An Lárionad Náisiúnta Cibearshlándála
National Cyber Security Centre

NCSC #2605220213

NCSC Advisory

Critical Vulnerability in Drupal core - SQL Injection

CVE-2026-9082

26th, May 2026

STATUS: TLP:CLEAR

Recipients can spread this to the world, there is no limit on disclosure. Sources may use TLP:CLEAR when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release. Subject to standard copyright rules, TLP:CLEAR information may be shared without restriction.

For more information on the Traffic Light Protocol, see https://www.first.org/tlp/. Please treat this document in accordance with the TLP assigned.

Description

CVE ID: CVE-2026-9082

Published: 2026-05-20

Vendor: Drupal

Product: Drupal core

CVSS Score[1]: 6.5

Products Affected

Product	Version
Drupal core	8.9.0 < 10.4.10
Drupal core	10.5.0 < 10.5.10
Drupal core	10.6.0 < 10.6.9
Drupal core	11.0.0 < 11.1.10
Drupal core	11.2.0 < 11.2.12
Drupal core	11.3.0 < 11.3.10

Impact

Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Drupal Drupal core allows SQL Injection.

Common Weakness Enumeration (CWE)[2]: CWE-89: CWE-89 Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')

Known Exploited Vulnerability (KEV) catalog[3]: Yes

Used by Ransomware Operators: N/A

[1] https://www.first.org/cvss/
[2] https://cwe.mitre.org
[3] https://www.cisa.gov/known-exploited-vulnerabilities-catalog

Recommendations

The NCSC strongly recommends installing updates for vulnerable systems with the highest priority, after thorough testing. Affected organisations should review the latest release notes and install the relevant updates from Drupal.

- https://nvd.nist.gov/vuln/detail/CVE-2026-9082
- https://www.cve.org/CVERecord?id=CVE-2026-9082
- https://www.drupal.org/sa-core-2026-004