

PHP2Shell-Checkliste für TYPO3

So prüfst du in wenigen Minuten, ob deine TYPO3-Website von der kritischen PHP-Lücke betroffen ist, und was du jetzt Schritt für Schritt tun musst.

Kurz erklärt

PHP2Shell sind zwei kritische Lücken im PHP-Kern (CVE-2026-109618 und CVE-2026-109619, je 9,2 von 10 nach CVSS 4.0). Angreifer können ohne Login, ohne Passwort und ohne dein Zutun eigenen Code auf dem Server ausführen und Speicher auslesen, zum Beispiel Passwörter, Tokens oder API-Schlüssel. Das BSI hat am 21.10.2026 die Warnstufe Orange ausgerufen und rechnet mit großflächigen Angriffen binnen weniger Stunden.

Stell dir PHP wie den Motor vor und TYPO3 wie das Auto obendrauf. Der Fehler steckt im Motor. Deshalb hilft **kein** Update im TYPO3-Backend, sondern nur ein PHP-Update auf dem Server.

Sichere PHP-Versionen

PHP-Zweig	Sicher ab Version	Hinweis
PHP 8.5	8.5.12	offiziell gepatcht
PHP 8.4	8.4.27	offiziell gepatcht, gutes Ziel
PHP 8.3	8.3.36	offiziell gepatcht, gutes Ziel (8.3.6 ist nicht sicher)
PHP 8.2	8.2.35	gepatcht, Sicherheitssupport endet am 31.12.2026
PHP 7.4, 8.0, 8.1	kein offizielles Release	End of Life, nur Quellcode-Backports; Pakete nur über Distribution, LTS-Anbieter oder Hoster
PHP 7.3 und älter	kein Fix	dringend aktualisieren

Entscheidend ist die **ganze** Versionsnummer. Pakete von Linux-Distributionen können den Fix auch unter einer älteren Nummer enthalten: dann im Changelog nach CVE-2026-109618 und CVE-2026-109619 suchen oder den Hoster fragen.

Wo läuft deine Seite?

Webhosting-Paket (IONOS, Strato, All-Inkl u. a.): Hoster spielt das Update ein. Du prüfst die Version und lässt dir den Patch schriftlich bestätigen. **Eigener Server, vServer, Docker**: du bist selbst dran, und zwar heute. **Agentur betreut**: anrufen oder mailen, Version und Patch schriftlich bestätigen lassen.

1 PHP-Version prüfen

- ☐ Als **Admin** ins TYPO3-Backend einloggen. Oben rechts auf das Symbol **System-Information** klicken. Dort steht die PHP-Version.
- ☐ Alternativ: **Admin-Tools** → **Umgebung (Environment)** → **Environment Status**.
- ☐ Vollständige Nummer mit der Tabelle auf Seite 1 vergleichen.

Achtung: Der Hinweis „Dein System ist voll funktionsfähig“ bezieht sich **nicht** auf diese Lücke. PHP 8.3.6 wird dort zum Beispiel als funktionsfähig angezeigt, ist aber nicht sicher. Sicher wäre 8.3.36. Du bist nur Redakteur? Dann frag deine Agentur.

Beim Hoster nachsehen (Beispiel IONOS)

Kundenkonto: **Menü** → **Hosting** → **Kachel PHP** → **Öffnen**. Dort siehst du die PHP-Version je Domain. Bei Shared Hosting steht oft nur „8.3“ ohne genaue Nummer. Dann den Patch schriftlich bestätigen lassen (Vorlage unten).

2 Auf PHP 8.3 umstellen (bei 8.1 oder älter)

- ☐ Vorher ein vollständiges **Backup** von Dateien und Datenbank machen.
- ☐ Kompatibilität prüfen: TYPO3 12 und 13 laufen auf PHP 8.2 und 8.3 (TYPO3 13 braucht mindestens 8.2). TYPO3 11 läuft auch auf 8.2 und 8.3, vorher die Erweiterungen prüfen.
- ☐ Im Hoster-Konto auf 8.3 umstellen, am besten zuerst auf einer Subdomain testen.
- ☐ Eigener Server: Pakete aktualisieren bzw. Images neu bauen, danach Apache, PHP-FPM und Worker **neu starten** (nicht nur reload).

Danach testen

- ☐ Startseite und mehrere Unterseiten
- ☐ Kontaktformular (Testanfrage abschicken)
- ☐ Login ins Backend
- ☐ Bei Shops: kompletter Bestellvorgang

Was nicht hilft

- Updates im CMS-Backend und Sicherheits-Plugins: Der Angriff passiert, bevor dein CMS überhaupt lädt.
- „Fix-Plugins“ oder Konfig-Tricks aus Foren (z. B. `memory_limit=-1`, `session.upload_progress.enabled=0`, Uploads am Proxy blocken): Laut PHP-Team blockieren sie nur einzelne Angriffswege.
- Ein Wartungsmodus per Plugin: PHP läuft trotzdem weiter. Offline nehmen heißt auf Server-Ebene, z. B. per `.htaccess-503` oder Passwortschutz beim Hoster.

Zwischenlösung Cloudflare

Läuft deine Seite über Cloudflare, sind laut Cloudflare für bekannte Angriffswege bereits Schutzregeln aktiv, auch im kostenlosen Tarif. Das verschafft dir Zeit, ersetzt das PHP-Update aber nicht und wirkt nur für Traffic, der über Cloudflare läuft.

3 Patch schriftlich bestätigen lassen

Schick diese Vorlage an deinen Hoster oder deine Agentur:

Betreff: PHP2Shell (CVE-2026-109618 / CVE-2026-109619): Bitte Patch-Stand bestätigen

Hallo [Name],

wegen der PHP-Lücke PHP2Shell (BSI-Warnstufe Orange vom 21.10.2026) bitte ich um eine kurze schriftliche Bestätigung für meine Website [Domain]:

1. Welche PHP-Version läuft genau (vollständige Versionsnummer)?
2. Ist das Update auf 8.3.36 bei mir eingespielt (bzw. 8.2.35, 8.4.27, 8.5.12 oder neuer)? Falls ein Distributions-Paket mit älterer Nummer läuft: Enthält es den Fix für beide CVEs?
3. Wurden Apache bzw. PHP-FPM danach neu gestartet?

Bitte bestätigt mir das schriftlich. Danke!

Viele Grüße
[Name]

4 Prüfen, ob schon jemand drin war

Das Update schließt die Tür. Eine Hintertür, die vorher schon platziert wurde, bleibt aber offen.

- ☐ Backend-Benutzer durchgehen: Gibt es Admins, die du nicht kennst?
- ☐ Fremde oder neue PHP-Dateien suchen, besonders in `fileadmin/` und `typo3temp/`.
- ☐ Kürzlich geänderte Template- und Erweiterungsdateien prüfen.
- ☐ Neue Cronjobs auf dem Server kontrollieren.
- ☐ Seltsame Weiterleitungen oder Spam-Seiten? Seite stichprobenartig aufrufen und bei Google mit `site:deine-domain.de` prüfen.

Weitere Warnzeichen laut Wiz und PHP-Team: gehäufte HTTP-500- oder Memory-Limit-Fehler nach ungewöhnlichen Uploads, auffällig große PHPSESSID-Cookies, PHP-Prozesse, die grundlos neu starten.

Bei Verdacht

Seite offline lassen, Logs sichern, ein sauberes Backup von vor dem Angriff einspielen und alle Passwörter und API-Schlüssel ändern. Sind personenbezogene Daten betroffen, muss eine Datenpanne nach Art. 33 DSGVO in der Regel binnen 72 Stunden an die Aufsichtsbehörde gemeldet werden (keine Rechtsberatung).

5 Sonderfall: alte TYPO3-Versionen

TYPO3 10, 9 und älter laufen nur bis PHP 7.4. Du kannst PHP also nicht auf eine sicher gepatchte offizielle Version hochstellen, ohne dass die Website kaputtgeht. Für 7.4 gibt es vom PHP-Projekt kein offizielles Release, nur Quellcode-Backports. Du bist dann komplett davon abhängig, ob dein Hoster selbst einen Patch nachbaut. Hier hilft kein schneller Klick mehr: Plane ein **TYPO3-Upgrade oder einen Relaunch**, und zwar bevor etwas passiert.

Langfristig: weniger Server, weniger Risiko

Wer seine Website selbst hostet, muss schneller patchen, als Angreifer mit KI-Tools neue Lücken ausnutzen. Das schafft kaum ein Unternehmen nebenbei. Deshalb empfehlen wir für die meisten Unternehmenswebsites **Webflow**: Dort gibt es keinen eigenen PHP-Server, den du pflegen musst. Hosting, Server-Updates und Sicherheit übernimmt Webflow. TYPO3 und WordPress sind trotzdem nicht schlecht, wir bauen beides selbst. Wer selbst hostet, ist aber auch selbst verantwortlich.

Deine Kurz-Checkliste

- ☐ PHP-Version im Backend oder beim Hoster geprüft
- ☐ Backup gemacht
- ☐ Bei 8.1 oder älter auf 8.3 umgestellt und getestet
- ☐ Patch schriftlich bestätigt (z. B. 8.3.36)
- ☐ Benutzer, Dateien, Cronjobs und Weiterleitungen geprüft
- ☐ Bei TYPO3 10 oder älter: Upgrade oder Relaunch geplant

Du brauchst Unterstützung?

Wir helfen dir beim PHP-Update, beim TYPO3-Upgrade, beim Relaunch oder beim Umzug zu Webflow. Kurzfristig und ohne Umwege.

Kostenloses Erstgespräch: webwavers.de/kontakt · Ratgeber: webwavers.de/ratgeber/php2shell-php-sicherheitsluecke

Quellen

- BSI, Cyber-Sicherheitswarnung PHP2Shell, 21.10.2026 (bsi.bund.de)
- php.net, offizielle Release-Hinweise zu 8.2.35, 8.3.36, 8.4.27, 8.5.12
- Help Net Security, 21.10.2026: helpnetsecurity.com/2026/10/21/php2shell-php-vulnerabilities-patched-cve-2026-109618-cve-2026-109619/
- The Hacker News: thehackernews.com/2026/10/php-issues-emergency-patches-for-two.html
- Greenbone: greenbone.net/blog/php2shell-php-schwachstelle-patchen-cve-2026-109618-cve-2026-109619/
- Dr. Web: drweb.de/php2shell-update-php-versionen/
- IT-Business/dpa: it-business.de/kritische-php-luecke-php2shell-bsi-warnt-a-c04d323dad5aee01615751ff7f72319b/