PHP-Sicherheitslücke vom 21.10.2026: in zehn Minuten prüfen

Für Praxis-Websites mit WordPress, TYPO3 oder Joomla · Stand: 12.11.2026

---

1. **Welches System?** Baukasten (Wix, Jimdo, Squarespace): nichts zu tun. WordPress, TYPO3, Joomla: weiter.
2. **PHP-Version nachsehen.** WordPress: Werkzeuge → Website-Zustand → Bericht → Server. Sonst im Kundenmenü des Hosters. Das Update vom 21.10.2026 trägt die Nummer 8.5.12, 8.4.27, 8.3.36 oder 8.2.35, oder eine höhere derselben Reihe.
3. **Den Hoster fragen** (Vorlage unten).
4. **PHP 8.1 oder älter:** Wechsel auf 8.3+ planen, Theme und Erweiterungen prüfen lassen.
5. **PHP 8.2:** läuft am 31.12.2026 aus, das Upgrade gleich mit einplanen.
6. **Verdacht auf Angriff und Formulare mit personenbezogenen Daten (etwa Terminanfragen):** Hoster informieren, Datenschutzbeauftragte einbeziehen, falls vorhanden. Eine Datenpanne meldet die Praxis unverzüglich und möglichst binnen 72 Stunden ab Kenntnis der Datenschutz-Aufsichtsbehörde, außer sie führt voraussichtlich nicht zu einem Risiko für die Rechte und Freiheiten der Betroffenen (Art. 33 DSGVO). Bei voraussichtlich hohem Risiko sind auch die Betroffenen unverzüglich zu benachrichtigen (Art. 34 DSGVO). Allgemeiner Hinweis, keine Rechtsberatung.
7. **Wer spielt bei Ihnen Updates ein?** Wenn niemand: Ihre Agentur, ein Bekannter oder ich.

Mail-Vorlage für Ihren Hoster

Betreff: PHP-Sicherheitsupdate vom 21.10.2026 (CVE-2026-109618 / CVE-2026-109619)

Guten Tag,

meine Website [Domain] liegt in Ihrem Paket [Paketname]. Bitte bestätigen Sie mir kurz:

1. welche PHP-Version aktiv ist,
2. ob das Sicherheitsupdate vom 21.10.2026 eingespielt ist,
3. ob Ihnen Hinweise auf eine Kompromittierung meines Pakets vorliegen.

Vielen Dank und freundliche Grüße
[Name, Praxis]

Zuständigkeit Praxis-Website – zum Abheften im QM-Ordner

Stand der Vorlage: 12.11.2026

Damit niemand suchen muss, wenn es eilt: einmal ausfüllen, abheften und beim nächsten Kontrolltermin aktualisieren.

Angabe	Eintrag
Website-Adresse	
System (z. B. WordPress, TYPO3, Joomla, Baukasten)	
PHP-Version	_____ geprüft am _____
Hoster	_____ Kundennummer _____
Updates spielt ein (Name, Telefon oder E-Mail)	
Zugangsdaten liegen hier (nur den Ort notieren, nicht die Zugangsdaten selbst, z. B. „Passwortmanager der Praxis“)	
Nächster Kontrolltermin	
Datenschutzbeauftragte:r, falls vorhanden	

Kontrollen

Datum	PHP-Version	geprüft von	Bemerkung

Ausgefüllt am _____ von _____