AKTIV AUSGENUTZT · CISA KEV

THREAT INTELLIGENCE BRIEFING

CVE-2026-132165

Website-Übernahme ohne Anmeldung über den Drupal-Installer.

Über die nach der Installation liegengebliebene Datei install.php können Angreifer eine Drupal-Website unter bestimmten Bedingungen neu installieren lassen – und sie so übernehmen oder eigenen Code ausführen. Laut Drupal laufen Angriffe seit dem 19.11.2026; CISA führt die Lücke seit 24.11.2026 als aktiv ausgenutzt. Ein Folge-Advisory vom 25.11. schließt Restwege.

> **Geschäftsrisiko:** Übernahme der Unternehmenswebsite samt Administratorkonto, Manipulation von Inhalten und Formularen, Abfluss von Nutzer- und Kontaktdaten sowie Einstieg in den Webserver – ein wahrscheinlich meldepflichtiger Vorfall nach DSGVO / NIS-2.

9,8 / 10

KRITISCH
CVSS 3.1 BASISWERT

Niedrig | Mittel | Hoch | Kritisch

`CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H` – aus dem Netz, ohne Anmeldung, ohne Mitwirkung eines Nutzers, mit voller Wirkung. Basiswert von NVD; CISA (ADP) bewertet mit 8,1, Drupal selbst mit 20/25 „Highly critical“.

AKTIV AUSGENUTZT	BETROFFEN	HANDLUNGSBEDARF
CISA KEV seit 24.11.2026	Drupal Core bis 10.6.21, 11.0–11.3.21, 11.4.0–11.4.12 (empfohlen: 10.6.23 / 11.3.23 / 11.4.14)	Sofort – aktiv ausgenutzt

Bildmotive: KI-generierte Symbolbilder

Das Wichtigste in 60 Sekunden.

9,8 · KRITISCH
CVSS-Schweregrad

Ohne Konto
Aufruf von install.php · CWE-306

Aktiv ausgenutzt
CISA KEV seit 24.11.2026

Fix verfügbar
10.6.23 / 11.3.23 / 11.4.14

Die Ursache: Fehlende Authentifizierung einer kritischen Funktion (**CWE-306**): Der Installer **core/install.php** bleibt nach der Einrichtung auf dem Server erreichbar. Unter bestimmten Bedingungen akzeptiert er erneut einen **Installationslauf**. Damit lässt sich die Website übernehmen oder Code ausführen. Schreibrechte des Webservers auf **settings.php** erweitern die Angriffswege. Seiten in unvollständigem Installationszustand bleiben laut SA-CORE-2026-019 auch nach dem ersten Fix angreifbar.

ANGRIFFSKETTE

01	02	03	04
Installer erreichbar – /core/install.php antwortet aus dem Netz	**Neuinstallation** – Angreifer startet einen Installationslauf	**Admin-Übernahme** – Konto 1 bzw. Einstellungen gehen an den Angreifer	**Codeausführung** – Befehle laufen als Webserver-Benutzer

Betroffenheit & Fixversionen

Zweig	Verwundbar bis	Fixversion (Ziel)
Drupal 11.4.x	`11.4.0–11.4.12`	`11.4.13 (empf. 11.4.14)`
Drupal 11.3.x	`11.3.0–11.3.21`	`11.3.22 (empf. 11.3.23)`
Drupal 10.6.x	`bis 10.6.21`	`10.6.22 (empf. 10.6.23)`
Drupal ≤ 11.2 / ≤ 10.5 / 8 / 9	End of Life	kein Fix – Migration

Die Fixstände vom 18.11. schützen **nicht** vor dem Folgefehler CVE-2026-136716 (SA-CORE-2026-019, ebenfalls ausgenutzt). Nach dem Update `update.php` ausführen.

Regulatorischer Hinweis: Ein bestätigter unbefugter Zugriff auf Systeme mit personenbezogenen Daten ist in der Regel meldepflichtig – DSGVO unverzüglich (i. d. R. 72 h), NIS-2 nach den für Sie geltenden Fristen. Die Meldung bleibt bei Ihnen; wir unterstützen bei Bewertung und Dokumentation.

ZEITACHSE

18.11.2026
SA-CORE-2026-017 + Updates

19.11.2026
Erste Angriffe (laut Drupal)

24.11.2026
Aufnahme in CISA KEV

25.11.2026
Folge-Fix SA-CORE-2026-019

Bildmotive: KI-generierte Symbolbilder

Ihr Maßnahmenplan.

In dieser Reihenfolge – Installer sperren vor Update, Update vor Entwarnung.

SOFORT	KURZFRISTIG	PARALLEL
install.php sperren	Core aktualisieren	Auf Einbruch prüfen

01 Installer sofort sperren

Zugriff auf `/core/install.php` in der Webserver-Konfiguration blockieren oder die Datei entfernen. Danach prüfen: Aufruf muss 403 oder 404 liefern.

02 Drupal Core aktualisieren

Auf `10.6.23`, `11.3.23` oder `11.4.14` gehen und anschließend `update.php` ausführen. Ältere Zweige sind End of Life.

03 Administratorkonto prüfen

E-Mail-Adresse von Benutzer 1, unbekannte Administratoren und Sitzungen von Benutzer 1 prüfen; den Installationszeitpunkt (`install_time`) auf Plausibilität kontrollieren.

04 Logs seit 18.11. auswerten

Zugriffslogs auf POST-Aufrufe von `install.php` mit 302/303, große Antworten und Parameter `op=`/`id=` durchsuchen. Bei Treffern als kompromittiert behandeln.

Kompromittierungs-Indikatoren (IoCs)

ÖFFENTLICHE IOCS

Keine IPs oder Hashes veröffentlicht – Drupal nennt Prüfmuster statt Indikatoren

AUSWERTUNGSQUELLEN

Webserver- und CDN-Logs, Benutzer- und Sitzungstabelle, Drupal-State

AUFFÄLLIGE MUSTER

POST install.php mit 302/303

geänderte E-Mail von Benutzer 1

Zur Einordnung: HTTP 200 auf install.php ist bei installierten Seiten normal und allein kein Befund. Manche Hoster halten Logs nur wenige Tage – jetzt sichern.

Wichtig: Das Update allein bereinigt keine bereits übernommene Website. Angelegte Konten, Dateien und Einstellungen bleiben bestehen.

Bildmotive: KI-generierte Symbolbilder

Lassen Sie das von unseren Experten prüfen.

Drei Bausteine, die genau auf diese Schwachstelle einzahlen – vom schnellen Exposure-Check bis zur laufenden Absicherung.

Cyber Defense Center

Worauf wir bei dieser Schwachstelle achten: POST auf install.php mit Umleitung. Das setzt voraus, dass die nötigen Logquellen angebunden sind.

Vulnerability & Exposure Management

Wir finden Drupal-Websites mit erreichbarem install.php über Ihren gesamten Perimeter – bevor Angreifer sie finden – und priorisieren nach realer Ausnutzung.

Incident-Response-Retainer

Bei Verdacht auf einen bereits erfolgten Zugriff übernimmt unser IR-Team Forensik und Eindämmung – mit vertraglich zugesicherter Reaktionszeit.

SO GEHEN WIR VOR

01 Exposure-Check

Wir prüfen, ob Ihre Drupal-Systeme verwundbar konfiguriert und exponiert sind.

02 Sofortmaßnahmen begleiten

Mitigation und Patch-Fahrplan gemeinsam mit Ihrem Team umgesetzt.

03 Absichern & überwachen

Prüfung auf Angriffsspuren, danach laufendes Monitoring und IR-Bereitschaft – 24/7, wenn Ihr Team das nicht selbst leisten kann.

Empfehlung für die Geschäftsleitung

- Klären lassen, welche Drupal-Websites im Haus oder bei Agenturen laufen.
- Sperre des Installers und Update mit Termin einfordern.
- Prüfung auf Kompromittierung anordnen, bevor entwarnt wird.

Ihr Part · unser Part. **Sie behalten die Kontrolle über Konfiguration und Freigaben; wir liefern Analyse, Bewertung und – im Retainer – die Reaktionskette.**

Rollen, Eingriffstiefe und SLAs im Erstgespräch (RACI, AVV/TOM auf Anfrage) · Datenhaltung auf Wunsch in Deutschland · ISO/IEC 27001 (TÜV SÜD) · deutschsprachige Analysten.

Sprechen Sie mit uns, bevor es ein Angreifer tut.

Kostenloses 30-Minuten-Erstgespräch – wir prüfen Ihre Exposure gegenüber CVE-2026-132165 und dem Drupal-Perimeter.

+49 89 45 24 24-100 · kontakt@argos.security · www.argos.security

Termin buchen

Bildmotive: KI-generierte Symbolbilder

Quellen: Drupal SA-CORE-2026-017 (18.11.) und -019 (25.11.) · Drupal-Prüfanleitung · CVE-Record · NVD (CVSS 9,8) · CISA KEV (24.11.2026). Stand 27.11.2026. Argos Security ist ISO/IEC 27001 (TÜV SÜD) zertifiziert.