Cal OES
GOVERNOR'S OFFICE
OF EMERGENCY SERVICES

Critical Remote Code Execution Vulnerability in Drupal Core Field UI Module

Remote Code Execution	Contributed Module Paths	One Path Needs No Login	Updates Available

The Cal-CSIC has become aware of a remote code execution vulnerability, CVE-2026-108097, in the Field UI module of Drupal core. Field UI lets administrators add and configure the fields that structure Drupal website content and control their display. Where contributed modules or custom code expose the vulnerable functionality, an attacker could execute code on the site's server, putting its content and data at risk. There is no official CVSS rating as of 19 October 2026 however Drupal rates the issue Critical at 19/25 on its own security-risk scale[1,2,3]

Drupal states that core alone does not provide a direct exploit path. Contributed modules create multiple serious paths to the vulnerable Field UI functionality, including at least one that does not require authentication; custom code may also expose it. An attacker who reaches such a path could execute code on an affected Drupal site. Drupal has not identified the contributed modules or published exploitation steps in its advisory.[1]

Drupal released fixed versions 10.6.19, 11.3.19 and 11.4.10 on 14 October 2026; 12.0.0-beta2 includes the fix for its prerelease line. Uninstalling the core Field UI module (field_ui) is the vendor's temporary mitigation. Drupal Steward protects against some known attack paths but does not cover every possible exploit. Open-source reporting as of 19 October 2026 found no confirmed public proof of concept (PoC) or confirmed exploitation in the wild.[1,4,5]

The Cal-CSIC recommends that clients operating affected Drupal sites update supported installations immediately to 10.6.19, 11.3.19 or 11.4.10, as appropriate. Clients on end-of-life branches should migrate to a supported patched release. Where an immediate update is not possible, uninstall field_ui while preparing the upgrade; Drupal Steward coverage alone is insufficient. Clients should check enabled modules and custom code for exposure and review application logs and site changes if compromise is suspected.[1]

For additional details regarding CVE-2026-108097, please use this link:

Drupal Security Advisory:

https://www.drupal.org/sa-core-2026-014

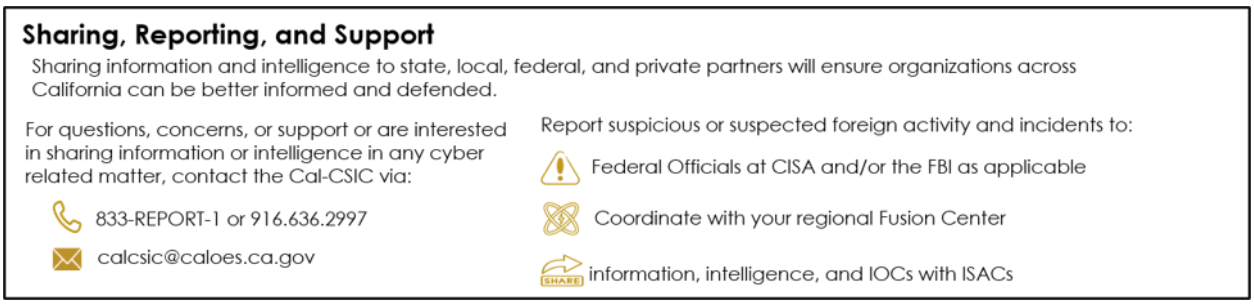
WARNING: This document is the property of the California Cybersecurity Integration Center (CAL-CSIC) and follows Traffic Light Protocol (TLP) standards. Except for **TLP: CLEAR**, all TLP designations require recipients to control, store, handle, transmit, and dispose of this product accordingly. Do not release to the public, media, or unauthorized personnel without prior CAL-CSIC approval. This document may contain information exempt from public release under the California Public Records Act (Govt. Code Sec. 7920.000 et seq.). CAL-CSIC does not guarantee the completeness or accuracy of the information.

Affected Products and Versions

Product	Affected Version	Fixed Release
Drupal core 8.9-10.5 (EOL)	>=8.9.0 <10.6.0	Migrate to supported patched branch
Drupal core 10.6.x	>=10.6.0 <10.6.19	10.6.19
Drupal core 11.0-11.2 (EOL)	>=11.0.0 <11.3.0	Migrate to supported patched branch
Drupal core 11.3.x	>=11.3.0 <11.3.19	11.3.19
Drupal core 11.4.x	>=11.4.0 <11.4.10	11.4.10
Drupal core 12 prerelease	>=12.0.0-alpha1 <12.0.0-beta2	12.0.0-beta2

Listed releases contain vulnerable code; exploitation also requires an exposed path through contributed modules or custom code. Older branches are at End Of Life (EOL) and receive no security coverage. Drupal 12 beta releases are not intended for production.[1,4]

Sharing, Reporting, and Support



References

[1] Drupal Security Team; "Drupal core - Critical - Remote code execution - SA-CORE-2026-014"; https://www.drupal.org/sa-core-2026-014; accessed 19 October 2026
[2] Drupal; "Field UI module overview"; https://www.drupal.org/docs/8/core/modules/field-ui/overview; accessed 19 October 2026
[3] Drupal Security Team; "Security risk levels defined"; https://www.drupal.org/drupal-security-team/security-risk-levels-defined; accessed 19 October 2026
[4] Drupal; "drupal 12.0.0-beta2"; https://www.drupal.org/project/drupal/releases/12.0.0-beta2; accessed 19 October 2026

WARNING: This document is the property of the California Cybersecurity Integration Center (CAL-CSIC) and follows Traffic Light Protocol (TLP) standards. Except for **TLP: CLEAR**, all TLP designations require recipients to control, store, handle, transmit, and dispose of this product accordingly. Do not release to the public, media, or unauthorized personnel without prior CAL-CSIC approval. This document may contain information exempt from public release under the California Public Records Act (Govt. Code Sec. 7920.000 et seq.). CAL-CSIC does not guarantee the completeness or accuracy of the information.

[5] ThreatWire; "CVE-2026-108097 Drupal core Field UI RCE: update to 11.4.10, 11.3.19, 10.6.19"; https://www.threatwire.tech/cve/cve-2026-108097; accessed 19 October 2026

WARNING: This document is the property of the California Cybersecurity Integration Center (CAL-CSIC) and follows Traffic Light Protocol (TLP) standards. Except for **TLP: CLEAR**, all TLP designations require recipients to control, store, handle, transmit, and dispose of this product accordingly. Do not release to the public, media, or unauthorized personnel without prior CAL-CSIC approval. This document may contain information exempt from public release under the California Public Records Act (Govt. Code Sec. 7920.000 et seq.). CAL-CSIC does not guarantee the completeness or accuracy of the information.