AKTIV AUSGENUTZT · CISA KEV

THREAT INTELLIGENCE BRIEFING

CVE-2026-129448

Code-Ausführung ohne Anmeldung über den XML-RPC-Endpunkt von Apache Roller.

Apache Roller ist ein quelloffener Blog-Server auf Java-Basis. Sein XML-RPC-Endpunkt verarbeitet eingehende Daten, bevor er prüft, wer anfragt – ein Angreifer aus dem Netz kann so ohne Anmeldung eigenen Code auf dem Server ausführen. Apache hat die Lücke am 17.11.2026 für alle Versionen ab 4.0.0 bestätigt und meldet aktive Ausnutzung; die CISA hat sie am 20.11.2026 in ihren KEV-Katalog aufgenommen. Die Fixversion 6.1.6 ist seit September 2026 verfügbar.

> **Geschäftsrisiko:** Übernahme des Blog-Servers und des Applikationsservers dahinter – mit Zugriff auf Inhalte, Konten und Datenbank, einem Brückenkopf ins interne Netz und einem möglicherweise meldepflichtigen Sicherheitsvorfall nach NIS-2 / DSGVO.

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 das System. Basiswert laut Apache (CNA), vom NVD übernommen; die eigene NIST-Bewertung steht noch aus.

AUSNUTZUNG BELEGT SEIT
17.11.2026 (laut Apache; Beginn nicht veröffentlicht)

BETROFFEN
Apache Roller 4.0.0 bis 6.1.5 (6.1.5 als CVE-2026-82384)

HANDLUNGSBEDARF
Notfall-Change – sofort patchen oder Endpunkt schließen

Bildmotive: KI-generierte Symbolbilder

Das Wichtigste in 60 Sekunden.

9,8 · KRITISCH
CVSS-Schweregrad

Ohne Anmeldung
XML-RPC-Endpunkt · CWE-502

Aktiv ausgenutzt
laut Apache · CISA KEV seit 20.11.2026 · PoC öffentlich

6.1.6 · 6.1.7
Fixversion · aktuelles Release

Die Ursache: Der XML-RPC-Endpunkt von Roller (`/roller-services/xmlrpc`) akzeptiert die herstellerspezifischen Erweiterungstypen der verwendeten XML-RPC-Bibliothek und wandelt die darin enthaltenen Java-Objekte zurück, bevor der Anfragende authentifiziert wird (CWE-502, Deserialisierung nicht vertrauenswürdiger Daten). Das Servlet ist immer eingebunden – auch dann, wenn XML-RPC in der Administrationsoberfläche ausgeschaltet ist. Laut Apache führt das zur Ausführung beliebigen Codes. Die Lücke wurde im September 2026 zunächst nur für Version 6.1.5 gemeldet (CVE-2026-82384); am 17.11.2026 hat Apache sie mit CVE-2026-129448 auf alle Versionen ab 4.0.0 ausgeweitet.

ANGRIFFSKETTE

01	02	03	04
Endpunkt erreichbar – Roller ist aus dem Netz erreichbar, der XML-RPC-Pfad antwortet	**Präparierte Anfrage** – XML-RPC-Aufruf mit eingebettetem Java-Objekt als Erweiterungstyp	**Code-Ausführung** – Objekt wird vor der Anmeldeprüfung deserialisiert, Code läuft im Roller-Prozess	**Festsetzen** – Zugriff auf Inhalte, Datenbank-Zugangsdaten und Weg ins interne Netz

Betroffenheit & Fixversionen

Roller-Version	Verwundbar bis	Fixversion (Ziel)
Roller 4.0.0 – 6.1.4	`4.0.0 bis 6.1.4 (CVE-2026-129448)`	`6.1.6 (aktuell 6.1.7)`
Roller 6.1.5	`6.1.5 (CVE-2026-82384)`	`6.1.6 (aktuell 6.1.7)`
Roller 6.1.6	nicht betroffen	6.1.7 empfohlen (weitere Fixes)
Roller vor 4.0.0	von Apache nicht bewertet	auf 6.1.7 migrieren

Angaben laut Apache-Advisory vom 17.11.2026 und CVE-2026-82384 (25.09.2026). Apache patcht ältere Release-Linien nicht nachträglich – der Weg ist das Upgrade auf das aktuelle Release `6.1.7` (11.11.2026), das u. a. eine zweite Deserialisierungslücke in Ping-Antworten schließt (CVE-2026-123374). Notlösung bis zum Update: in `WEB-INF/web.xml` `enabledForExtensions` auf `false` setzen oder das Mapping `/roller-services/xmlrpc` entfernen und Roller neu starten. **Das Abschalten von XML-RPC in der Administrationsoberfläche reicht nicht.**

Regulatorischer Hinweis: Ein bestätigter unbefugter Zugriff auf den Server kann eine meldepflichtige Verletzung darstellen – 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

24.–25.09.2026
Roller 6.1.6 · CVE-2026-82384 (nur 6.1.5 genannt)

28.09.2026
Exploit-Code für CVE-2026-82384 öffentlich auf GitHub

17.11.2026
CVE-2026-129448: 4.0.0 bis 6.1.4 betroffen, aktive Ausnutzung (Apache)

20.11.2026
CISA KEV · Frist für US-Behörden 23.11.2026

Bildmotive: KI-generierte Symbolbilder

Ihr Maßnahmenplan.

In dieser Reihenfolge – Endpunkt schließen vor Patch, Patch vor Entwarnung.

SOFORT	KURZFRISTIG	PARALLEL
XML-RPC-Endpunkt schließen	Update auf 6.1.7	Kompromittierung prüfen

01 Betroffenheit feststellen

Alle Roller-Installationen erfassen, auch Blogs einzelner Abteilungen und eingebettete Installationen. Betroffen ist jede Version von `4.0.0` bis `6.1.5`. Klären, ob der Pfad `/roller-services/xmlrpc` aus dem Internet oder aus Partnernetzen erreichbar ist.

02 Patchen

Auf das aktuelle Release `6.1.7` aktualisieren, mindestens auf `6.1.6`. Apache korrigiert ältere Versionen nicht nachträglich. Vor dem Update die Release Notes zu 6.1.7 lesen – Apache weist auf geänderte Verhaltensweisen hin.

03 Risiko bis zum Update senken

In `WEB-INF/web.xml` `enabledForExtensions` auf `false` setzen oder das Servlet-Mapping `/roller-services/xmlrpc` entfernen, dann Roller neu starten. Der Schalter in der Administrationsoberfläche schützt nicht. Zusätzlich den Pfad am Reverse Proxy oder an der WAF sperren.

04 Kompromittierung ausschließen

Zugriffsprotokolle auf POST-Anfragen an `/roller-services/xmlrpc` durchsuchen, mindestens zurück bis Ende September 2026 (öffentlicher Exploit-Code seit 28.09.). Auf unerwartete Prozesse, Dateien und ausgehende Verbindungen des Applikationsservers prüfen. Ein Patch schließt die Lücke – nicht einen bereits erfolgten Zugriff.

Kompromittierungs-Indikatoren (IoCs)

ÖFFENTLICHE IOCS

Keine veröffentlicht

Apache und CISA nennen keine Indikatoren

AUSWERTUNGSQUELLEN

Webserver-, Proxy- und WAF-Logs

Logs des Java-Applikationsservers

AUFFÄLLIGE MUSTER

XML-RPC-Anfragen mit Erweiterungstypen aus fremden Netzen

Shell- oder Netzwerkprozesse als Kind des Java-Prozesses

Zur Einordnung: Zu den laufenden Angriffen hat Apache keine Details veröffentlicht. Die genannten Muster sind Suchansätze aus dem Angriffsweg, kein vollständiger Ausschluss.

Wichtig: Ein Blog-Server wirkt harmlos – läuft er aber im eigenen Rechenzentrum, ist er nach einer Übernahme ein Einstiegspunkt ins Firmennetz. Gefährdet sind gerade selten gepflegte Altinstallationen.

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 Roller-Java-Prozess, der eine Shell oder einen Download startet. Das setzt voraus, dass die nötigen Logquellen angebunden sind.

Vulnerability & Exposure Management

Wir finden Aus dem Internet erreichbare Apache-Roller-Instanzen 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 Roller-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

- Update aller Roller-Installationen auf 6.1.7 als Notfall-Change anordnen.
- Bis dahin den XML-RPC-Endpunkt per Konfiguration und am Proxy schließen lassen.
- Eine Prüfung auf Kompromittierung seit Ende September 2026 beauftragen.

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-2026-129448 und dem Roller-Perimeter.

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

Termin buchen

Bildmotive: KI-generierte Symbolbilder

Quellen: Apache Roller Advisory CVE-2026-129448 (lists.apache.org, oss-security, 17.11.2026, Versionen 4.0.0 bis 6.1.4, aktive Ausnutzung, CVSS 3.1 9,8) · Apache Roller Advisory CVE-2026-82384 (25.09.2026, Version 6.1.5, Fix 6.1.6) · Apache Roller Security-Seite (6.1.6 vom 24.09.2026, 6.1.7 vom 11.11.2026) · NVD (CVSS 3.1 Basiswert 9,8 laut Apache als CNA, CWE-502, Analyse läuft) · CISA KEV (aufgenommen 20.11.2026, Frist 23.11.2026) · GitHub, öffentlicher PoC zu CVE-2026-82384 (28.09.2026). Stand 20.11.2026. Argos Security ist ISO/IEC 27001 (TÜV SÜD) zertifiziert.