 11.3.19, or 10.6.19 depending on your current major version
3. Conduct an inventory of all contributed modules installed on each Drupal instance and assess their necessity
4. Review web application firewall rules and intrusion detection signatures to detect potential exploitation attempts targeting Drupal Field UI
5. Monitor Drupal security advisories for updates on vulnerable contributed modules as details become available

6. Schedule penetration testing of public-facing Drupal sites to validate patch effectiveness and identify residual exposure