AKTIV AUSGENUTZT · CISA KEV

THREAT INTELLIGENCE BRIEFING

CVE-2026-136716

Website-Übernahme über den Installer trotz erstem Drupal-Patch.

Der erste Fix für den Drupal-Installer vom 18.11. (CVE-2026-132165) reicht nicht für alle Websites: Seiten in einem ungewöhnlichen oder unvollständigen Installationszustand lassen sich weiter über install.php übernehmen – auch Produktivseiten. Drupal meldet Angriffe, CISA führt die Lücke seit 27.11.2026 als aktiv ausgenutzt.

> **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 CISA (ADP) in NVD; Drupal selbst bewertet mit 21/25 „Highly critical".

AKTIV AUSGENUTZT	BETROFFEN	HANDLUNGSBEDARF
CISA KEV seit 27.11.2026	Drupal Core vor 10.6.23, 11.0–11.3.22, 11.4.0–11.4.13 (Fix: 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-754

Aktiv ausgenutzt
CISA KEV seit 27.11.2026

Fix verfügbar
10.6.23 / 11.3.23 / 11.4.14

Die Ursache: Unzureichende Prüfung ungewöhnlicher Zustände (**CWE-754**): Der Installer **core/install.php** erkennt bestimmte **unvollständige Installationszustände** nicht als abgeschlossen. Websites in diesem Zustand bleiben nach dem Fix aus SA-CORE-2026-017 übernehmbar. In der Oberfläche ist der Zustand nicht zu erkennen, und bereits übernommene Seiten zeigen ihn oft nicht mehr. Erst ein **Update-Hook** (update.php) bereinigt bestehende Seiten.

ANGRIFFSKETTE

01	02	03	04
Installer erreichbar – /core/install.php antwortet aus dem Netz	**Sonderzustand** – Seite gilt dem Installer als nicht fertig eingerichtet	**Admin-Übernahme** – Benutzer 1 geht an den Angreifer	**Vollzugriff** – Inhalte, Daten und Code der Website

Betroffenheit & Fixversionen

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

Wer am 18.11. auf 10.6.22 / 11.3.22 / 11.4.13 gepatcht hat, ist **nicht** geschützt. Nach dem Update unbedingt `update.php` ausführen. Ein bereits gesicherter Installer schließt die Lücke laut Drupal ebenfalls.

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
Erster Fix SA-CORE-2026-017

25.11.2026
Folge-Fix SA-CORE-2026-019

26.11.2026
CVE veröffentlicht (NVD)

27.11.2026
Aufnahme in CISA KEV

Bildmotive: KI-generierte Symbolbilder

Ihr Maßnahmenplan.

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

SOFORT	KURZFRISTIG	PARALLEL
install.php sperren	Core + update.php	Auf Einbruch prüfen

01 Installer sofort sperren

Zugriff auf `/core/install.php` in der Webserver-Konfiguration blockieren. Danach prüfen: Aufruf aus dem Netz muss 403 oder 404 liefern.

02 Core aktualisieren, update.php ausführen

Auf `10.6.23`, `11.3.23` oder `11.4.14` gehen. Erst `update.php` bereinigt bestehende Seiten im Sonderzustand.

03 Benutzer 1 absichern

E-Mail-Adresse von Benutzer 1 auf eine eigene Adresse prüfen, Passwort zurücksetzen, unbekannte Administratoren und Sitzungen entfernen.

04 Logs seit 18.11. auswerten

Zugriffslogs auf Aufrufe von `install.php` und Änderungen an oder durch Benutzer 1 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

AUFFÄLLIGE MUSTER

Aufrufe von install.php, geänderte E-Mail von Benutzer 1

Zur Einordnung: Ob eine Seite im verwundbaren Zustand war, ist nachträglich oft nicht zu sehen. 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: Zugriffe auf install.php, Änderung Benutzer 1. 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, ob die Drupal-Websites schon auf dem Stand vom 25.11. sind.
- Sperre des Installers und update.php 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-2026-136716 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-2026-019 (25.11.) und -017 (18.11.) · NVD (CVSS 9,8, CISA-ADP) · CISA KEV (27.11.2026). Stand 27.11.2026. Argos Security ist ISO/IEC 27001 (TÜV SÜD) zertifiziert.