

PHP-LEK "PHP2SHELL": WAT U MOET WETEN

Een kritiek lek treft PHP, een taal die veel wordt gebruikt voor websites en online beheertools. Sinds 17 oktober worden uitbuitingspogingen waargenomen. Deze gids helpt u na te gaan of u getroffen bent en wat u kunt doen.

Het lek eenvoudig uitgelegd

- **Nog vóór uw website verschijnt**, ontvangt PHP het verzoek van de bezoeker (een pagina, formulier of bestandsupload) en bereidt het voor in het geheugen.
- Een aanvaller stuurt een **gemanipuleerd verzoek** om die voorbereiding te laten "overlopen". PHP stopt abrupt en laat informatie **half geordend** achter in het geheugen.
- PHP merkt die wanorde niet op en gebruikt de informatie, soms bij het volgende verzoek. De aanvaller heeft die echter voorbereid: hij heeft er **zijn eigen instructies** in verwerkt, die PHP uiteindelijk **als de zijne uitvoert**.
- Gevolg: **zonder wachtwoord of account** kan hij de website overnemen: gegevens stelen (klanten, bestellingen), malware installeren, spam versturen of uw bezoekers omleiden.

Waarom dit ernstig is: het lek zit in PHP zelf, niet in uw website. Een volledig bijgewerkte website (WordPress, PrestaShop...) blijft kwetsbaar zolang PHP niet is gepatcht.

✓ Uw TapTap-schermen zijn niet getroffen

- **Uw installatie gebruikt geen PHP.** De software die uw schermen aanstuurt en uw inhoud weergeeft, berust op andere technologieën die niet door dit lek worden getroffen.
- **Uw installatie wordt aangestuurd door haar controller, software geïnstalleerd op uw computer,** anders dan oplossingen die het schermbeheer centraliseren op een online platform.
- **De players die uw schermen aansturen, zijn niet bereikbaar via het internet.** Ze hebben geen publiek adres: onze teams beheren ze uitsluitend via een privénetwerk met versleuteling.

Voor uw schermen hoeft u niets te doen.

⚠ Controleer wel uw website en beheertools

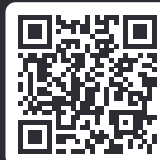
Als uw website, webshop of een van uw tools PHP gebruikt en bij u of een dienstverlener gehost wordt, moet die **onmiddellijk** bijgewerkt worden. De volgende pagina's leggen uit hoe u dit in twee minuten controleert en vermelden de gepatchte versies; de meest gebruikte tools staan in de bijlage.

→ WAS DEZE GIDS NUTTIG VOOR U? BEZORG HEM AAN UW COLLEGA'S EN UW WEBDIENSTVERLENER.

GEEN DIENSTVERLENER, OF NOOD AAN ADVIES?

Onze teams kunnen u met hun expertise helpen **uw website te beschermen** of u begeleiden bij de **migratie naar een technologie die niet door dit lek wordt getroffen**, zoals Odoo.

Contacteer ons: sales@taptap.be



KORT: WAT MOET U DOEN?

1. Identificeren

Vind uw PHP-tools via de methode "Hoe weet u" (pagina 2) en de lijst met tools in de bijlage.

2. Contacteren

Vraag uw webdienstverlener of hostingprovider om PHP bij te werken naar een gepatchte versie.

3. Bevestigen

Vraag voor uw online tools met abonnement (SaaS) de softwareleverancier om te bevestigen dat de patch is toegepast.

HOE WEET U OF UW WEBSITE PHP GEBRUIKT?

Methode	Werkwijze	Betrouwbaarheid
Vraag uw dienstverlener	"Welke PHP-versie gebruiken mijn website en tools? Is die gepatcht tegen PHP2Shell?"	Zeker
Gratis online tool	Voer uw webadres in op builtwith.com of whatcms.org . Verschijnt "PHP", "WordPress", "WooCommerce"...? Laat de PHP-versie controleren: de tool toont niet of de patch is geïnstalleerd.	Goed
Aanwijzingen in het adres	Een adres met ".php" of een bestaande pagina uw-website.be/wp-admin (WordPress).	Indicatief
Geen zichtbare aanwijzingen?	Sommige hostingproviders verbergen die aanwijzingen. Geen aanwijzing betekent niet dat uw website geen PHP gebruikt.	Onvoldoende → vraag het na

GEPATCHTE PHP-VERSIES

PHP-tak	Minimale gepatchte versie	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 ondersteuning tot 31/12/2026
PHP 8.1 en ouder	Geen officiële versie	Niet meer ondersteund gepatcht pakket van de leverancier (bv. Ubuntu), daarna migratie

Ubuntu: PHP 8.1 (Ubuntu 22.04) wordt gepatcht met een gewone update; PHP 7.4 (Ubuntu 20.04) via **Ubuntu Pro**, gratis tot 5 fysieke machines, ook voor een bedrijf (één account per bedrijf); daarboven betalend (ubuntu.com/pro).

Bronnen: officiële beveiligingsadviezen van het PHP-team (GHSA-w8hw-w9fx-j79w en GHSA-6wmf-4rv5-p3rp, gepubliceerd op 21 oktober 2026), php.net en Ubuntu USN-8948-1/-2. Na de update moet de dienst die PHP uitvoert opnieuw worden gestart (zie checklist, pagina 3).

→ WAS DEZE GIDS NUTTIG VOOR U? BEZORG HEM AAN UW COLLEGA'S EN UW WEBDIENSTVERLENER.

GEEN DIENSTVERLENER, OF NOOD AAN ADVIES?

Onze teams kunnen u met hun expertise helpen uw website te beschermen of u begeleiden bij de migratie naar een technologie die niet door dit lek wordt getroffen, zoals Odoo.

Contacteer ons: sales@taptap.be



BEHEERT U ZELF UW HOSTING?

Checklist voor uw IT-medewerker of de beheerder van uw server (VPS, dedicated server, cPanel, Plesk, Docker...).

Stap	Wat moet er gebeuren?
☐ 1. Werkelijk gebruikte versie nagaan	De opdracht <code>php -v</code> volstaat niet: controleer welke versie werkelijk elke website bedient (die van de webserver: PHP-FPM, Apache, LiteSpeed...). Bij cPanel of Plesk kan elk domein een eigen versie hebben.
☐ 2. PHP bijwerken	Naar 8.2.35, 8.3.36, 8.4.27, 8.5.12 of nieuwer, of een gepatcht pakket van de leverancier (ook voor 8.1 en ouder). • Distributiepakketten (Ubuntu, Debian, Red Hat, AlmaLinux...): de patch wordt vaak verwerkt zonder het versienummer te wijzigen; controleer of CVE-2026-109618 en CVE-2026-109619 in het wijzigingslogboek van het pakket staan. • cPanel / Plesk: bijwerken via het paneel. • Docker: image opnieuw bouwen op een gepatchte PHP-basis en opnieuw uitrollen.
☐ 3. PHP herstarten	Herstart de dienst die PHP uitvoert op uw server: meestal PHP-FPM , anders Apache (<code>mod_php</code>), LiteSpeed , FastCGI, FrankenPHP... Bij een Docker -container bouwt u de image opnieuw en rolt u die opnieuw uit. Vraag bij twijfel uw hostingprovider om hulp. Controleer daarna of er geen oude PHP-processen meer draaien: anders blijft de oude versie uw websites bedienen.
☐ 4. Kunt u niet meteen bijwerken?	Tijdelijke maatregelen, opgelegd in de server- of poolconfiguratie, niet wijzigbaar door websites (geen <code>.user.ini</code>): • <code>memory_limit = -1</code> met een externe geheugenlimiet (container, cgroup), nooit <code>RLIMIT_AS/DATA</code>; • <code>session.upload_progress.enabled = 0</code>; bij PHP 8.5 ook <code>fatal_error_backtraces = 0</code>; • grootte van verzoeken en uploads beperken op de webserver; • PHP-FPM: <code>pm.max_requests = 1</code> als de prestaties dit toelaten. Daarna alle PHP-processen herstarten. Deze maatregelen beperken het risico, maar vervangen geen gepatchte PHP-versie.
☐ 5. Blootstelling beperken	PHP alleen via de hoofdwebserver bereikbaar (geen Apache of PHP op een extra poort die openstaat voor het internet); geen PHP-parameters die de webserver bij elk verzoek doorgeeft (<code>PHP_VALUE</code>); <code>phpinfo</code> -bestanden verwijderen; phpMyAdmin en beheerpanelen alleen toegankelijk maken voor vertrouwde adressen of via een VPN.
☐ 6. Tekenen van een aanval zoeken	Sinds 17 oktober: POST-verzoeken met <code>PHP_SESSION_UPLOAD_PROGRESS</code> in de logboeken; recente of onbekende <code>.php</code> -bestanden in de webmappen; onbekende processen gestart door de webservergebruiker. Fouten "Allowed memory size exhausted" kunnen op pogingen wijzen; het ontbreken ervan bewijst niet dat alles in orde is. Raadpleeg bij twijfel een specialist.

→ WAS DEZE GIDS NUTTIG VOOR U? BEZORG HEM AAN UW COLLEGA'S EN UW WEBDIENSTVERLENER.

GEEN DIENSTVERLENER, OF NOOD AAN ADVIES?

Onze teams kunnen u met hun expertise helpen uw website te beschermen of u begeleiden bij de migratie naar een technologie die niet door dit lek wordt getroffen, zoals Odoo.

Contacteer ons: sales@taptap.be



BIJLAGE: VEELGEBRUIKTE TOOLS OP BASIS VAN PHP

Als ze **bij u of een dienstverlener gehost worden**, zijn ze mogelijk getroffen en moeten ze bijgewerkt worden.

Wat moet u doen? **Contacteer uw dienstverlener** (webdienstverlener, hostingprovider of ontwikkelaar) om PHP te laten bijwerken. Die kent uw toepassing door en door en is dus het best geplaatst.

- AbanteCart (webshop)
- Akaunting (boekhouding)
- Akeneo (productcatalogus)
- Amelia (reserveringen, WordPress-module)
- Bagisto (webshop)
- Bolt CMS (website)
- Bookly (reserveringen, WordPress-module)
- BookStack (interne documentatie)
- Cacti (netwerkbewaking)
- CakePHP (ontwikkeling op maat)
- Chamilo (online opleidingen)
- CiviCRM (CRM voor verenigingen)
- CodeIgniter (ontwikkeling op maat)
- Concrete CMS (website)
- Contact Form 7 (formulieren, WordPress-module)
- Contao (website)
- Craft CMS (website)
- CubeCart (webshop)
- DokuWiki (wiki)
- Dolibarr (ERP / CRM)
- Drupal (website)
- Elementor (paginaopbouw, WordPress)
- EspoCRM (CRM)
- FacturaScripts (facturatie)
- FreeScout (klantendienst)
- FrontAccounting (boekhouding)
- GLPI (IT-middelen / support)
- Grav (website)
- Gravity Forms (formulieren, WordPress-module)
- Horde (webmail)
- Houzez (vastgoedthema, WordPress)
- Ibexa (eZ Platform) (website)
- Invoice Ninja (facturatie)
- InvoicePlane (facturatie)
- Joomla (website)
- Kanboard (projectbeheer)
- Kimai (tijdregistratie)
- Kirby (website)
- Laravel (ontwikkeling op maat)
- Leantime (projectbeheer)
- LimeSurvey (enquêtes)
- LiteCart (webshop)
- Magento / Adobe Commerce (webshop)
- MantisBT (ticketopvolging)
- Matomo (webstatistieken)
- Mautic (marketingautomatisering)
- MediaWiki (wiki)
- MODX (website)
- Moodle (online opleidingen)
- Nextcloud (bestandsdeling)
- October CMS (website)
- Open Real Estate (vastgoedwebsite)
- OpenCart (webshop)
- OpenEMR (medisch dossier)
- OroCommerce (B2B-e-commerce)
- OroCRM (CRM)
- osTicket (klantendienst)
- ownCloud Server (bestandsdeling)
- phpBB (forum)
- phpList (nieuwsbrieven)
- phpMyAdmin (databankbeheer)
- Pimcore (productcatalogus / media)
- Piwigo (fotogalerij)
- PrestaShop (webshop)
- ProcessWire (website)
- RealHomes (vastgoedthema, WordPress)
- Roundcube (webmail)
- Sendy (nieuwsbrieven)
- Shopware (webshop)
- SilverStripe (website)
- Simple Machines Forum (forum)
- SnappyMail / RainLoop (webmail)
- Snipe-IT (IT-middelen)
- SquirrelMail (webmail)
- Statamic (website)
- SugarCRM (CRM)
- SuiteCRM (CRM)
- Sulu (website)
- Sylius (webshop)
- Symfony (ontwikkeling op maat)
- Thelia (webshop)
- Vtiger (CRM)
- WHMCS (hostingfacturatie)
- WooCommerce (webshop, WordPress)
- WordPress (website)
- WP Residence (vastgoedthema, WordPress)
- WPForms (formulieren, WordPress-module)
- Yii (ontwikkeling op maat)
- Zabbix (bewaking, webinterface)
- Zen Cart (webshop)

... en ook **alle WordPress-thema's en -modules** en elke toepassing op maat in PHP. **Vetgedrukt:** de meest gebruikte tools.

Deze gids biedt algemene informatie op datum van 22 oktober 2026. Hij vormt geen beveiligingsaudit van uw systemen. De vermelde productnamen behoren toe aan hun respectieve eigenaars en dienen enkel om de betrokken technologieën te helpen identificeren.

→ **WAS DEZE GIDS NUTTIG VOOR U? BEZORG HEM AAN UW COLLEGA'S EN UW WEBDIENSTVERLENER.**

GEEN DIENSTVERLENER, OF NOOD AAN ADVIES?

Onze teams kunnen u met hun expertise helpen **uw website te beschermen** of u begeleiden bij de **migratie naar een technologie die niet door dit lek wordt getroffen**, zoals **Odoo**.

Contacteer ons: **sales@taptap.be**

