CIBERSEGURIDAD APLICADA

Guía para mitigar vulnerabilidades en aplicaciones con PHP

Qué revisar, cómo reducir la exposición y qué hacer mientras se prepara la actualización.

PHP2Shell agrupa las fallas **CVE-2026-109618** y **CVE-2026-109619**.
Pueden permitir ejecución remota de código sin autenticación, según las condiciones del entorno.

¿DÓNDE SE CONCENTRA EL RIESGO?

Aplicación web
Sitio, portal o API

›

Motor PHP
Versión y configuración

›

Información
Datos y servicios

La revisión debe llegar al PHP que ejecuta cada aplicación.

IDENTIFICAR
Ubica versiones y exposición.

CONTENER
Reduce el riesgo temporal.

CORREGIR
Actualiza y verifica.

01 / IDENTIFICACIÓN DEL RIESGO

Revisa el motor de la aplicación

Las fallas afectan el manejo de memoria durante solicitudes web. El impacto depende del despliegue, con mayor riesgo señalado para **Apache con mod_php. PHP-FPM** también requiere revisión.

¿Qué aplicaciones revisar?

- WordPress, Joomla, Drupal, Laravel y desarrollos a medida pueden utilizar PHP.
- El nombre del producto no determina por sí solo la exposición.
- Comprueba la versión activa, la configuración y los paquetes del proveedor.

Versiones que incorporan la corrección

Referencia de PHP para las dos fallas PHP2Shell, publicada el 21 de octubre.

RAMA PHP	VERSIÓN CORREGIDA
8.5	**8.5.12**
8.4	**8.4.27**
8.3	**8.3.36**
8.2	**8.2.35**

> **PHP 8.1 y anteriores**
> Sin mantenimiento regular del proyecto PHP.
> Planifica la migración y verifica si tu proveedor dispone de un parche específico.

Antes de seleccionar el paquete

Elige la versión estable corregida más reciente y compatible.
En Windows, los paquetes con sufijo -1 del 26 de octubre incluyen además una corrección de Brotli.
Un proveedor puede aplicar parches sin cambiar la versión base.

Actualizar solo el CMS o sus plugins no corrige necesariamente el motor PHP

02 / CONTENCIÓN TEMPORAL

Contén el riesgo mientras actualizas

Combina medidas según la criticidad del servicio. Define un responsable y una fecha de corrección para evitar que la contención se vuelva permanente.

01 Protección WAF

Activa reglas para patrones conocidos y revisa su aplicación. Un firewall de aplicaciones web puede filtrar ataques, pero no elimina la falla.

02 Acceso restringido

Limita el acceso público. Si usas un WAF, impide conexiones directas al servidor que puedan eludirlo.

03 Segmentación

Permite solo las conexiones necesarias hacia bases de datos y servicios internos. Separa cargas vulnerables de otros sistemas.

04 Configuración validada

Aplica medidas oficiales compatibles con tu entorno. Revisa la nota técnica inferior y prueba los cambios antes de desplegarlos.

05 Monitoreo reforzado

Busca solicitudes anómalas, errores, procesos inesperados y cambios de archivos. Si hay indicios de intrusión, activa la respuesta a incidentes.

06 Suspensión evaluada

Si el riesgo residual es inaceptable, coordina retirar temporalmente el servicio de Internet hasta aplicar las correcciones.

Nota técnica para el área de TI

PHP recomienda **desactivar session.upload_progress.enabled** en la configuración del servidor y reiniciar todos los workers. Revisa el aviso del 23 de octubre sobre **CVE-2026-115560**.
No confíes en **ini_set()** para aplicar esta medida antes del procesamiento de la solicitud.

Mitigar reduce la exposición. Actualizar corrige la vulnerabilidad

03 / PLAN DE ACCIÓN

De la identificación a la corrección

01 Identificar
Registra aplicación, PHP activo, servidor, exposición y responsable.

02 Priorizar
Atiende primero servicios públicos, críticos o con información sensible.

03 Preparar
Respalda datos y configuración. Prueba dependencias y define una reversión.

04 Actualizar
Instala paquetes corregidos. Redespliega contenedores y reinicia los servicios necesarios.

05 Validar
Comprueba todos los nodos y workers, funciones clave y registros de seguridad.

Lista de verificación

- ☐ Aplicaciones inventariadas
- ☐ Versiones vulnerables identificadas
- ☐ Sistemas críticos priorizados
- ☐ Respaldos disponibles
- ☐ Compatibilidad validada
- ☐ Actualizaciones aplicadas
- ☐ Funcionamiento y monitoreo revisados

Cierra el trabajo con evidencia

Documenta la versión desplegada, las pruebas y los pendientes.

Si detectas un posible compromiso, actualizar no reemplaza la investigación del incidente.