

FAILLE PHP « PHP2SHELL » : CE QU'IL FAUT SAVOIR

Une faille critique touche PHP, langage très utilisé par les sites web et les outils de gestion en ligne. Des tentatives d'exploitation sont observées depuis le 17 octobre. Ce guide vous aide à savoir si vous êtes concerné, et quoi faire.

La faille expliquée simplement

- **Avant même que votre site ne s'affiche**, PHP reçoit la demande du visiteur (une page, un formulaire, un envoi de fichier) et la prépare en mémoire.
- Un pirate envoie une **demande piégée**, conçue pour faire « déborder » cette préparation. PHP s'interrompt brutalement et laisse derrière lui des informations **à moitié rangées** en mémoire.
- PHP ne voit pas ce désordre et s'en sert, parfois à la demande suivante. Or le pirate l'a préparé : il y a glissé **ses propres instructions**, que PHP finit par **exécuter comme les siennes**.
- Résultat : **sans mot de passe ni compte**, il peut prendre le contrôle du site : voler des données (clients, commandes), installer un programme malveillant, envoyer du spam ou rediriger vos visiteurs.

Pourquoi c'est grave : la faille se trouve dans PHP lui-même, pas dans votre site. Un site parfaitement à jour (WordPress, PrestaShop...) reste vulnérable tant que PHP n'est pas corrigé.

✓ Vos écrans TapTap ne sont pas concernés

- **Votre installation n'utilise pas PHP**. Les logiciels qui pilotent vos écrans et diffusent vos contenus reposent sur d'autres technologies, non concernées par cette faille.
- **Votre installation est pilotée par son contrôleur, un logiciel installé sur votre ordinateur**, contrairement aux solutions qui centralisent la gestion des écrans sur une plateforme en ligne.
- **Les players qui pilotent vos écrans ne sont pas joignables depuis Internet**. Ils n'ont aucune adresse publique : nos équipes les administrent uniquement à travers un réseau privé et chiffré.

Pour vos écrans, aucune action n'est nécessaire.

⚠ En revanche, vérifiez votre site web et vos outils de gestion

Si votre site, votre boutique en ligne ou l'un de vos outils fonctionne avec PHP et est hébergé chez vous ou chez un prestataire, il doit être mis à jour **sans attendre**. Les pages suivantes expliquent comment vérifier en deux minutes et indiquent les versions corrigées ; la liste des outils les plus courants figure en annexe.

→ CE GUIDE VOUS A ÉTÉ UTILE ? TRANSMETTEZ-LE À VOS COLLÈGUES ET À VOTRE PRESTATAIRE WEB.

PAS DE PRESTATAIRE, OU BESOIN D'UN CONSEIL ?

Nos équipes peuvent vous apporter leur expertise pour **protéger votre site**, ou vous accompagner dans sa **migration vers une technologie non concernée par cette faille**, comme Odoo.

Contactez-nous : sales@taptap.be



EN BREF : QUE FAIRE ?

1. Identifier

Repérez vos outils en PHP grâce à la méthode « Comment savoir » (page 2) et à la liste des outils en annexe.

2. Contacter

Demandez à votre prestataire web ou à votre hébergeur de passer PHP dans une version corrigée.

3. Confirmer

Pour vos outils en abonnement en ligne (SaaS), demandez à l'éditeur de confirmer que le correctif est appliqué.

COMMENT SAVOIR SI VOTRE SITE UTILISE PHP ?

Méthode	Comment faire	Fiabilité
Demander à votre prestataire	« Quelle version de PHP fait tourner mon site et mes outils ? Est-elle corrigée contre PHP2Shell ? »	Certaine
Outil en ligne gratuit	Saisir l'adresse de votre site sur builtwith.com ou whatcms.org . Si « PHP », « WordPress », « WooCommerce »... apparaît, faites vérifier la version de PHP : l'outil ne dit pas si le correctif est installé.	Bonne
Indices dans l'adresse	Une adresse qui contient « .php », ou une page votre-site.be/wp-admin qui existe (WordPress).	Indicative
Aucun signe visible ?	Certains hébergeurs masquent ces indices. L'absence de signe ne prouve pas que votre site n'utilise pas PHP.	Insuffisant → demandez

VERSIONS DE PHP CORRIGÉES

Branche PHP	Version corrigée minimale	Statut
PHP 8.5	8.5.12	Corrigée
PHP 8.4	8.4.27	Corrigée
PHP 8.3	8.3.36	Corrigée
PHP 8.2	8.2.35	Corrigée fin de support le 31/12/2026
PHP 8.1 et antérieures	Pas de version officielle	Hors support paquet corrigé du fournisseur (ex. Ubuntu), puis migration

Ubuntu : PHP 8.1 (Ubuntu 22.04) est corrigé par une simple mise à jour ; PHP 7.4 (Ubuntu 20.04) via **Ubuntu Pro**, gratuit jusqu'à 5 machines physiques, y compris pour une société (un compte par société) ; au-delà, offre payante (ubuntu.com/pro).

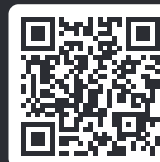
Sources : avis de sécurité officiels de l'équipe PHP (GHSA-w8hw-w9fx-j79w et GHSA-6wmf-4rv5-p3rp, publiés le 21 octobre 2026), php.net et Ubuntu USN-8948-1/-2. Après la mise à jour, le service qui exécute PHP doit être redémarré (voir la check-list, page 3).

→ CE GUIDE VOUS A ÉTÉ UTILE ? TRANSMETTEZ-LE À VOS COLLÈGUES ET À VOTRE PRESTATAIRE WEB.

PAS DE PRESTATAIRE, OU BESOIN D'UN CONSEIL ?

Nos équipes peuvent vous apporter leur expertise pour **protéger votre site**, ou vous accompagner dans sa **migration vers une technologie non concernée par cette faille**, comme **Odoo**.

Contactez-nous : sales@taptap.be



VOUS GÉREZ VOUS-MÊME VOTRE HÉBERGEMENT ?

Check-list à transmettre à votre informaticien ou à la personne qui gère votre serveur (VPS, serveur dédié, cPanel, Plesk, Docker...).

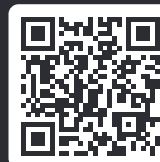
Étape	Ce qu'il faut faire
☐ 1. Identifier la version réellement utilisée	La commande <code>php -v</code> ne suffit pas : vérifiez la version qui sert réellement chaque site (celle utilisée par le serveur web : PHP-FPM, Apache, LiteSpeed...). Avec cPanel ou Plesk, chaque domaine peut avoir sa propre version.
☐ 2. Mettre PHP à jour	Vers 8.2.35, 8.3.36, 8.4.27, 8.5.12 ou plus récent, ou un paquet corrigé du fournisseur (aussi pour 8.1 et antérieurs). • Paquets de distribution (Ubuntu, Debian, Red Hat, AlmaLinux...) : le correctif est souvent intégré sans changer le numéro de version ; vérifiez que CVE-2026-109618 et CVE-2026-109619 figurent dans le journal des modifications du paquet. • cPanel / Plesk : mise à jour depuis le panneau. • Docker : reconstruire l'image sur une base PHP corrigée, puis redéployer.
☐ 3. Redémarrer PHP	Redémarrez le service qui exécute PHP sur votre serveur : le plus souvent PHP-FPM , sinon Apache (<code>mod_php</code>), LiteSpeed , FastCGI, FrankenPHP... En conteneur Docker , reconstruisez et redéployez l'image. En cas de doute, demandez à votre hébergeur. Vérifiez ensuite qu' aucun ancien processus PHP ne tourne encore : sinon, l'ancienne version continue de servir vos sites.
☐ 4. Mise à jour impossible tout de suite ?	Mesures provisoires, imposées dans la configuration du serveur ou du pool, non modifiables par les sites (pas <code>.user.ini</code>) : • <code>memory_limit = -1</code> avec une limite mémoire externe (conteneur, cgroup), jamais <code>RLIMIT_AS/DATA</code> ; • <code>session.upload_progress.enabled = 0</code> ; sur PHP 8.5, aussi <code>fatal_error_backtraces = 0</code> ; • limiter taille des requêtes et envois de fichiers au niveau du serveur web ; • PHP-FPM : <code>pm.max_requests = 1</code> si les performances le permettent. Puis redémarrer tous les processus PHP . Ces mesures réduisent le risque mais ne remplacent pas un PHP corrigé.
☐ 5. Réduire l'exposition	PHP joignable uniquement via le serveur web principal (pas d'Apache ou de PHP sur un port annexe ouvert à Internet) ; aucun paramètre PHP transmis par le serveur web à chaque requête (<code>PHP_VALUE</code>) ; supprimer les fichiers <code>phpinfo</code> ; réserver phpMyAdmin et les panneaux d'administration aux adresses de confiance ou à un VPN.
☐ 6. Rechercher des signes d'attaque	Depuis le 17 octobre : requêtes POST contenant <code>PHP_SESSION_UPLOAD_PROGRESS</code> dans les journaux ; fichiers <code>.php</code> récents ou inconnus dans les dossiers web ; processus inconnus lancés par l'utilisateur du serveur web. Des erreurs « Allowed memory size exhausted » peuvent signaler des tentatives ; leur absence ne prouve pas que tout va bien. En cas de doute, faites appel à un spécialiste.

→ CE GUIDE VOUS A ÉTÉ UTILE ? TRANSMETTEZ-LE À VOS COLLÈGUES ET À VOTRE PRESTATAIRE WEB.

PAS DE PRESTATAIRE, OU BESOIN D'UN CONSEIL ?

Nos équipes peuvent vous apporter leur expertise pour **protéger votre site**, ou vous accompagner dans sa **migration vers une technologie non concernée par cette faille**, comme **Odoo**.

Contactez-nous : sales@taptap.be



ANNEXE : OUTILS COURANTS FONCTIONNANT AVEC PHP

S'ils sont **hébergés chez vous ou chez un prestataire**, ils sont potentiellement concernés et doivent être mis à jour.

Que faire ? Prenez contact avec votre prestataire (web, hébergeur ou développeur) pour faire mettre PHP à jour. C'est la meilleure personne, car elle connaît parfaitement votre application.

- AbanteCart (boutique en ligne)
- Akaunting (comptabilité)
- Akeneo (catalogue produits)
- Amelia (réservation, module WordPress)
- Bagisto (boutique en ligne)
- Bolt CMS (site web)
- Bookly (réservation, module WordPress)
- BookStack (documentation interne)
- Cacti (supervision réseau)
- CakePHP (développement sur mesure)
- Chamilo (formation en ligne)
- CiviCRM (CRM associatif)
- CodeIgniter (développement sur mesure)
- Concrete CMS (site web)
- Contact Form 7 (formulaires, module WordPress)
- Contao (site web)
- Craft CMS (site web)
- CubeCart (boutique en ligne)
- DokuWiki (wiki)
- Dolibarr (ERP / CRM)
- Drupal (site web)
- Elementor (création de pages, WordPress)
- EspoCRM (CRM)
- FacturaScripts (facturation)
- FreeScout (support client)
- FrontAccounting (comptabilité)
- GLPI (parc informatique / support)
- Grav (site web)
- Gravity Forms (formulaires, module WordPress)
- Horde (webmail)
- Houzez (thème immobilier, WordPress)
- Ibexa (eZ Platform) (site web)
- Invoice Ninja (facturation)
- InvoicePlane (facturation)
- Joomla (site web)
- Kanboard (gestion de projet)
- Kimai (suivi du temps)
- Kirby (site web)
- Laravel (développement sur mesure)
- Leantime (gestion de projet)
- LimeSurvey (enquêtes)
- LiteCart (boutique en ligne)
- **Magento / Adobe Commerce** (boutique en ligne)
- MantisBT (suivi de tickets)
- Matomo (statistiques web)
- Mautic (marketing automation)
- MediaWiki (wiki)
- MODX (site web)
- Moodle (formation en ligne)
- Nextcloud (partage de fichiers)
- October CMS (site web)
- Open Real Estate (site immobilier)
- **OpenCart** (boutique en ligne)
- OpenEMR (dossier médical)
- OroCommerce (e-commerce B2B)
- OroCRM (CRM)
- osTicket (support client)
- ownCloud Server (partage de fichiers)
- phpBB (forum)
- phpList (newsletters)
- **phpMyAdmin** (administration de bases de données)
- Pimcore (catalogue produits / médias)
- Piwigo (galerie photo)
- **PrestaShop** (boutique en ligne)
- ProcessWire (site web)
- RealHomes (thème immobilier, WordPress)
- **Roundcube** (webmail)
- Sendy (newsletters)
- **Shopware** (boutique en ligne)
- SilverStripe (site web)
- Simple Machines Forum (forum)
- SnappyMail / RainLoop (webmail)
- Snipe-IT (parc informatique)
- SquirrelMail (webmail)
- Statamic (site web)
- SugarCRM (CRM)
- SuiteCRM (CRM)
- Sulu (site web)
- Sylius (boutique en ligne)
- **Symfony** (développement sur mesure)
- Thelia (boutique en ligne)
- Vtiger (CRM)
- WHMCS (facturation d'hébergement)
- **WooCommerce** (boutique en ligne, WordPress)
- **WordPress** (site web)
- WP Residence (thème immobilier, WordPress)
- WPForms (formulaires, module WordPress)
- Yii (développement sur mesure)
- Zabbix (supervision, interface web)
- Zen Cart (boutique en ligne)

... ainsi que **tous les thèmes et modules WordPress** et toute application développée sur mesure en PHP. **En gras** : les outils les plus répandus.

Ce guide est une information générale établie au 22 octobre 2026. Il ne constitue pas un audit de sécurité de vos systèmes. Les noms de produits cités appartiennent à leurs propriétaires respectifs et sont mentionnés uniquement pour aider à identifier les technologies concernées.

→ CE GUIDE VOUS A ÉTÉ UTILE ? TRANSMETTEZ-LE À VOS COLLÈGUES ET À VOTRE PRESTATAIRE WEB.

PAS DE PRESTATAIRE, OU BESOIN D'UN CONSEIL ?

Nos équipes peuvent vous apporter leur expertise pour **protéger votre site**, ou vous accompagner dans sa **migration vers une technologie non concernée par cette faille**, comme **Odoo**.

Contactez-nous : **sales@taptap.be**

