Gerado a 22/10/2026 07:31

BASE DE CONHECIMENTO · DOCUMENTO PÚBLICO

Falhas críticas do PHP de Outubro de 2026 (CVE-2026-109618 e CVE-2026-109619): o que fizemos e o que deve fazer

Segurança

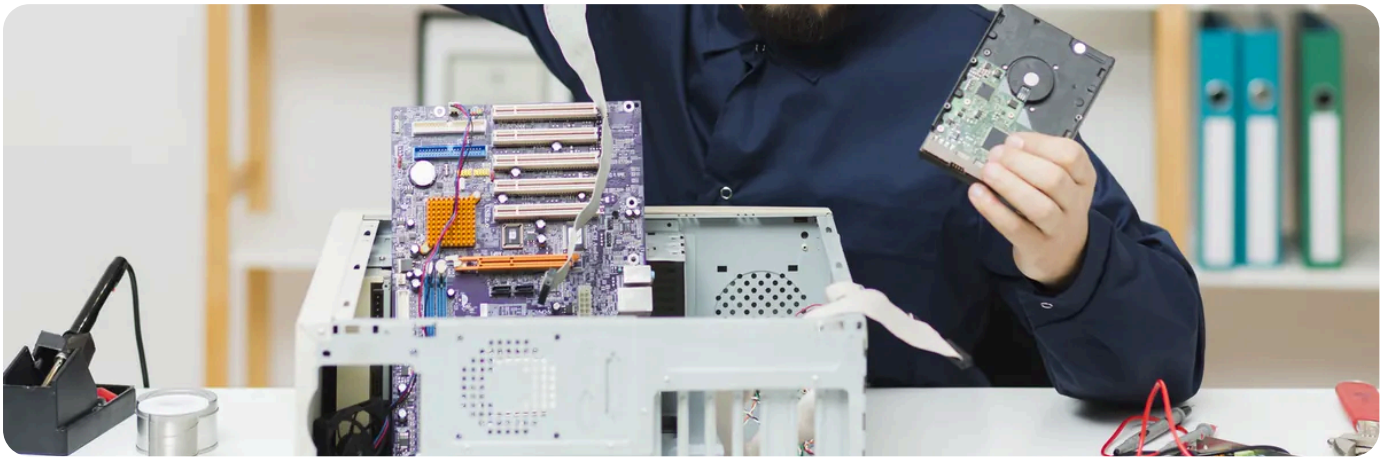
CÓDIGO	VERSÃO	PAÍS · IDIOMA
RLX-PT-KB-7074	v2026.10.21	Portugal · Português

MozOut Portugal
RLX Holdings (Pty) Ltd. · Grupo RLX Holdings
N.º fiscal (SARS) 943 907 6234 · N.º de registo (CIPC) 2025/667953/07

https://www.my.mozout.com/knowledgebase/7074

Falhas críticas do PHP de Outubro de 2026 (CVE-2026-109618 e CVE-2026-109619): o que fizemos e o que deve fazer

Segurança · Criado em **21 de outubro de 2026** · 6 min de leitura



A resposta curta: a 21/10/2026 foram publicadas duas falhas críticas no PHP, a linguagem em que funcionam o WordPress e a maior parte dos sites. **Se tem alojamento partilhado ou de revenda connosco, está protegido e não tem de fazer nada**: aplicámos medidas de protecção no mesmo dia em todos os nossos servidores de alojamento. **Se tem um VPS, um Cloud ou um servidor dedicado**, a gestão do sistema é sua (tem o acesso root) e, por isso, **tem de actualizar o PHP já**. Este artigo mostra como.

> **O anúncio oficial:**
> O aviso que publicámos no My MozOut sobre estas falhas está em **Falhas críticas do PHP: medidas aplicadas nos nossos servidores**.

O que são estas falhas

São dois erros no próprio PHP, com gravidade de 9,2 em 10. Em certas condições, permitem que alguém de fora **execute código no servidor sem precisar de login**, apenas com pedidos enviados ao site. Afectam todas as versões do PHP, em qualquer fornecedor do mundo, e todos os modos de execução (PHP-FPM, Apache com mod_php, LiteSpeed e outros).

Falha	O que pode permitir	Versões afectadas	Versões corrigidas
CVE-2026-109618	Executar código no servidor, sem login, quando um pedido esgota a memória do PHP a meio, por exemplo durante o envio de um ficheiro por formulário.	8.2 antes da 8.2.35 8.3 antes da 8.3.36 8.4 antes da 8.4.27 8.5 antes da 8.5.12 8.1 e anteriores	8.2.35, 8.3.36, 8.4.27 e 8.5.12
CVE-2026-109619	Executar código no servidor, sem login, aproveitando dados de um pedido anterior que ficaram por limpar, por exemplo depois de um erro fatal.	8.2 antes da 8.2.35 8.3 antes da 8.3.36 8.4 antes da 8.4.27 8.5 antes da 8.5.12 8.1 e anteriores	8.2.35, 8.3.36, 8.4.27 e 8.5.12

O PHP 8.1 e as versões anteriores (7.4, 8.0) já não recebem correcções do projecto PHP: a correcção, se existir, vem do fabricante do seu sistema operativo. Se o seu site ainda usa uma dessas versões, este é o momento de passar para uma versão suportada. Fontes: o aviso 2026-018 do CERT-EU (cert.europa.eu) e o anúncio do php.net de 21/10/2026.

O que fizemos no alojamento partilhado e na revenda

1. **No mesmo dia**, aplicámos medidas de protecção em todos os nossos servidores de alojamento partilhado e de revenda: desligámos a função do PHP onde a falha foi confirmada (a barra de progresso dos envios) e pusemos limites aos envios.

2. **A actualização definitiva** (o PHP corrigido) será instalada assim que o fabricante do sistema operativo dos nossos servidores a disponibilizar. A distribuição já começou e verificamos de hora a hora.

3. **Os seus sites, e-mails e ficheiros continuam como estavam.** A única mudança que pode notar: os envios de ficheiros por formulários ficam limitados a **32 MB**. Se precisar de mais, peça-nos através de um pedido de suporte no My MozOut.

Num VPS, Cloud ou servidor dedicado: actualizar o PHP

Entre por SSH como root (ou com um utilizador com sudo) e siga o caso do seu servidor. Se puder, faça antes uma cópia de segurança do servidor, mas não adie a actualização por isso.

1. **Veja que versão tem:** `php -v` Um servidor pode ter várias versões do PHP, e o site pode usar uma versão diferente da que a consola mostra: actualize todas.

2. **Com cPanel e WHM:** no WHM, abra **Software » EasyApache 4** e carregue em **Run System Update**. Pela consola, actualize os pacotes ea-php e reinicie o PHP-FPM: `dnf upgrade 'ea-php*'` `/usr/local/cpanel/scripts/restartsrv_apache_php_fpm --hard` Para ver cada versão, troque 83 pela sua: `ea-php83 -v`

3. **Com Plesk:** em **Tools & Settings » Updates**, separador **Update Components**, escolha os componentes do PHP com actualização disponível e carregue em Continue. Pela consola: `plesk installer --select-release-latest --upgrade-installed-components` Na mesma área, em Update Settings, pode ligar a actualização automática dos componentes de terceiros, que vem desligada.

4. **Ubuntu ou Debian sem painel:** `sudo apt update` `sudo apt upgrade` Depois reinicie o PHP-FPM da sua versão (veja o nome com `systemctl list-units 'php*'`), e também o Apache, se usa mod_php: `sudo systemctl restart php8.3-fpm` `sudo systemctl restart apache2`

5. **AlmaLinux ou Rocky Linux sem painel:** `sudo dnf upgrade 'php*'` `sudo systemctl restart php-fpm` `sudo systemctl restart httpd`

6. **Verifique.** Corra outra vez `php -v` e confirme também pela web: crie no site um ficheiro versao.php com `<?php echo PHP_VERSION;`, abra-o no navegador e **apague-o logo a seguir**.

O número da versão pode não mudar. Nos pacotes do Ubuntu, do Debian, do AlmaLinux e do Rocky Linux, o fabricante costuma corrigir a versão que já distribui, sem a mudar para 8.3.36 ou outra das versões acima. Nesse caso, confirme nos avisos de segurança do seu sistema que o pacote instalado já traz a correcção dos dois CVE.

Se ainda não há pacote corrigido: as medidas provisórias

O CERT-EU indica estas medidas para quem ainda não pode actualizar. Reduzem o risco, mas **não substituem a actualização**: aplique-as já e actualize assim que o pacote corrigido estiver disponível.

1. **Desligue a barra de progresso dos envios** no php.ini de cada versão do PHP: `session.upload_progress.enabled = 0` No cPanel, no WHM, em **Software » MultiPHP INI Editor**, separador Editor Mode, versão a versão. No Plesk, em **Tools & Settings » PHP Settings**, escolha a versão e abra o separador php.ini. Sem painel, `php --ini` mostra o ficheiro usado na consola; o do PHP-FPM está noutra pasta (no Debian e no Ubuntu, `/etc/php/8.3/fpm/php.ini`).

2. **Limite os envios:** `post_max_size = 8M` se o site não recebe ficheiros, ou `post_max_size = 32M` se recebe, com `upload_max_filesize` abaixo desse valor (por exemplo, 30M).

3. **No PHP 8.5**, acrescente também `fatal_error_backtraces = 0`.

4. **Reinicie todos os processos do PHP**, com os comandos indicados acima para o seu servidor. Sem reiniciar, as mudanças não têm efeito.

5. **Não consegue actualizar nem aplicar estas medidas?** O CERT-EU recomenda tirar o servidor do acesso público até estar corrigido. Fale connosco antes de o fazer.

Não confie só no .user.ini nem no ini_set().

O CERT-EU avisa que, para esta falha, a mudança tem de estar no php.ini do servidor (ou na configuração do PHP-FPM), porque é aí que o PHP a lê antes de tratar o pedido. E **reinicie os processos do PHP** depois de actualizar ou de mudar o php.ini: os processos que já estavam a correr continuam com o código e a configuração antigos.

Aproveite para pôr o resto em dia.

Mantenha o WordPress, os plugins e os temas actualizados (**actualizar o WordPress** e **actualizar temas e plugins**), use senhas fortes e, num VPS Ubuntu ou Debian, ligue as actualizações automáticas de segurança: **como actualizar um VPS Debian ou Ubuntu**.

PRECISA DE AJUDA?

Tem um VPS, Cloud ou servidor dedicado e precisa de ajuda para actualizar o PHP? Ou precisa de enviar ficheiros maiores do que 32 MB? Fale connosco.

Abrir um pedido de suporte →

VEJA TAMBÉM

- **Como actualizar um VPS Debian ou Ubuntu e ligar as actualizações automáticas de segurança**
- **Instalar o cPanel e o WHM no seu VPS, passo a passo**
- **Instalar o Plesk no seu VPS, passo a passo**
- **Primeiros passos com o seu VPS**
- **VPS gerido ou não gerido: qual escolher e quem faz o quê**

mozout

MozOut Portugal

RLX Holdings (Pty) Ltd. · Grupo RLX Holdings

N.º FISCAL (SARS)	943 907 6234
N.º DE REGISTO (CIPC)	2025/667953/07
SEDE	72 York Road, Kensington Joanesburgo 2094, Gauteng, África do Sul
CONTACTOS	info@mozout.com · +27 78 823 3325 · www.mozout.com
HORÁRIO	2ª. à 6ª. Feira - 08 à 16 Horas Sábado & Domingo - Fechado

Versão online deste documento

RLX-PT-KB-7074 · v2026.10.21 · Gerado a 22/10/2026 07:31