

# PHP "PHP2SHELL" FLAW: WHAT YOU NEED TO KNOW

A critical vulnerability affects PHP, a language widely used for websites and online management tools. Exploitation attempts have been observed since 17 October. This guide helps you find out whether you are affected and what to do.

## The vulnerability explained simply

- **Before your website is even displayed**, PHP receives the visitor's request (a page, a form, a file upload) and prepares it in memory.
- An attacker sends a **crafted request** designed to make this preparation "overflow". PHP stops abruptly, leaving information **half organised** in memory.
- PHP does not notice this disorder and uses the information, sometimes on the next request. But the attacker has prepared it: they have slipped in **their own instructions**, which PHP ends up **executing as its own**.
- Result: **without a password or account**, they can take control of the website: steal data (customers, orders), install malware, send spam or redirect your visitors.

**Why this is serious:** the vulnerability is in PHP itself, not in your website. A fully updated website (WordPress, PrestaShop...) remains vulnerable until PHP is patched.

## ✓ Your TapTap screens are not affected

- **Your installation does not use PHP.** The software that controls your screens and displays your content uses other technologies, which are not affected by this vulnerability.
- **Your installation is managed by its controller, software installed on your computer**, unlike solutions that centralise screen management on an online platform.
- **The players controlling your screens cannot be reached from the Internet.** They have no public address: our teams manage them only through a private, encrypted network.

**No action is needed for your screens.**

## ⚠ Do check your website and management tools

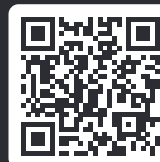
If your website, online shop or any of your tools uses PHP and is hosted on your premises or by a provider, it must be updated **immediately**. The following pages explain how to check in two minutes and list the patched versions; the most common tools are listed in the appendix.

→ FOUND THIS GUIDE USEFUL? SHARE IT WITH YOUR COLLEAGUES AND YOUR WEB SERVICE PROVIDER.

### NO PROVIDER, OR NEED ADVICE?

Our teams can help **protect your website** or support its **migration to a technology unaffected by this vulnerability**, such as Odo.

Contact us: [sales@taptap.be](mailto:sales@taptap.be)



## AT A GLANCE: WHAT TO DO

### 1. Identify

Identify your PHP tools using the "How to tell" method (page 2) and the list of tools in the appendix.

### 2. Contact

Ask your web service provider or hosting provider to update PHP to a patched version.

### 3. Confirm

For online subscription tools (SaaS), ask the software vendor to confirm that the patch has been applied.

## HOW TO TELL WHETHER YOUR WEBSITE USES PHP

| Method               | How to check                                                                                                                                                                                                                                                                 | Reliability           |
|----------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------|
| Ask your provider    | "Which version of PHP runs my website and tools? Is it patched against PHP2Shell?"                                                                                                                                                                                           | Certain               |
| Free online tool     | Enter your website address on <a href="https://builtwith.com">builtwith.com</a> or <a href="https://whatcms.org">whatcms.org</a> . If "PHP", "WordPress", "WooCommerce"... appears, have the PHP version checked: the tool does not tell you whether the patch is installed. | Good                  |
| Clues in the address | An address containing ".php", or an existing <a href="#">your-site.be/wp-admin</a> page (WordPress).                                                                                                                                                                         | Indicative            |
| No visible clues?    | Some hosting providers hide these clues. Their absence does not prove that your website does not use PHP.                                                                                                                                                                    | Insufficient<br>→ ask |

## PATCHED PHP VERSIONS

| PHP branch          | Minimum patched version | Status                                                              |
|---------------------|-------------------------|---------------------------------------------------------------------|
| PHP 8.5             | 8.5.12                  | Patched                                                             |
| PHP 8.4             | 8.4.27                  | Patched                                                             |
| PHP 8.3             | 8.3.36                  | Patched                                                             |
| PHP 8.2             | 8.2.35                  | Patched support ends on 31/12/2026                                  |
| PHP 8.1 and earlier | No official version     | Out of support patched vendor package (e.g. Ubuntu), then migration |

**Ubuntu:** PHP 8.1 (Ubuntu 22.04) is patched with a simple update; PHP 7.4 (Ubuntu 20.04) via **Ubuntu Pro**, free for up to 5 physical machines, even for a company (one account per company); beyond that, a paid plan ([ubuntu.com/pro](https://ubuntu.com/pro)).

Sources: official PHP team security advisories (GHSA-w8hw-w9fx-j79w and GHSA-6wmf-4rv5-p3rp, published on 21 October 2026), php.net and Ubuntu USN-8948-1/-2. After updating, the service running PHP must be restarted (see the checklist, page 3).

→ FOUND THIS GUIDE USEFUL? SHARE IT WITH YOUR COLLEAGUES AND YOUR WEB SERVICE PROVIDER.

### NO PROVIDER, OR NEED ADVICE?

Our teams can help **protect your website** or support its **migration to a technology unaffected by this vulnerability**, such as **Odoo**.

Contact us: [sales@taptap.be](mailto:sales@taptap.be)



## DO YOU MANAGE YOUR OWN HOSTING?

Checklist to pass on to your IT specialist or the person managing your server (VPS, dedicated server, cPanel, Plesk, Docker...).

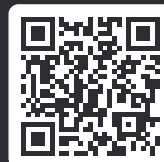
| Step                                                             | What to do                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
|------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <input type="checkbox"/> 1. Identify the version actually in use | The <code>php -v</code> command is not enough: check the version <b>actually</b> serving each website (the one used by the web server: PHP-FPM, Apache, LiteSpeed...). With cPanel or Plesk, <b>each domain</b> may have its own version.                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| <input type="checkbox"/> 2. Update PHP                           | To <b>8.2.35, 8.3.36, 8.4.27, 8.5.12</b> or newer, or a <b>patched package</b> from the vendor (also for 8.1 and earlier). <ul style="list-style-type: none"><li>• <b>Distribution packages</b> (Ubuntu, Debian, Red Hat, AlmaLinux...): the patch is often included <b>without changing the version number</b>; check that CVE-2026-109618 and CVE-2026-109619 appear in the package changelog.</li><li>• <b>cPanel / Plesk</b>: update through the panel.</li><li>• <b>Docker</b>: rebuild the image on a patched PHP base, then redeploy.</li></ul>                                                                                                                              |
| <input type="checkbox"/> 3. Restart PHP                          | Restart the service running PHP on your server: usually <b>PHP-FPM</b> , otherwise <b>Apache</b> ( <code>mod_php</code> ), <b>LiteSpeed</b> , FastCGI, FrankenPHP... For a <b>Docker</b> container, rebuild and redeploy the image. If unsure, ask your hosting provider. Then check that <b>no old PHP processes</b> are still running: otherwise, the old version continues to serve your websites.                                                                                                                                                                                                                                                                               |
| <input type="checkbox"/> 4. Cannot update immediately?           | Temporary measures, enforced in the server or pool configuration, not changeable by websites (no <code>.user.ini</code> ): <ul style="list-style-type: none"><li>• <code>memory_limit = -1</code> with an external memory limit (container, cgroup), never <code>RLIMIT_AS/DATA</code>;</li><li>• <code>session.upload_progress.enabled = 0</code>; on PHP 8.5, also <code>fatal_error_backtraces = 0</code>;</li><li>• limit request and file upload sizes at web server level;</li><li>• PHP-FPM: <code>pm.max_requests = 1</code> if performance allows.</li></ul> Then <b>restart all PHP processes</b> . <b>These measures reduce the risk but do not replace patched PHP.</b> |
| <input type="checkbox"/> 5. Reduce exposure                      | PHP reachable <b>only through the main web server</b> (no Apache or PHP on an additional Internet-facing port); no PHP parameters passed by the web server with each request ( <code>PHP_VALUE</code> ); remove <code>phpinfo</code> files; restrict phpMyAdmin and administration panels to trusted addresses or a VPN.                                                                                                                                                                                                                                                                                                                                                            |
| <input type="checkbox"/> 6. Look for signs of attack             | Since 17 October: POST requests containing <code>PHP_SESSION_UPLOAD_PROGRESS</code> in logs; recent or unknown <code>.php</code> files in web directories; unknown processes started by the web server user. "Allowed memory size exhausted" errors may indicate attempts; their absence does not prove that everything is fine. <b>If unsure, consult a specialist.</b>                                                                                                                                                                                                                                                                                                            |

→ FOUND THIS GUIDE USEFUL? SHARE IT WITH YOUR COLLEAGUES AND YOUR WEB SERVICE PROVIDER.

### NO PROVIDER, OR NEED ADVICE?

Our teams can help **protect your website** or support its **migration to a technology unaffected by this vulnerability**, such as **Odoo**.

Contact us: [sales@taptap.be](mailto:sales@taptap.be)



## APPENDIX: COMMON TOOLS THAT USE PHP

If they are **hosted on your premises or by a provider**, they are potentially affected and must be updated.

**What to do?** **Contact your provider** (web service provider, hosting provider or developer) to have PHP updated. They are best placed to help, as they know your application thoroughly.

- AbanteCart (online shop)
- Akaunting (accounting)
- Akeneo (product catalogue)
- Amelia (booking, WordPress plugin)
- Bagisto (online shop)
- Bolt CMS (website)
- Bookly (booking, WordPress plugin)
- BookStack (internal documentation)
- Cacti (network monitoring)
- CakePHP (custom development)
- Chamilo (online learning)
- CiviCRM (CRM for associations)
- CodeIgniter (custom development)
- Concrete CMS (website)
- Contact Form 7 (forms, WordPress plugin)
- Contao (website)
- Craft CMS (website)
- CubeCart (online shop)
- DokuWiki (wiki)
- Dolibarr (ERP / CRM)
- Drupal (website)
- Elementor (page builder, WordPress)
- EspoCRM (CRM)
- FacturaScripts (invoicing)
- FreeScout (customer support)
- FrontAccounting (accounting)
- GLPI (IT assets / support)
- Grav (website)
- Gravity Forms (forms, WordPress plugin)
- Horde (webmail)
- Houzez (real estate theme, WordPress)
- Ibexa (eZ Platform) (website)
- Invoice Ninja (invoicing)
- InvoicePlane (invoicing)
- Joomla (website)
- Kanboard (project management)
- Kimai (time tracking)
- Kirby (website)
- Laravel (custom development)
- Leantime (project management)
- LimeSurvey (surveys)
- LiteCart (online shop)
- Magento / Adobe Commerce (online shop)
- MantisBT (ticket tracking)
- Matomo (web statistics)
- Mautic (marketing automation)
- MediaWiki (wiki)
- MODX (website)
- Moodle (online learning)
- Nextcloud (file sharing)
- October CMS (website)
- Open Real Estate (real estate website)
- OpenCart (online shop)
- OpenEMR (medical record)
- OroCommerce (B2B e-commerce)
- OroCRM (CRM)
- osTicket (customer support)
- ownCloud Server (file sharing)
- phpBB (forum)
- phpList (newsletters)
- phpMyAdmin (database administration)
- Pimcore (product catalogue / media)
- Piwigo (photo gallery)
- PrestaShop (online shop)
- ProcessWire (website)
- RealHomes (real estate theme, WordPress)
- Roundcube (webmail)
- Sendy (newsletters)
- Shopware (online shop)
- SilverStripe (website)
- Simple Machines Forum (forum)
- SnappyMail / RainLoop (webmail)
- Snipe-IT (IT assets)
- SquirrelMail (webmail)
- Statamic (website)
- SugarCRM (CRM)
- SuiteCRM (CRM)
- Sulu (website)
- Sylius (online shop)
- Symfony (custom development)
- Thelia (online shop)
- Vtiger (CRM)
- WHMCS (hosting billing)
- WooCommerce (online shop, WordPress)
- WordPress (website)
- WP Residence (real estate theme, WordPress)
- WPForms (forms, WordPress plugin)
- Yii (custom development)
- Zabbix (monitoring, web interface)
- Zen Cart (online shop)

... as well as **all WordPress themes and plugins** and any application custom-built in PHP. **In bold**: the most widely used tools.

This guide provides general information as of 22 October 2026. It is not a security audit of your systems. The product names mentioned belong to their respective owners and are included solely to help identify the technologies affected.

→ FOUND THIS GUIDE USEFUL? SHARE IT WITH YOUR COLLEAGUES AND YOUR WEB SERVICE PROVIDER.

### NO PROVIDER, OR NEED ADVICE?

Our teams can help **protect your website** or support its **migration to a technology unaffected by this vulnerability**, such as **Odoo**.

Contact us: **sales@taptap.be**

