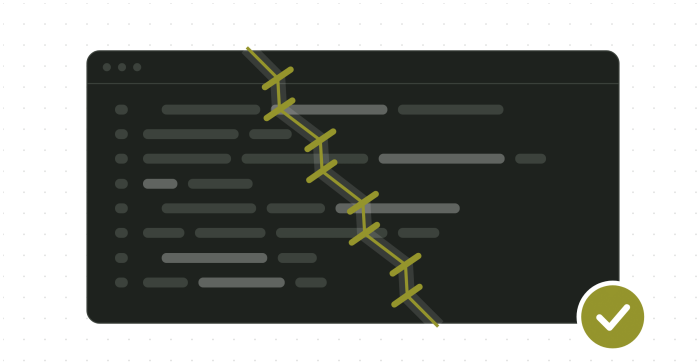
VULNERABILIDAD CRÍTICA DE PHP: LO QUE DEBEN SABER LOS RESPONSABLES DE UNA WEB

Posted on 22 de octubre de 2026 by Alexander



Una vulnerabilidad de PHP que acaba de salir a la luz está dando mucho que hablar. No afecta a un plugin de WordPress concreto ni a un gestor de contenidos determinado, sino a **una base técnica sobre la que funcionan muchísimas webs y aplicaciones web en todo el mundo**.

El equipo de seguridad de PHP califica de críticos dos fallos detectados. En determinadas condiciones, un atacante podría ejecutar código malicioso en un servidor sin necesidad de iniciar sesión. Si gestiona una web, no hace falta dejarse llevar por el pánico, pero sí reaccionar rápido y con criterio.

¿QUÉ HA PASADO?

PHP es un lenguaje de programación del lado del servidor y, en muchas webs, es la base que funciona en segundo plano. Numerosas instalaciones de WordPress y de otros gestores de contenidos dependen de él. Por eso, una vulnerabilidad de PHP puede afectar a muchos más sistemas que, por ejemplo, un fallo en un único plugin.

El 21 de octubre de 2026 se publicaron actualizaciones de seguridad para dos vulnerabilidades calificadas como críticas. Están registradas como **CVE-2026-109618** y **CVE-2026-109619**, y cada una tiene una puntuación CVSS de 9,2.

Dicho de forma sencilla: en determinadas condiciones, estos fallos pueden permitir la ejecución remota de código: un atacante podría ejecutar código arbitrario en el servidor. La facilidad para

atacar una web concreta depende de la versión de PHP, de la configuración del servidor y de otros factores técnicos. Por eso, no es cierto que cualquier web con PHP esté ya comprometida, pero tampoco conviene ignorar los avisos.

POR QUÉ AHORA ES CLAVE ACTUAR RÁPIDO

Cuando aparece una vulnerabilidad crítica, los administradores suelen entrar en una carrera contrarreloj. En cuanto se conocen los detalles técnicos de un fallo, los investigadores de seguridad pueden analizarlo, pero los atacantes también.

El propio proyecto PHP deja clara la urgencia: ha publicado actualizaciones de seguridad para las ramas afectadas e insta a instalarlas cuanto antes. Las protecciones provisionales o algunos ajustes de configuración pueden reducir el riesgo, pero no sustituyen al parche.

Para una empresa, la conclusión es clara: el mantenimiento técnico de una web no termina el día en que se publica. Hay que seguir los avisos de seguridad, valorar cómo afectan a la propia infraestructura y aplicar los cambios necesarios lo antes posible.

CÓMO HEMOS REACCIONADO: TRES PASOS

En Wisea actuamos en cuanto se conoció el problema en todas las **webs alojadas en la infraestructura de servidores que gestionamos**. El primer objetivo era limitar el riesgo de forma provisional y, el segundo, instalar las actualizaciones de seguridad publicadas.

Acción	Qué se ha hecho	Objetivo
Protección adicional	Se ha ajustado la configuración del servidor para proteger mejor, sobre todo, los formularios de las webs que gestionamos.	Limitar posibles vías de ataque antes de la actualización completa
Parches de seguridad de PHP	Se han instalado en el servidor los parches de PHP publicados.	Cerrar las vulnerabilidades conocidas en la capa de PHP
Actualización del servidor	Se ha actualizado el software del servidor a la última versión disponible.	Mantener al día todo el entorno, además de aplicar los parches de PHP

El orden no es casual. Cuando se descubre una vulnerabilidad, lo primero es reducir el riesgo

cuanto antes. En cuanto hay actualizaciones oficiales, toca eliminar la causa del problema.

¿BASTA CON ACTUALIZAR WORDPRESS?

No. Esta es una diferencia importante respecto a muchos avisos de seguridad a los que los responsables de una web están acostumbrados.

Esta vulnerabilidad de PHP no está en WordPress, sino en el propio lenguaje. Un WordPress completamente actualizado puede funcionar, aun así, sobre un entorno PHP vulnerable. Y, al revés, el aviso tampoco significa que el propio WordPress tenga un problema de seguridad.

Hay que mirar el conjunto de la web: sistema operativo, servidor web, versión de PHP, gestor de contenidos y extensiones tienen que funcionar bien juntos y mantenerse al día. Por eso, la gestión de la seguridad no termina al pulsar el botón de actualizar en el panel de WordPress.

Capa de la web	Relación con la vulnerabilidad
Plugins y tema	No es donde está el fallo
WordPress / gestor de contenidos	Actualizarlo no cierra el fallo
PHP	**Aquí está la vulnerabilidad**
Servidor web	Su configuración puede reducir el riesgo
Sistema operativo	También debe estar actualizado

Modelo de capas de una web: la vulnerabilidad está en PHP, no en WordPress

QUÉ DEBERÍAN REVISAR AHORA LOS RESPONSABLES DE UNA WEB

Ante esta vulnerabilidad de PHP, si gestiona usted mismo su web o su servidor, compruebe cuanto antes qué versión de PHP utiliza y si ya incluye las últimas correcciones de seguridad. Si no es así, toca actualizar PHP. Para las ramas de PHP con soporte actual se han publicado las versiones de seguridad correspondientes.

Además, merece la pena revisar todo el entorno:

- ¿Tiene el paquete de PHP instalado todas las actualizaciones de seguridad?

- ¿Se siguen usando versiones antiguas de PHP que ya no reciben actualizaciones de seguridad?
- ¿Está también actualizado el sistema operativo del servidor?
- ¿Hay sistemas accesibles desde internet que ya no se necesitan?
- ¿Se siguen de forma continua los avisos de seguridad de los sistemas que utiliza?
- ¿Existe un proceso para revisar e instalar con rapidez las actualizaciones críticas?

El último punto se suele subestimar. Un buen proceso de mantenimiento no consiste solo en actualizar con regularidad, sino también en poder reaccionar ante avisos de seguridad excepcionales fuera del ciclo normal de actualizaciones.

EL MANTENIMIENTO TÉCNICO FORMA PARTE DE LA SEGURIDAD DE UNA WEB

Las webs se juzgan a menudo por lo que se ve: diseño, contenidos, funciones y posicionamiento. Pero buena parte de su calidad está en segundo plano: actualizaciones, configuración del servidor, monitorización y respuesta ante nuevos riesgos de seguridad.

Casos como esta vulnerabilidad de PHP muestran la diferencia entre una web que simplemente está alojada en algún sitio y un entorno con mantenimiento técnico continuo. Los avisos de seguridad críticos no esperan a las fechas de mantenimiento. Por eso, llegado el momento, alguien tiene que poder valorar si hay que actuar, qué protecciones provisionales tienen sentido y cuándo hay que instalar un parche.

Para nosotros no es un extra, sino parte esencial de un servicio web profesional. Si está pensando en renovar su web, en nuestro artículo sobre el relanzamiento del sitio web le explicamos qué tener en cuenta.

CONCLUSIÓN: LA VULNERABILIDAD DE PHP ES SERIA, Y EN LOS SERVIDORES DE WISEA YA ESTÁ CORREGIDA

Conviene tomarse en serio estas vulnerabilidades de PHP. Afectan a un componente técnico central de muchas webs y el propio proyecto PHP las ha calificado de críticas. Si es usted responsable de su entorno PHP, compruebe si ya están instaladas las actualizaciones de seguridad necesarias.

Si su web está alojada en la infraestructura de servidores que gestiona Wisea, no tiene que hacer nada por su parte respecto a esta vulnerabilidad: reaccionamos en cuanto se conoció el problema, primero con protecciones adicionales en la configuración del servidor, después instalando los parches de seguridad de PHP y, por último, actualizando el entorno del servidor.

Así, en las webs que alojamos, la situación ya está bajo control. **En cambio, si su web tiene un alojamiento externo, no podemos garantizarlo**, porque ahí no tenemos acceso directo a la configuración del servidor. En ese caso, conviene preguntar a su proveedor de alojamiento si ya ha instalado los parches de seguridad de PHP.

Seguirá habiendo nuevas vulnerabilidades. Por eso, la cuestión no es si un software tendrá fallos, sino con qué rapidez se detectan, se valoran y se corrigen. En la infraestructura que gestionamos, eso forma parte del mantenimiento técnico continuo.

En **Wisea** le ayudamos a mantener su web segura y al día. ¿Quiere saber si su web y su alojamiento están preparados? No dude en ponerse en contacto con nuestra agencia.