Wichtige Sicherheitsinformation für Joomla-Websites

Hintergrund

Für die weit verbreitete Joomla-Erweiterung **JCE Editor**, die seit vielen Jahren von zahlreichen Joomla-Websites als Alternative zum Joomla-Standardeditor eingesetzt wird, wurde eine schwerwiegende Sicherheitslücke bekannt.

Die Schwachstelle wurde Anfang Juni 2026 entdeckt und am 16.06.2026 offiziell als CVE veröffentlicht. Seitdem werden weltweit automatisierte Angriffe auf betroffene Websites beobachtet.

Über diese Sicherheitslücke können Angreifer unter Umständen Dateien auf dem Webserver ablegen und ausführen, ohne sich mit einem gültigen Benutzerkonto anmelden zu müssen. Dadurch können Websites kompromittiert und für weitere Angriffe missbraucht werden.

Da der JCE Editor seit vielen Jahren zu den beliebtesten Joomla-Erweiterungen gehört, ist davon auszugehen, dass eine größere Anzahl von Websites betroffen sein könnte.

Aus diesem Grund empfehlen wir allen Verantwortlichen von Joomla-Websites dringend zu prüfen, ob der JCE Editor eingesetzt wird und ob die eigene Website bereits betroffen ist.

Schritt 1: Prüfen, ob JCE installiert ist

Melden Sie sich im Administrationsbereich Ihrer Joomla-Website an.

Öffnen Sie:

System → Erweiterungen → Verwalten

Geben Sie im Suchfeld ein:

JCE

Wird dort eine Erweiterung mit dem Namen **JCE Editor** angezeigt, ist Ihre Website potenziell betroffen.

Alternativ können Sie unter:

System → Plugins

nach **JCE** suchen.

Wenn JCE installiert ist, sollten die folgenden Prüfungen zeitnah durchgeführt werden.

Schritt 2: Prüfen, ob Ihre Website bereits betroffen ist

2.1. Benutzerkonten prüfen

Öffnen Sie:

Benutzer → Verwalten

Prüfen Sie:

- Sind alle Benutzerkonten bekannt?
- Wurden neue Administratoren angelegt?
- Gibt es Benutzer mit unbekannten E-Mail-Adressen?

Falls Ihnen Benutzerkonten unbekannt vorkommen, sollten Sie umgehend Ihren technischen Dienstleister informieren.

2.2. Dateien prüfen

Falls Sie Zugriff auf das Hosting oder einen FTP-Zugang besitzen, kontrollieren Sie insbesondere folgende Verzeichnisse:

root > Hauptverzeichnis
root/cache
root/images
root/tmp
root/media

administrator
administrator/cache
administrator/logs

Verdächtig sind beispielsweise:

cachec393d7index.php
cfg7c2443index.php
inc528d3bindex.php
3c75b69e92d0.php
c67cbfbd4b5f.php
image127.php.gif

Ebenso verdächtig sind:

- unbekannte PHP-Dateien
- Dateien mit zufälligen Buchstaben- und Zahlenfolgen
- kürzlich angelegte PHP-Dateien in den Verzeichnissen images, tmp oder media
- Dateien, die erst in den letzten Tagen erstellt wurden und Ihnen nicht bekannt sind

Wenn Sie solche Dateien finden, sollten Sie diese nicht eigenständig löschen, sondern Ihren technischen Dienstleister kontaktieren.

2.3. Wichtiger Hinweis

Bei den aktuell beobachteten Angriffen bleiben die eigentlichen Inhalte der Website häufig unverändert.

Das Fehlen sichtbarer Auffälligkeiten bedeutet daher nicht, dass eine Website nicht betroffen ist.

Angreifer legen oftmals lediglich zusätzliche Dateien auf dem Webserver ab, um dauerhaft Zugriff zu erhalten oder die Website für Suchmaschinenmanipulationen zu missbrauchen. Die Website selbst funktioniert dabei zunächst scheinbar unverändert weiter.

Aus diesem Grund sind die Prüfung installierter Erweiterungen, Benutzerkonten und Dateien deutlich aussagekräftiger als eine reine Sichtprüfung der Website.

Schritt 3: JCE entfernen oder aktualisieren

3.1. JCE entfernen (empfohlen)

Wenn Sie die erweiterten Funktionen des JCE Editors nicht benötigen, empfehlen wir:

- aktuelle Datensicherung erstellen
- JCE deinstallieren
- Joomla TinyMCE aktivieren

Dies erfolgt unter:

System → Konfiguration → Standard-Editor

Dort wählen Sie:

TinyMCE

aus. Da TinyMCE Bestandteil von Joomla ist, reduziert sich die Angriffsfläche Ihrer Website und der Aufwand für die Pflege zusätzlicher Erweiterungen.

3.2. JCE aktualisieren

Wenn Sie auf die erweiterten Funktionen des JCE Editors angewiesen sind, sollten Sie die installierte Version zeitnah auf die aktuelle Version aktualisieren.

Vor der Aktualisierung empfehlen wir:

- aktuelle Datensicherung erstellen
- Website auf Auffälligkeiten prüfen
- Administrator-Passwörter überprüfen
- Zwei-Faktor-Authentifizierung aktivieren

Installieren Sie anschließend die aktuelle vom Hersteller bereitgestellte JCE-Version. Version 2.9.99.5 und alle nachfolgenden Versionen schließen die bekannt gewordene Sicherheitslücke.

3.3. Wichtiger Hinweis

Die Aktualisierung verhindert zukünftige Angriffe über diese Sicherheitslücke. Wurde die Website bereits kompromittiert, bleiben möglicherweise bereits abgelegte Schaddateien – unabhängig davon, ob Sie den JCE entfernen oder aktualisieren – weiterhin auf dem Webserver vorhanden.

Führen Sie deshalb die in diesem Dokument beschriebenen Prüfungen durch und stellen Sie die Website bei Verdacht auf eine Kompromittierung aus einer nachweislich sauberen Datensicherung wieder her.

Eine reine Aktualisierung oder Deinstallation des JCE Editors ersetzt keine Überprüfung und gegebenenfalls notwendige Bereinigung der Website.

Schritt 4: Website bereinigen

Wurden verdächtige Dateien, unbekannte Benutzerkonten oder andere Auffälligkeiten festgestellt, sollte die Website als potenziell kompromittiert betrachtet werden.

Wir empfehlen ausdrücklich, die Website aus einer Datensicherung wiederherzustellen, die nachweislich vor dem Sicherheitsvorfall erstellt wurde. Empfohlen wird die Wiederherstellung eines vollständigen, unkomprimierten Backups der Website-Dateien und der Datenbank.

Nach der Wiederherstellung sollten:

- JCE entfernt oder aktualisiert werden
- alle Benutzerkonten überprüft werden
- alle Administrator-Passwörter geändert werden
- Zwei-Faktor-Authentifizierung aktiviert werden
- die Website auf korrekte Funktion geprüft werden
- die Website verstärkt überwacht werden

Bei einer manuellen Suche und Entfernung von Schaddateien besteht die Gefahr, dass eine übersehene Datei sofort wieder zur Infektion führen kann.

Bewahren Sie die verdächtigen Dateien, am besten eine vollständige Sicherung, bis zur Klärung des Vorfalls auf und löschen Sie diese nicht vorschnell. Sie können wichtige Hinweise auf Art und Umfang einer Kompromittierung liefern.

Schritt 5: Benutzerkonten absichern

Wir empfehlen dringend:

- Zwei-Faktor-Authentifizierung (2FA) für alle Administratoren aktivieren
- Zwei-Faktor-Authentifizierung (2FA) für alle Redakteure aktivieren
- starke und individuelle Passwörter verwenden
- nicht mehr benötigte Benutzerkonten löschen

Wann sollten Sie Hilfe anfordern?

Bitte wenden Sie sich an Ihren technischen Dienstleister, wenn:

- JCE installiert ist und Sie die Prüfung nicht selbst durchführen können
- unbekannte Dateien gefunden werden
- unbekannte Benutzerkonten vorhanden sind
- Sie keinen Zugriff auf Hosting oder Datensicherungen haben
- Sie unsicher sind, ob Ihre Website betroffen ist

Checkliste – Kurzfassung

- ☐ Im Joomla-Backend prüfen, ob JCE installiert ist
- ☐ Benutzerkonten auf unbekannte Benutzer prüfen
- ☐ Verzeichnisse images, tmp, media und administrator kontrollieren
- ☐ Auf unbekannte oder neu angelegte PHP-Dateien achten
- ☐ Verdächtige Dateien dokumentieren
- ☐ Aktuelle Datensicherung erstellen
- ☐ JCE deinstallieren und TinyMCE als Standard-Editor aktivieren

  oder ☐ JCE aktualisieren
- ☐ Nicht davon ausgehen, dass durch Entfernung oder Aktualisierung des JCE bereits abgelegte Schaddateien entfernt werden
- ☐ Bei Auffälligkeiten Website aus einem sauberen Backup wiederherstellen
- ☐ Administrator-Passwörter ändern
- ☐ Zwei-Faktor-Authentifizierung für Administratoren aktivieren
- ☐ Zwei-Faktor-Authentifizierung für Redakteure aktivieren
- ☐ Website in den folgenden Wochen verstärkt überwachen
- ☐ Bei Unsicherheiten technischen Dienstleister kontaktieren

Autor:

DMT direktmarketingtool.de GmbH
Osterbergweg 2
93059 Regensburg