

KNOWLEDGE BASE · PUBLIC DOCUMENT

Critical PHP vulnerabilities of October 2026 (CVE-2026-109618 and CVE-2026-109619): what we did and what you should do

Security

CODE

RLX-MZ-KB-2330

VERSION

v2026.10.21

COUNTRY · LANGUAGE

Mozambique · English

Interweb Mozambique

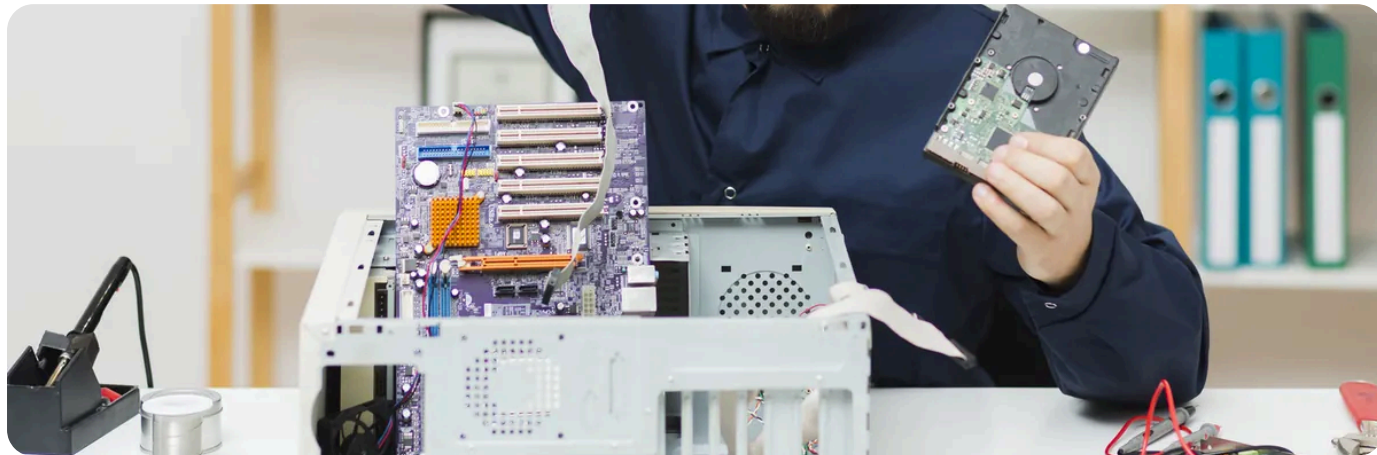
RLX Holdings, S.A. · Group RLX Holdings

Tax ID (NUIT) 401 191 607 · Legal entity no. (NUEL) 105 045 974 · Economic activity code (CAE) 62022

<https://www.meu.interweb.co.mz/knowledgebase/2330>

Critical PHP vulnerabilities of October 2026 (CVE-2026-109618 and CVE-2026-109619): what we did and what you should do

📁 Security 📅 Created on **October 21, 2026** ⌚ 6 min read



The short answer: on 21/10/2026 two critical vulnerabilities were published in PHP, the language WordPress and most websites run on. **If you have shared or reseller hosting with us, you are protected and there is nothing you need to do:** we applied protective measures the same day on all our hosting servers. **If you have a VPS, a Cloud server or a dedicated server,** you manage the system yourself (you have root access), so **you need to update PHP now.** This article shows how.



The official announcement:

The notice we published in My Interweb about these vulnerabilities is at **Critical PHP vulnerabilities: measures applied on our servers.**

🔍 What these vulnerabilities are

They are two flaws in PHP itself, rated 9.2 out of 10. Under certain conditions, they let an outsider **run code on the server without logging in**, just by sending requests to the site. They affect every PHP version, at every provider in the world, and every way of running it (PHP-FPM, Apache with mod_php, LiteSpeed and others).

Vulnerability	What it can allow	Affected versions	Fixed versions
CVE-2026-109618	Running code on the server, without logging in, when a request runs PHP out of memory halfway through, for example while a file is uploaded through a form.	8.2 before 8.2.35 8.3 before 8.3.36 8.4 before 8.4.27 8.5 before 8.5.12 8.1 and older	8.2.35, 8.3.36, 8.4.27 and 8.5.12
CVE-2026-109619	Running code on the server, without logging in, by using data from an earlier request that was not cleaned up, for example after a fatal error.	8.2 before 8.2.35 8.3 before 8.3.36 8.4 before 8.4.27 8.5 before 8.5.12 8.1 and older	8.2.35, 8.3.36, 8.4.27 and 8.5.12

PHP 8.1 and older versions (7.4, 8.0) no longer get fixes from the PHP project: a fix, if there is one, comes from your operating system vendor. If your site still runs one of those versions, now is the time to move to a supported one. Sources: CERT-EU advisory 2026-018 (cert.europa.eu) and the php.net announcement of 21/10/2026.

What we did on shared and reseller hosting

- 1

The same day, we applied protective measures on all our shared and reseller hosting servers: we switched off the PHP feature where the flaw was confirmed (the upload progress bar) and put limits on uploads.
- 2

The permanent fix (the patched PHP) will be installed as soon as the vendor of our servers' operating system makes it available. The rollout has already started and we check every hour.
- 3

Your sites, e-mail and files stay as they were. The only change you may notice: file uploads through forms are limited to **32 MB**. If you need more, ask us through a support ticket in My Interweb.

On a VPS, Cloud or dedicated server: updating PHP

Log in over SSH as root (or as a user with sudo) and follow the case that fits your server. If you can, take a backup of the server first, but do not delay the update because of it.

1 Check which version you have: `php -v` A server can have several PHP versions, and the site may use a different version from the one the console shows: update them all.

2 With cPanel and WHM: in WHM, open **Software » EasyApache 4** and press **Run System Update**. From the console, update the ea-php packages and restart PHP-FPM: `dnf upgrade 'ea-php*'`
`/usr/local/cpanel/scripts/restartsrv_apache_php_fpm --hard` To check each version, replace 83 with yours: `ea-php83 -v`

3 With Plesk: in **Tools & Settings » Updates**, on the **Update Components** tab, select the PHP components that have updates and press Continue. From the console: `plesk installer --select-release-latest --upgrade-installed-components` In the same area, under Update Settings, you can turn on automatic updates for third-party components, which are off by default.

4 Ubuntu or Debian without a panel: `sudo apt update`
`sudo apt upgrade` Then restart PHP-FPM for your version (find its name with `systemctl list-units 'php*'`), and Apache if you use mod_php: `sudo systemctl restart php8.3-fpm`
`sudo systemctl restart apache2`

5 AlmaLinux or Rocky Linux without a panel: `sudo dnf upgrade 'php*'`
`sudo systemctl restart php-fpm`
`sudo systemctl restart httpd`

6 Verify. Run `php -v` again and also check from the web: create a file called version.php on the site containing `<?php echo PHP_VERSION;`, open it in your browser and **delete it straight away**.

The version number may not change. In Ubuntu, Debian, AlmaLinux and Rocky Linux packages, the vendor usually patches the version it already ships, without moving it to 8.3.36 or one of the other versions above. In that case, check your system's security notices to confirm the installed package already carries the fix for both CVEs.

No patched package yet: the temporary measures

CERT-EU lists these measures for anyone who cannot update yet. They reduce the risk but **do not replace the update**: apply them now and update as soon as the patched package is available.

1 Switch off the upload progress bar in the `php.ini` of each PHP version: `session.upload_progress.enabled = 0` On cPanel, go to WHM, **Software » MultiPHP INI Editor**, Editor Mode tab, one version at a time. On Plesk, in **Tools & Settings » PHP Settings**, choose the version and open the `php.ini` tab. Without a panel, `php --ini` shows the file used on the command line; the PHP-FPM one is in another folder (on Debian and Ubuntu, `/etc/php/8.3/fpm/php.ini`).

2 Limit uploads: `post_max_size = 8M` if the site does not receive files, or `post_max_size = 32M` if it does, with `upload_max_filesize` below that value (for example, 30M).

3 On PHP 8.5, also add `fatal_error_backtraces = 0`.

4 Restart every PHP process, using the commands for your server above. Without a restart, the changes do not take effect.

5 Cannot update or apply these measures? CERT-EU recommends taking the server off public access until it is fixed. Talk to us first.



Do not rely on .user.ini or ini_set() alone.

CERT-EU warns that, for this flaw, the change has to be in the server's `php.ini` (or the PHP-FPM configuration), which is read before the request is handled. And **restart the PHP processes** after updating or changing `php.ini`: the processes already running keep the old code and settings.



Take the opportunity to bring everything else up to date.

Keep WordPress, plugins and themes updated (**updating WordPress** and **updating themes and plugins**), use strong passwords and, on an Ubuntu or Debian VPS, turn on automatic security updates: **how to update a Debian or Ubuntu VPS**.



NEED A HAND?

Do you have a VPS, Cloud or dedicated server and need help updating PHP? Or do you need to upload files larger than 32 MB? Talk to us.



Open a support ticket →



SEE ALSO

How to update a Debian or Ubuntu VPS, and turn on automatic security updates



Installing cPanel and WHM on your VPS, step by step



Installing Plesk on your VPS, step by step



First steps with your VPS



Managed or unmanaged VPS: which to choose and who does what



interweb

Interweb Mozambique

RLX Holdings, S.A. · Group RLX Holdings

TAX ID (NUIT)	401 191 607
LEGAL ENTITY NO. (NUEL)	105 045 974
ECONOMIC ACTIVITY CODE (CAE)	62022
REGISTERED OFFICE	Bairro 7 de Setembro Vilankulo 1304 · CEP 0411-02, Inhambane, Mozambique
CONTACT	info@interweb.co.mz · +258 84 635 1111 · +258 86 635 1111 · www.interweb.co.mz
OPENING HOURS	Monday to Friday - 08 AM to 04 PM Saturday & Sunday - Closed

RLX-MZ-KB-2330 · v2026.10.21 · Generated on 22/10/2026 08:28



Online version of this document