CISA adds three actively exploited GeoServer and Drupal flaws to its KEV Catalog



CISA has added two OSGeo GeoServer flaws and one Drupal Core flaw to its KEV Catalog on evidence of active exploitation. Organisations running these products should check exposure and prioritise remediation.

- CISA added three vulnerabilities to the KEV Catalog based on evidence of active exploitation.
- CVE-2026-120705 is an XML injection flaw and CVE-2026-129243 an incorrect authorization flaw, both in OSGeo GeoServer.
- CVE-2026-136716 is an improper check for unusual or exceptional conditions in Drupal Core.
- BOD 26-04 binds only US federal civilian agencies, but CISA encourages all organisations to adopt risk-based vulnerability management and prioritise KEV entries.

CISA has added three vulnerabilities to its Known Exploited Vulnerabilities (KEV) Catalog after finding evidence that they are being exploited. CISA notes that flaws of this kind are a frequent attack vector for malicious actors.

What was added

- **CVE-2026-120705**: XML injection vulnerability in OSGeo GeoServer
- **CVE-2026-129243**: incorrect authorization vulnerability in OSGeo GeoServer
- **CVE-2026-136716**: improper check for unusual or exceptional conditions in Drupal Core

The source does not give affected versions, patch details or technical specifics, so teams should consult the vendors' own advisories for those.

Why it matters beyond US agencies

Binding Operational Directive 26-04 requires US Federal Civilian Executive Branch agencies to remediate quickly the KEV-listed vulnerabilities on publicly exposed assets that give full control after exploitation, and to defer lower-risk items. It also sets basic expectations for checking whether a system was compromised before the patch was applied.

The directive does not apply to organisations outside those agencies. CISA nonetheless encourages all organisations to adopt risk-based vulnerability management and to prioritise KEV Catalog entries. For institutions in the Kingdom, the KEV Catalog is a useful, evidence-based input to patch prioritisation, particularly for internet-facing systems.

Suggested approach

Confirm whether GeoServer or Drupal is used anywhere in your estate, including by third parties, and whether those instances are reachable from the internet. Where they are, treat remediation as a priority and review for signs of earlier compromise.

What to do now

1. Inventory all GeoServer and Drupal instances, including those run by vendors or hosting providers.
2. Identify which instances are internet-facing and rank them first for remediation.
3. Apply vendor fixes or mitigations for the three CVEs, following the vendors' advisories.
4. Review logs and systems on exposed instances for signs of compromise before patching.
5. Add KEV Catalog monitoring to your vulnerability management process as a prioritisation input.