CYBER ADVISORY

Friday, May 22, 2026 **CAL-CSIC-202605-A-012**

Expected Rapid Exploitation of Drupal CMS

Drupal	Authentication Bypass	Remote Code Execution	Patch Available

The Cybersecurity Integration Center (CSIC) has been notified of a highly critical security vulnerability within the core architecture of the Drupal Content Management System (CMS) platform. The Drupal Security Team has published a Public Service Announcement (PSA-2026-05-18) detailing this vulnerability, which has been assigned a severity score of 20 out of 25 on Drupal's security risk matrix. The flaw stems from an undisclosed structural defect within Drupal core that requires no prior authentication or special access conditions to exploit. Successful exploitation could allow a remote attacker to compromise the confidentiality and integrity of a vulnerable site, potentially granting full administrative control over the underlying application environment.

The security flaw impacts almost all modern deployments of Drupal[1]. Officially supported branches, including Drupal 11.3.x, 11.2.x, 10.6.x, and 10.5.x, are directly affected. Demonstrating the severity of this risk, the Drupal Security Team is breaking standard protocol to provide out-of-band updates for end-of-life (EOL) minor versions (11.1.x and 10.4.x) alongside manual patch files for fully EOL major versions (Drupal 8.9 and 9.5). Drupal 7 installations are confirmed to be unaffected.

This vulnerability is particularly severe due to its zero-authentication requirement, lack of configuration dependencies across general deployments, and Drupal's widespread use as foundational infrastructure for enterprise, university, and government websites. Threat intelligence indicates that once security patches are published, malicious actors can quickly reverse-engineer the code changes to build working exploit payloads. The effective buffer between patch release and widespread public exploitation is anticipated to be measured in hours rather than days as noted by Drupal in their PSA, thus exposing vulnerable web applications to immediate threat vectors. Automated scanning and exploitation by threat clusters are expected immediately following disclosure since this risk profile heavily mirrors historic "Drupalgeddon"[2].

Cal-CSIC strongly recommends that all organizations operating Drupal-powered infrastructure urgently schedule emergency maintenance windows to apply the

published core security updates. In preparation, administrators should immediately upgrade to the latest available bugfix release within their respective minor branches to minimize deployment friction. For legacy and unsupported configurations, organizations must manually apply Drupal's provided hotfix patches or implement compensating network-layer web application firewall (WAF) rules, while aggressively prioritizing a migration path to a fully supported, stable release[3].

Cal-CSIC services are provided at no cost to assist organizations in strengthening their cybersecurity defenses. If you need assistance or wish to verify this communication, please contact us at (833) REPORT-1, or (916) 636-2997. Visit our website for more details: California Cybersecurity Integration Center | California Governor's Office of Emergency Services

References

[1] Drupal; "Upcoming highly critical release on May 20, 2026 - PSA-2026-05-18"; https://www.drupal.org/psa-2026-05-18#:~:text=Sites%20that%20use%20Drupal%20Steward,additional%20attack%20vectors%20are%20discovered.; accessed 20 May 2026

[2] Tech Times; "Drupal Core Patch Drops Today: No-Login Flaw Puts Government and University Sites at Immediate Risk"; https://www.techtimes.com/articles/316916/20260520/drupal-core-patch-drops-today-no-login-flaw-puts-government-university-sites-immediate-risk.htm; accessed 20 May 2026

[3] University of Michigan; "Apply Updates for Drupal Core Security Release May 20, 2026"; https://safecomputing.umich.edu/security-alerts/apply-updates-drupal-core-security-release-may-20-2026#:~:text=However%2C%20given%20the%20potential%20severity,introduce%20other%20bugs%20or%20regressions.; accessed 20 May 2026