

PHP-LÜCKE „PHP2SHELL“: WAS SIE WISSEN MÜSSEN

Eine kritische Lücke betrifft PHP, eine häufig für Websites und Online-Verwaltungstools genutzte Sprache. Seit dem 17. Oktober werden Angriffsversuche beobachtet. Dieser Leitfaden hilft Ihnen zu prüfen, ob Sie betroffen sind und was zu tun ist.

Die Lücke einfach erklärt

- **Noch bevor Ihre Website erscheint**, empfängt PHP die Anfrage des Besuchers (Seite, Formular, Datei-Upload) und bereitet sie im Speicher vor.
- Ein Angreifer sendet eine **manipulierte Anfrage**, die diese Vorbereitung zum „Überlaufen“ bringt. PHP bricht abrupt ab und hinterlässt **halb geordnete** Informationen im Speicher.
- PHP erkennt diese Unordnung nicht und nutzt die Informationen, manchmal erst bei der nächsten Anfrage. Der Angreifer hat sie jedoch vorbereitet: Er hat **eigene Anweisungen** eingeschleust, die PHP schließlich **wie seine eigenen ausführt**.
- Folge: **Ohne Passwort oder Konto** kann er die Website übernehmen: Daten stehlen (Kunden, Bestellungen), Schadsoftware installieren, Spam versenden oder Ihre Besucher umleiten.

Warum das ernst ist: Die Lücke liegt in PHP selbst, nicht in Ihrer Website. Auch eine vollständig aktuelle Website (WordPress, PrestaShop...) bleibt anfällig, solange PHP nicht gepatcht ist.

✓ Ihre TapTap-Bildschirme sind nicht betroffen

- **Ihre Installation nutzt kein PHP.** Die Software zur Steuerung Ihrer Bildschirme und Anzeige Ihrer Inhalte nutzt andere Technologien, die von dieser Lücke nicht betroffen sind.
- **Ihre Installation wird von ihrem Controller gesteuert, einer auf Ihrem Computer installierten Software**, anders als Lösungen, die die Bildschirmverwaltung auf einer Online-Plattform bündeln.
- **Die Player zur Steuerung Ihrer Bildschirme sind aus dem Internet nicht erreichbar.** Sie haben keine öffentliche Adresse: Unsere Teams verwalten sie nur über ein privates, verschlüsseltes Netzwerk.

Für Ihre Bildschirme müssen Sie nichts tun.

⚠ Prüfen Sie aber Ihre Website und Verwaltungstools

Wenn Ihre Website, Ihr Onlineshop oder eines Ihrer Tools PHP nutzt und bei Ihnen oder einem Dienstleister gehostet wird, muss es **sofort** aktualisiert werden. Die folgenden Seiten erklären die Prüfung in zwei Minuten und nennen gepatchte Versionen; die gängigsten Tools stehen im Anhang.

→ **HILFREICH? TEILEN SIE DEN LEITFADEN MIT IHREN KOLLEGEN UND IHREM WEBDIENSTLEISTER.**

KEIN DIENSTLEISTER? BERATUNG NÖTIG?

Unsere Teams helfen Ihnen mit ihrem Fachwissen, **Ihre Website zu schützen** oder begleiten Sie beim **Umstieg auf eine von dieser Lücke nicht betroffene Technologie**, wie **Odoo**.

Kontaktieren Sie uns: sales@taptap.be



KURZ: WAS IST ZU TUN?

1. Ermitteln

Ermitteln Sie Ihre PHP-Tools mit der Methode „So prüfen Sie“ (Seite 2) und der Tool-Liste im Anhang.

2. Kontaktieren

Bitten Sie Ihren Webdienstleister oder Hoster, PHP auf eine gepatchte Version zu aktualisieren.

3. Bestätigen lassen

Lassen Sie sich bei Online-Tools im Abo (SaaS) vom Anbieter bestätigen, dass der Patch angewendet wurde.

SO PRÜFEN SIE, OB IHRE WEBSITE PHP NUTZT

Methode	Vorgehen	Zuverlässigkeit
Dienstleister fragen	„Welche PHP-Version nutzen meine Website und Tools? Ist sie gegen PHP2Shell gepatcht?“	Sicher
Kostenloses Online-Tool	Geben Sie Ihre Webadresse auf builtwith.com oder whatcms.org ein. Erscheint „PHP“, „WordPress“, „WooCommerce“...? Lassen Sie die PHP-Version prüfen: Das Tool zeigt nicht, ob der Patch installiert ist.	Gut
Hinweise in der Adresse	Eine Adresse mit „ php “ oder eine vorhandene Seite ihre-website.be/wp-admin (WordPress).	Hinweis
Keine sichtbaren Hinweise?	Manche Hoster verbergen diese Hinweise. Fehlende Hinweise beweisen nicht, dass Ihre Website kein PHP nutzt.	Ungenügend → nachfragen

GEPATCHTE PHP-VERSIONEN

PHP-Zweig	Erste gepatchte Version	Status
PHP 8.5	8.5.12	Gepatcht
PHP 8.4	8.4.27	Gepatcht
PHP 8.3	8.3.36	Gepatcht
PHP 8.2	8.2.35	Gepatcht Supportende am 31.12.2026
PHP 8.1 und älter	Keine offizielle Version	Support beendet gepatchtes Anbieterpaket (z. B. Ubuntu), danach Migration

Ubuntu: PHP 8.1 (Ubuntu 22.04) wird per einfaches Update gepatcht; PHP 7.4 (Ubuntu 20.04) über **Ubuntu Pro**, kostenlos für bis zu 5 physische Rechner, auch für Firmen (ein Konto pro Firma); darüber kostenpflichtig (ubuntu.com/pro).

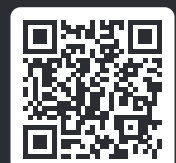
Quellen: offizielle Sicherheitshinweise des PHP-Teams (GHSA-w8hw-w9fx-j79w und GHSA-6wmf-4rv5-p3rp, veröffentlicht am 21. Oktober 2026), php.net und Ubuntu USN-8948-1/-2. Nach dem Update muss der Dienst, der PHP ausführt, neu gestartet werden (siehe Checkliste, Seite 3).

→ HILFREICH? TEILEN SIE DEN LEITFADEN MIT IHREN KOLLEGEN UND IHREM WEBDIENSTLEISTER.

KEIN DIENSTLEISTER? BERATUNG NÖTIG?

Unsere Teams helfen Ihnen mit ihrem Fachwissen, **Ihre Website zu schützen** oder begleiten Sie beim **Umstieg auf eine von dieser Lücke nicht betroffene Technologie**, wie **Odoo**.

Kontaktieren Sie uns: sales@taptap.be



VERWALTEN SIE IHR HOSTING SELBST?

Checkliste für Ihren IT-Fachmann oder Serververwalter (VPS, dedizierter Server, cPanel, Plesk, Docker...).

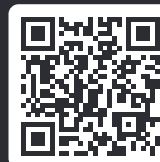
Schritt	Was ist zu tun?
☐ 1. Tatsächlich genutzte Version prüfen	Der Befehl <code>php -v</code> reicht nicht: Prüfen Sie die tatsächlich für jede Website genutzte Version (die des Webserver: PHP-FPM, Apache, LiteSpeed...). Bei cPanel oder Plesk kann jede Domain ihre eigene Version haben.
☐ 2. PHP aktualisieren	Auf 8.2.35, 8.3.36, 8.4.27, 8.5.12 oder neuer, oder auf ein gepatchtes Paket des Anbieters (auch für 8.1 und älter). • Distributionspakete (Ubuntu, Debian, Red Hat, AlmaLinux...): Der Patch wird oft ohne Änderung der Versionsnummer eingebaut; prüfen Sie, ob CVE-2026-109618 und CVE-2026-109619 im Änderungsprotokoll des Pakets stehen. • cPanel / Plesk: Update über das Panel. • Docker: Image auf gepatchter PHP-Basis neu bauen und erneut bereitstellen.
☐ 3. PHP neu starten	Starten Sie den Dienst neu, der PHP auf Ihrem Server ausführt: meist PHP-FPM , sonst Apache (mod_php), LiteSpeed , FastCGI, FrankenPHP... Bei einem Docker -Container das Image neu bauen und bereitstellen. Fragen Sie im Zweifel Ihren Hoster. Prüfen Sie danach, ob keine alten PHP-Prozesse mehr laufen: Sonst bedient die alte Version weiterhin Ihre Websites.
☐ 4. Update nicht sofort möglich?	Übergangsmaßnahmen in der Server- oder Poolkonfiguration erzwingen, von Websites nicht änderbar (keine <code>.user.ini</code>): • <code>memory_limit = -1</code> mit externer Speichergrenze (Container, cgroup), nie <code>RLIMIT_AS/DATA</code>; • <code>session.upload_progress.enabled = 0</code>; bei PHP 8.5 auch <code>fatal_error_backtraces = 0</code>; • Anfrage- und Uploadgröße auf Webserverebene begrenzen; • PHP-FPM: <code>pm.max_requests = 1</code>, falls die Leistung es zulässt. Dann alle PHP-Prozesse neu starten . Diese Maßnahmen senken das Risiko, ersetzen aber kein gepatchtes PHP.
☐ 5. Angriffsfläche reduzieren	PHP nur über den Hauptwebserver erreichbar (kein Apache oder PHP auf einem zusätzlichen, zum Internet offenen Port); keine vom Webserver bei jeder Anfrage übergebenen PHP-Parameter (<code>PHP_VALUE</code>); <code>phpinfo</code> -Dateien löschen; phpMyAdmin und Verwaltungspanels nur für vertrauenswürdige Adressen oder über ein VPN zugänglich machen.
☐ 6. Angriffsspuren suchen	Seit dem 17. Oktober: POST-Anfragen mit <code>PHP_SESSION_UPLOAD_PROGRESS</code> in Protokollen; neue oder unbekannte <code>.php</code> -Dateien in Webverzeichnissen; unbekannte Prozesse, gestartet vom Webserverbenutzer. Fehler „Allowed memory size exhausted“ können auf Versuche hindeuten; ihr Fehlen beweist nicht, dass alles in Ordnung ist. Ziehen Sie im Zweifel einen Spezialisten hinzu.

→ HILFREICH? TEILEN SIE DEN LEITFADEN MIT IHREN KOLLEGEN UND IHREM WEBDIENSTLEISTER.

KEIN DIENSTLEISTER? BERATUNG NÖTIG?

Unsere Teams helfen Ihnen mit ihrem Fachwissen, **Ihre Website zu schützen** oder begleiten Sie beim **Umstieg auf eine von dieser Lücke nicht betroffene Technologie**, wie **Odoo**.

Kontaktieren Sie uns: sales@taptap.be



ANHANG: GÄNGIGE TOOLS AUF PHP-BASIS

Wenn sie **bei Ihnen oder einem Dienstleister gehostet werden**, sind sie möglicherweise betroffen und müssen aktualisiert werden.

Was ist zu tun? Kontaktieren Sie Ihren Dienstleister (Webdienstleister, Hoster oder Entwickler), um PHP aktualisieren zu lassen. Er kennt Ihre Anwendung bestens und ist dafür am besten geeignet.

- AbanteCart (Onlineshop)
- Akaunting (Buchhaltung)
- Akeneo (Produktkatalog)
- Amelia (Buchung, WordPress-Plugin)
- Bagisto (Onlineshop)
- Bolt CMS (Website)
- Bookly (Buchung, WordPress-Plugin)
- BookStack (interne Dokumentation)
- Cacti (Netzwerküberwachung)
- CakePHP (individuelle Entwicklung)
- Chamilo (Online-Schulungen)
- CiviCRM (CRM für Vereine)
- Codelgniter (individuelle Entwicklung)
- Concrete CMS (Website)
- Contact Form 7 (Formulare, WordPress-Plugin)
- Contao (Website)
- Craft CMS (Website)
- CubeCart (Onlineshop)
- DokuWiki (Wiki)
- Dolibarr (ERP / CRM)
- Drupal (Website)
- Elementor (Seitenerstellung, WordPress)
- EspoCRM (CRM)
- FacturaScripts (Rechnungsstellung)
- FreeScout (Kundensupport)
- FrontAccounting (Buchhaltung)
- GLPI (IT-Bestand / Support)
- Grav (Website)
- Gravity Forms (Formulare, WordPress-Plugin)
- Horde (Webmail)
- Houzez (Immobilien-Theme, WordPress)
- Ibexa (eZ Platform) (Website)
- Invoice Ninja (Rechnungsstellung)
- InvoicePlane (Rechnungsstellung)
- Joomla (Website)
- Kanboard (Projektverwaltung)
- Kimai (Zeiterfassung)
- Kirby (Website)
- Laravel (individuelle Entwicklung)
- Leantime (Projektverwaltung)
- LimeSurvey (Umfragen)
- LiteCart (Onlineshop)
- **Magento / Adobe Commerce** (Onlineshop)
- MantisBT (Ticketverfolgung)
- Matomo (Webstatistiken)
- Mautic (Marketingautomatisierung)
- MediaWiki (Wiki)
- MODX (Website)
- Moodle (Online-Schulungen)
- Nextcloud (Dateifreigabe)
- October CMS (Website)
- Open Real Estate (Immobilienwebsite)
- **OpenCart** (Onlineshop)
- OpenEMR (Patientenakte)
- OroCommerce (B2B-E-Commerce)
- OroCRM (CRM)
- osTicket (Kundensupport)
- ownCloud Server (Dateifreigabe)
- phpBB (Forum)
- phpList (Newsletter)
- **phpMyAdmin** (Datenbankverwaltung)
- Pimcore (Produktkatalog / Medien)
- Piwigo (Fotogalerie)
- **PrestaShop** (Onlineshop)
- ProcessWire (Website)
- RealHomes (Immobilien-Theme, WordPress)
- **Roundcube** (Webmail)
- Sendy (Newsletter)
- **Shopware** (Onlineshop)
- SilverStripe (Website)
- Simple Machines Forum (Forum)
- SnappyMail / RainLoop (Webmail)
- Snipe-IT (IT-Bestand)
- SquirrelMail (Webmail)
- Statamic (Website)
- SugarCRM (CRM)
- SuiteCRM (CRM)
- Sulu (Website)
- Sylius (Onlineshop)
- **Symfony** (individuelle Entwicklung)
- Thelia (Onlineshop)
- Vtiger (CRM)
- WHMCS (Hosting-Abrechnung)
- **WooCommerce** (Onlineshop, WordPress)
- **WordPress** (Website)
- WP Residence (Immobilien-Theme, WordPress)
- WPForms (Formulare, WordPress-Plugin)
- Yii (individuelle Entwicklung)
- Zabbix (Überwachung, Weboberfläche)
- Zen Cart (Onlineshop)

... sowie **alle WordPress-Themes und -Plugins** und jede in PHP individuell entwickelte Anwendung. **Fett:** die verbreitetsten Tools.

Dieser Leitfaden bietet allgemeine Informationen mit Stand vom 22. Oktober 2026. Er ist kein Sicherheitsaudit Ihrer Systeme. Die genannten Produktnamen gehören ihren jeweiligen Eigentümern und dienen nur dazu, betroffene Technologien zu erkennen.

→ **HILFREICH? TEILEN SIE DEN LEITFADEN MIT IHREN KOLLEGEN UND IHREM WEBDIENSTLEISTER.**

KEIN DIENSTLEISTER? BERATUNG NOTIG?

Unsere Teams helfen Ihnen mit ihrem Fachwissen, **Ihre Website zu schützen** oder begleiten Sie beim **Umstieg auf eine von dieser Lücke nicht betroffene Technologie**, wie **Odoo**.

Kontaktieren Sie uns: **sales@taptap.be**

