

SECURITY ADVISORY

Drupal Core Critical RCE and Cross-Site Scripting Flaws

A critical Field UI vulnerability and related browser-script flaws require website owners to review modules and patch Drupal core.

SEVERITY	PUBLISHED	CATEGORY	STATUS
CRITICAL	14 OCT 2026	CMS / APPSEC	PATCH AVAILABLE

Reviewed 23 Oct 2026. Severity and scope details appear below.

Severity: CRITICAL for Field UI RCE · Category: CMS / Application Security · Status: Patch available. Published 14 October 2026; reviewed 23 October 2026. Drupal rates the accompanying XSS issues moderately critical.

URGENT ACTION

Update affected sites and review enabled modules and custom integrations. The critical RCE is not directly exploitable with Drupal core alone: contributed modules or custom code can expose it, including a known unauthenticated path. [1]

01 INCIDENT SUMMARY

Drupal published three core security advisories on 14 October 2026. CVE-2026-108097 concerns remote code execution in Field UI. CVE-2026-108515 concerns XSS in the Link module, while CVE-2026-108514 concerns XSS in Navigation. CERT-In issued a combined critical notice on 22 October. [1-4]

The flaws have different prerequisites and severity ratings. Do not assume every Drupal website permits unauthenticated server compromise. Establish the core version, enabled modules, contributed code and relevant permissions for each site. [1-4]

02 POTENTIAL IMPACT

- Server-side execution: Exposed Field UI functionality can permit arbitrary code execution through affected integrations. [1, 4]
- Browser-side script injection: Insufficient sanitization in Link or Navigation can permit malicious scripts under the relevant module and permission conditions. [2, 3]
- Website integrity and data exposure: Successful exploitation could affect trusted content, application integrity or information accessible to the compromised context. [4]

03 PRIORITY ACTIONS FOR CUSTOMERS

1. Inventory sites and module exposure

Include multisite installations, staging systems, deployment images and managed hosting. Record enabled Field UI, Link and Navigation modules, contributed extensions, custom code and privileged roles.

2. Update to a fixed supported release

Deploy the applicable patched core build below, following Drupal's upgrade process. Test dependencies and application behavior, and verify the code actually serving each site. [1-3]

3. Apply temporary protection if needed

Drupal identifies uninstalling the Field UI module as an interim mitigation for the RCE while updating. Assess operational impact first. This does not replace fixes for Link or Navigation XSS. Drupal Steward covers some known RCE paths, not every possible path. [1]

4. Check for suspicious changes

Review unexpected PHP files, altered content, account or permission changes and unusual application activity. Preserve evidence and activate incident response if compromise is suspected; a successful upgrade alone does not establish that a site was clean.

TECHNICAL & RESPONSE DETAILS

Guidance for infrastructure, development, operations and security teams

04 TECHNICAL INFORMATION

- CVE-2026-108097 / SA-CORE-2026-014: Field UI RCE; Drupal risk 19/25 (Critical). This is Drupal's risk scale, not a CVSS score. [1]
- CVE-2026-108515 / SA-CORE-2026-015: Link-module XSS; risk 13/25 (Moderately critical). [2]
- CVE-2026-108514 / SA-CORE-2026-016: Navigation-module XSS; risk 12/25. Relevant HTML-entry or administer-menu permissions are required. [3]
- Exploitation status: The reviewed advisories describe exploitability but do not confirm active attacks as of 23 October 2026. [1-4]

05 PATCHED VERSIONS AND EXPOSURE

- Drupal 10.6: update to 10.6.19 or later. Drupal 11.3: update to 11.3.19 or later. Drupal 11.4: update to 11.4.10 or later.
- Drupal 12 prereleases: the advisories list fixes in 12.0.0-beta2; use the appropriate supported deployment path.
- Drupal 8/9, 10.5 and older, and 11.2 and older: the cited notices identify these as outside security coverage; migrate to a supported fixed branch. [1-3]

06 VALIDATION CHECKLIST

- Confirm fixed core versions across every live site and deployment image.
- Record module exposure, permissions and any temporary Field UI mitigation.
- Test authentication, content editing, links, menus and custom integrations.
- Document log review, suspicious changes and any provider-led remediation.

ADVISORY BASIS

Independent 443 Labs customer awareness guidance. Publication date follows Drupal's 14 October advisories; sources were reviewed on 23 October 2026. Assess each site's actual exposure. This notice does not establish compromise of any recipient.

PRIMARY SOURCES

[1] [Drupal SA-CORE-2026-014: Field UI RCE - 14 October 2026](#)

[2] [Drupal SA-CORE-2026-015: Link XSS - 14 October 2026](#)

[3] [Drupal SA-CORE-2026-016: Navigation XSS - 14 October 2026](#)

[4] [CERT-In CIVN-2026-0513 - 22 October 2026](#)