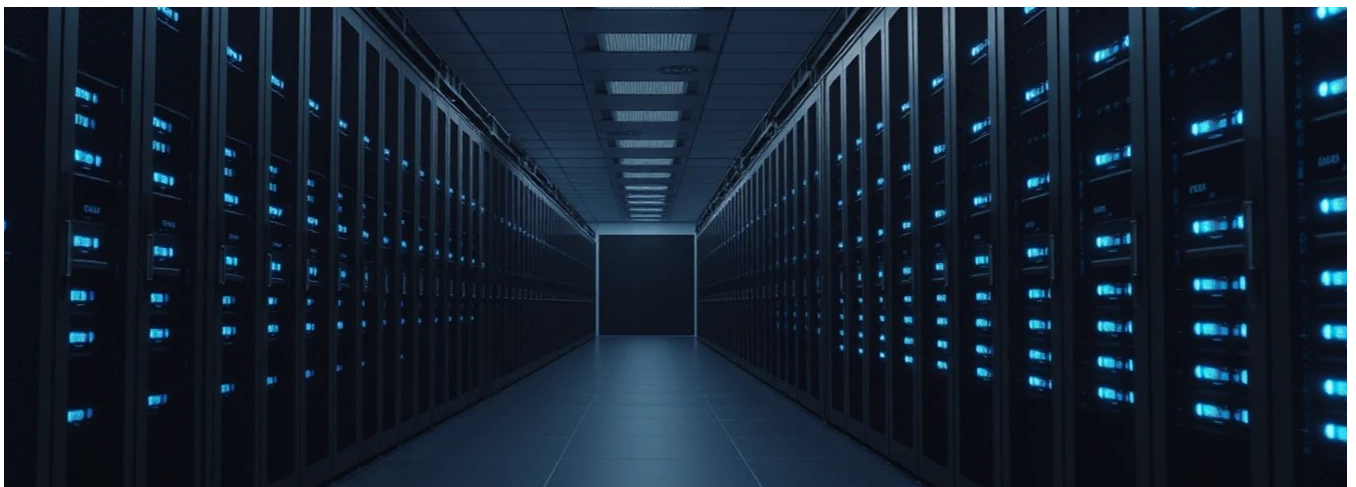


ÖSTERREICH UND DEUTSCHLAND / ARTIKEL MIT ARBEITSBOGEN

Kritische PHP-Lücke im Oktober 2026: Was passiert ist und wie du deine Webseite schützt

Zwei kritische PHP-Lücken erlauben Angriffe ohne Anmeldung. So prüfst du, ob deine Webseite betroffen ist, und was jetzt zu tun ist.

Recherche und Quellenstand: 22.10.2026.



Titelmotiv: KI-generiertes Symbolbild. Kein konkretes Immobilienangebot.

Am 21. Oktober 2026 hat das PHP-Projekt zwei kritische Sicherheitslücken geschlossen. Über sie können Angreifer ohne Anmeldung eigenen Programmcode auf einem Webserver ausführen. Viele Webseiten von Immobilienanbietern laufen mit WordPress, Joomla, TYPO3 oder Contao, und alle diese Systeme brauchen PHP. Hier erfährst du, was passiert ist, wie du herausfindest, ob deine Seite betroffen ist, und was du jetzt tun solltest.

Was passiert ist

PHP ist die Programmiersprache, mit der ein großer Teil aller Webseiten auf dem Server arbeitet. Am 20. Oktober 2026 kündigte das PHP-Sicherheitsteam ein dringendes Update an. Beide Lücken bewertete es mit 9,2 von 10 Punkten (CVSS 4.0) [S2]. Am 21. Oktober folgten die Updates zusammen mit einer Sicherheitswarnung [S1]:

- **CVE-2026-109618:** Wenn PHP der Speicher ausgeht, kann es eine Anfrage mitten im Aufbau abbrechen. Beim anschließenden Aufräumen werden halb fertige Daten als gültig behandelt [S1][S6].
- **CVE-2026-109619:** Daten einer früheren Anfrage bleiben im Speicher stehen, nachdem der Speicher bereits freigegeben wurde. Eine spätere Anfrage an denselben Server-Prozess kann sie wiederverwenden [S1][S3].

Im schlimmsten Fall führt ein Angreifer eigenen Code mit den Rechten des Webservers aus. Über eine der beiden Lücken kann er außerdem Speicherinhalte auslesen [S3]. Wer so auf einen Server kommt, kann etwa Inhalte verändern oder Schadsoftware ablegen (redaktionelle Erläuterung).

Betroffen sind alle üblichen Arten, wie PHP auf dem Server eingebunden ist: PHP-FPM, Apache mit mod_php, php-cgi, FrankenPHP und LiteSpeed [S1]. Welche Art bei dir läuft, weiß dein Hoster. Am größten ist die Gefahr laut

PHP-Projekt bei Apache mit mod_php. Dort reicht nachweislich eine Anfrage ohne Anmeldung, und der Angriff greift, bevor die eigentliche Webseite überhaupt geladen wird [S1].

Die beiden Lücken werden auch „PHP2Shell“ genannt. Amazon registrierte am 17. Oktober, also vor der Veröffentlichung, einen ersten Angriffsversuch auf eine eigene Köder-Anlage. Seit dem Tag der Updates werden die Lücken nach Angaben von Amazon breit ausgenutzt [S5][S9]. Das PHP-Projekt selbst macht dazu keine Angaben [S3]. Die britische Cybersicherheitsbehörde NCSC rät: Wer nicht sofort aktualisieren und auch keine Übergangseinstellungen setzen kann, sollte erwägen, das System bis dahin vom Netz zu nehmen [S4].

Was in Österreich und Deutschland passiert ist

In Österreich hat CERT.at die Warnung verbreitet, abgestimmt mit dem neuen Bundesamt für Cybersicherheit [S3][S8]. Die Webseiten der Universität Wien, der TU Wien und der NÖN waren zeitweise nicht erreichbar [S8]. Der österreichische Cloud-Anbieter Anexia bestätigte Angriffsversuche auf Webseiten, die bei ihm laufen [S8]. Laut Cloudflare stiegen die Angriffsversuche nach der Veröffentlichung von einigen Tausend auf Millionen [S8].

In Deutschland hat das Bundesamt für Sicherheit in der Informationstechnik (BSI) eine Cybersicherheitswarnung herausgegeben [S10]. Mehrere Kommunen, Behörden, Universitäten und Krankenhäuser nahmen ihre Webseiten vorsorglich vom Netz, darunter die Stadt Mainz und die Berliner Charité [S11][S12].

Welche Versionen sicher sind

Geschlossen sind die Lücken in diesen Versionen [S1][S3]:

- **PHP 8.5:** 8.5.12
- **PHP 8.4:** 8.4.27
- **PHP 8.3:** 8.3.36
- **PHP 8.2:** 8.2.35
- **PHP 8.1 und älter (auch 8.0 und 7.x):** keine fertigen Updates mehr

PHP 8.1 und ältere Versionen bekommen vom PHP-Projekt keine Updates mehr. Für 7.4, 8.0 und 8.1 gibt es nur minimale Notkorrekturen für Fachleute, die PHP selbst aus dem Quellcode bauen. Manche Linux-Distributionen liefern für alte Versionen eigene Korrekturen [S1][S3]. Läuft deine Seite noch auf PHP 8.1 oder älter, ist ein Umstieg auf eine unterstützte Version der sichere Weg [S3]. Auch PHP 8.2 erhält nur noch bis 31. Dezember 2026 Sicherheitsupdates [S1][S3].

Wichtig: Linux-Distributionen und Langzeit-Anbieter haben die Korrekturen vorab bekommen und spielen sie teilweise ein, ohne die Versionsnummer zu ändern [S1][S3]. Eine niedrigere Nummer bedeutet also nicht automatisch, dass deine Seite ungeschützt ist. Sicher weißt du es erst, wenn dein Hoster das Update bestätigt.

Bin ich betroffen? So findest du es heraus

Betroffen sein kannst du, wenn deine Webseite mit PHP läuft. Geschützt ist sie, wenn eine der oben genannten Versionen läuft oder dein Hoster bestätigt, dass die Korrektur eingespielt ist. Wer das prüft, hängt davon ab, wer deine Seite betreibt (redaktionelle Empfehlung):

- **Gehostete Komplettlösung** (Baukasten oder eine Anbieter-Webseite deines Immobilien-Softwareherstellers): Hier ist der Betreiber für den Server zuständig. Frag nach, ob das Update eingespielt ist.
- **Eigenes Webhosting mit WordPress, Joomla, TYPO3 oder Contao:** Die PHP-Version siehst du meist im Kundenbereich deines Hosters, oft unter „PHP-Version“ oder „PHP-Einstellungen“.

- Bei WordPress steht die PHP-Version auch im Dashboard unter **Werkzeuge → Website-Zustand → Bericht**, im Abschnitt **Server** [S7]. Auf derselben Seite warnt WordPress außerdem vor sehr alten PHP-Versionen [S7]. Ob das Oktober-Update eingespielt ist, erkennst du an dieser Warnung aber nicht.
- **Webagentur oder eigener Server:** Frag schriftlich nach, welche PHP-Version läuft und wann das Update eingespielt wurde.

Weil Distributionen und Langzeit-Anbieter die Korrekturen vorab bekamen [S1], konnten viele Hoster schnell aktualisieren. Ob das bei deinem Server passiert ist, weißt du aber erst nach einer Rückfrage.

Was du jetzt tun solltest

1. **Update einspielen lassen.** Nur ein Update auf eine der oben genannten Versionen behebt beide Lücken vollständig [S1][S3]. Das Sicherheitsupdate innerhalb einer Versionsreihe spielt in der Regel der Hoster ein. Selbst umstellen kannst du im Kundenbereich meist nur die Versionsreihe, etwa von 8.1 auf 8.3 (redaktionelle Empfehlung).
2. **Alte PHP-Versionen ersetzen.** Bei PHP 8.1 oder älter auf eine unterstützte Version wechseln. Prüfe vorher mit deiner Agentur, ob Theme und Erweiterungen damit laufen, und mach eine Sicherung (redaktionelle Empfehlung).
3. **Wenn es nicht sofort geht:** Das PHP-Projekt nennt Übergangseinstellungen für den Server, etwa ``session.upload_progress.enabled=0`` sowie Anpassungen bei Speicher- und Upload-Einstellungen. Sie ersetzen das Update ausdrücklich nicht und gehören in die Hände deines Hosters oder deiner Agentur [S1][S3]. Ist auch das nicht möglich, erwäge, die Seite bis zum Update vom Netz zu nehmen [S4].
4. **Auf Einbruchsspuren prüfen lassen.** Da die Lücken schon vor dem 21. Oktober angegriffen wurden, sollte dein Hoster oder deine Agentur Protokolle und Dateien ab dem 17. Oktober auf ungewöhnliche Änderungen ansehen [S4][S5].
5. **Weitere Updates nicht vergessen.** Halte auch dein Content-Management-System, Themes und Erweiterungen aktuell, am besten mit automatischen Updates (redaktionelle Empfehlung, vgl. [S3]).

Typische Fehler (redaktionelle Empfehlung)

- „Mein WordPress ist aktuell, also bin ich sicher.“ WordPress-Updates aktualisieren nicht PHP. PHP läuft auf dem Server und wird dort aktualisiert.
- „Die Seite ist klein, die greift keiner an.“ Solche Angriffe laufen automatisiert und durchsuchen das ganze Internet. Amazon sah erste Angriffe auf seine Köder-Anlagen wenige Stunden nach den Updates (vgl. [S5]).
- „Ich verstecke einfach die Fehlermeldungen.“ Das schützt nicht. Fehler auszublenden reicht laut PHP-Projekt ausdrücklich nicht aus [S1][S3].

Vorlage für die Anfrage an Hoster oder Agentur

Fiktives Beispiel für eine kurze Mail:

Betreff: PHP-Sicherheitsupdate vom 21.10.2026 für [Domain]

Hallo, welche PHP-Version läuft auf unserer Webseite [Domain]? Ist das Sicherheitsupdate vom 21.10.2026 eingespielt, also PHP 8.2.35, 8.3.36, 8.4.27 oder 8.5.12, oder die Korrektur über das Paket eurer Linux-Distribution? Falls noch PHP 8.1 oder älter läuft: Bis wann kann die Seite auf eine unterstützte Version umgestellt werden? Bitte prüft auch, ob es seit dem 17.10.2026 Hinweise auf einen Einbruch gibt. Danke!

DEIN ARBEITSBOGEN

Aus dem Lesen wird ein nächster Schritt

Für den eigenen Fall ausfüllen. Die Felder strukturieren deine Vorbereitung; sie bestätigen keine rechtliche, technische oder finanzielle Prüfung.

01 / Webseite und Domain

Notiere die Adresse deiner Webseite und, falls vorhanden, weitere Domains, die auf dieselbe Seite zeigen.

02 / Wer betreibt sie

Trag ein, wer für den Server zuständig ist: Hostler, Webagentur, Softwareanbieter oder du selbst, mit Ansprechperson.

03 / System der Webseite

Halte fest, womit die Seite gebaut ist, zum Beispiel WordPress, Joomla, TYPO3, Contao oder ein Baukasten.

04 / Aktuelle PHP-Version

Notiere die PHP-Version aus dem Hosting-Kundenbereich oder aus WordPress unter Website-Zustand, Bereich Server.

05 / Update eingespielt

Vermerke, ob 8.2.35, 8.3.36, 8.4.27 oder 8.5.12 läuft, wer es bestätigt hat und wann.

06 / Umstieg nötig

Läuft noch PHP 8.1 oder älter, notiere, wer den Umstieg plant und ob Theme und Erweiterungen dafür geprüft sind.

07 / Prüfung auf Einbruch

Halte fest, ob Hostler oder Agentur Protokolle und Dateien auf ungewöhnliche Änderungen geprüft haben und mit welchem Ergebnis.

08 / Sicherung und Updates

Notiere, wo die letzte Sicherung liegt und ob System, Themes und Erweiterungen automatisch aktualisiert werden.

QUELLEN UND GRENZEN

Nachlesen und richtig einordnen

[S1] [Security advisory: Critical remote code execution vulnerabilities, update now](#)

. Abruf am 22.10.2026.

[S2] [Upcoming Critical PHP Security Release](#)

. Abruf am 22.10.2026.

[S3] [Kritische Sicherheitslücken in PHP – Updates verfügbar](#)

. Abruf am 22.10.2026.

[S4] [Critical security issue affecting PHP](#)

. Abruf am 22.10.2026.

[S5] [Amazon threat intelligence identifies PHP2Shell exploitation prior to public disclosure in MadPot](#)

. Abruf am 22.10.2026.

[S6] [GHSA-w8hw-w9fx-j79w – RCE via OOM corruption \(CVE-2026-109618\)](#)

. Abruf am 22.10.2026.

[S7] [Site Health screen](#)

. Abruf am 22.10.2026.

[S8] [PHP-Lücke: Millionen Angriffsversuche im Netz](#)

. Abruf am 22.10.2026.

[S9] [„PHP2Shell“ angeblich schon Tage vor Bekanntmachung ausgenutzt](#)

. Abruf am 22.10.2026.

[S10] [PHP – Kritische Schwachstellen bedrohen Webanwendungen weltweit](#)

. Abruf am 22.10.2026.

[S11] [Programmiersprache PHP: Sicherheitslücke bedroht weltweit Webseiten](#)

. Abruf am 22.10.2026.

[S12] [PHP-Lücke: Gravierende Sicherheitslücke bedroht weltweit Webseiten](#)

. Abruf am 22.10.2026.

Über dieses Dokument

Mit Unterstützung von KI erstellt. Quellenfakten sind extern belegt; Beispiele, Arbeitsbogen und organisatorische Empfehlungen sind redaktionelle Einordnungen.

Inhalte wurden sorgfältig vorbereitet. Fehler, unvollständige Angaben und spätere Änderungen können dennoch nicht ausgeschlossen werden. Keine individuelle Rechts-, Steuer-, Finanzierungs- oder Bewertungsberatung. Maßgeblich sind die konkreten Umstände und die einschlägigen aktuellen Vorschriften. Bei verbindlichen Entscheidungen fachkundige Beratung einholen. Gesetzliche Verantwortung lässt sich nicht pauschal durch diesen Hinweis ausschließen.

Dokument-ID: WS26-IT-001-DL | Revision 2 | Land/Zielgruppe: Österreich und Deutschland | Redaktion: immosearch.eu | Stand: 22.10.2026.