AKTIV AUSGENUTZT · CISA KEV

THREAT INTELLIGENCE BRIEFING

CVE-2026-90817

Codeausführung ohne Anmeldung in REDCap-Forschungsservern.

Über den Link einer öffentlichen Umfrage können Angreifer ohne Konto eigenen Code auf einem REDCap-Server ausführen. REDCap ist in Kliniken, Universitäten und der Forschung weit verbreitet und speichert oft Studien- und Patientendaten. Updates sind verfügbar; CISA führt die Lücke seit 18.11.2026 als aktiv ausgenutzt.

> **Geschäftsrisiko:** Abfluss oder Manipulation von Studien- und Gesundheitsdaten, Übernahme des Servers als Einstieg ins Netz und ein wahrscheinlich meldepflichtiger Sicherheitsvorfall 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 auf den Server. Basiswert von Securifera als CNA, von NVD übernommen.

AKTIV AUSGENUTZT	BETROFFEN	HANDLUNGSBEDARF
CISA KEV seit 18.11.2026	REDCap ab 13.3.0 bis vor 16.0.49 LTS / 17.3.10 LTS / 17.4.4	Sofort – aktiv ausgenutzt

Bildmotive: KI-generierte Symbolbilder

Das Wichtigste in 60 Sekunden.

9,8 · KRITISCH
CVSS-Schweregrad

Ohne Konto
Umfrage-Link genügt · CWE-73

Aktiv ausgenutzt
CISA KEV seit 18.11.2026

3 Fix-Versionen
16.0.49 · 17.3.10 · 17.4.4

Die Ursache: Mehrere Fehler greifen ineinander (**CWE-73**, **CWE-94**): Eine doppelt kodierte Anfrage aus dem Kontext einer **öffentlichen Umfrage** erreicht den Datenimport, der dort fälschlich mit Administratorrechten läuft. Ein vom Angreifer gewählter **Dateipfad bzw. PHP-Stream** erlaubt dann das Überschreiben einer Vorlagendatei, die REDCap als Code ausführt. Nötig ist nur der Link einer aktiven öffentlichen Umfrage.

ANGRIFFSKETTE

01 **Umfrage-Link** – Angreifer kennt den Link einer öffentlichen Umfrage

02 **Umgeleitete Anfrage** – doppelt kodierter Aufruf erreicht den Datenimport

03 **Datei überschrieben** – präparierter Pfad schreibt in eine Vorlagendatei

04 **Codeausführung** – REDCap lädt die Datei, Angreifer steuert den Server

Betroffenheit & Fixversionen

Release-Linie	Verwundbar bis	Fixversion (Ziel)
LTS 16.0	ab 13.3.0	16.0.49
LTS 17.3	ab 13.3.0	17.3.10
Standard 17.4	ab 13.3.0	17.4.4
vor 13.3.0	laut CVE nicht betroffen	aktuelle Version

Fix-Versionen laut CVE-Record (CNA Securifera). Updates verteilt Vanderbilt **nur im REDCap-Konsortium**; Hosting-Partner aktualisieren selbst. Übergangsweise öffentliche Umfragen einschränken.

Regulatorischer Hinweis: REDCap enthält häufig Gesundheits- und Studiendaten (Art. 9 DSGVO). Ein bestätigter unbefugter Zugriff 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

20.09.2026
CVE-Record + Fix-Versionen

27.09.2026
Technische Analyse Securifera

18.11.2026
Aufnahme in CISA KEV

21.11.2026
Frist für US-Behörden

Bildmotive: KI-generierte Symbolbilder

Ihr Maßnahmenplan.

In dieser Reihenfolge – Erreichbarkeit vor Patch, Patch vor Entwarnung.

SOFORT	KURZFRISTIG	PARALLEL
Umfragen einschränken	REDCap aktualisieren	Auf Einbruch prüfen

01 Betroffenheit feststellen

Eigene und extern gehostete REDCap-Instanzen erfassen und die Version im Control Center ablesen. Betroffen sind alle Versionen ab 13.3.0 vor den Fix-Versionen.

02 REDCap aktualisieren

Auf `16.0.49` LTS, `17.3.10` LTS oder `17.4.4` aktualisieren, je nach Release-Linie. Bei gehosteten Instanzen das Update beim Betreiber mit Termin einfordern.

03 Risiko bis zum Update senken

Öffentliche Umfragen vorübergehend deaktivieren oder einschränken und per WAF Aufrufe aus dem Umfrage-Kontext auf Datenimport und Parcel-Controller sperren.

04 Kompromittierung ausschließen

Webserver-Logs auf doppelt kodierte `__passthru`-Werte und Umfrage-Aufrufe von `DataImportController` prüfen, außerdem Änderungen unter `temp/cache` und Prozesse des Webserver-Kontos.

Kompromittierungs-Indikatoren (IoCs)

ÖFFENTLICHE IOCS

Keine Signaturen – Prüfhinweise des Entdeckers

AUSWERTUNGSQUELLEN

Webserver-Zugriffslogs, PHP-Logs Dateisystem temp/cache, Prozessliste

AUFFÄLLIGE MUSTER

kodiertes __passthru, Route DataImport/Parcel fname mit php://filter, Shells des Webservers

Zur Einordnung: Die Muster stammen aus der technischen Analyse von Securifera, nicht aus beobachteten Angriffen. Sie sind Ansatzpunkte für eine Auswertung, keine bestätigten Signaturen.

Wichtig: Umfrage-Links werden bewusst öffentlich verteilt und sind oft über Suchmaschinen auffindbar. Der einzige Vorbehalt des Angriffs ist damit in der Praxis kaum eine Hürde.

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: Ein Umfrage-Aufruf, der den Datenimport erreicht. Das setzt voraus, dass die nötigen Logquellen angebunden sind.

Vulnerability & Exposure Management

Wir finden REDCap-Server mit öffentlichen Umfragen 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 REDCap-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, wo REDCap im Haus oder bei Partnern läuft.
- Update auf die Fix-Version 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-2026-90817 und dem REDCap-Perimeter.

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

Termin buchen

Bildmotive: KI-generierte Symbolbilder

Quellen: CVE-Record CVE-2026-90817 (CNA Securifera; Fix-Versionen, CVSS 9,8) · NVD · CISA KEV (18.11.2026) · Securifera-Analyse vom 27.09.2026. Stand 18.11.2026. Argos Security ist ISO/IEC 27001 (TÜV SÜD) zertifiziert.