

CRÍTICO



WAF · CLOUDFLARE · MITIGACIÓN DE VULNERABILIDADES

Protección PHP2Shell en Cloudflare WAF.

Procedimiento de configuración del Conjunto de reglas administradas de Cloudflare para bloquear la explotación de CVE-2026-109618 y CVE-2026-109619.

VULNERABILIDAD	CVE	PLATAFORMA	EMITIDO
PHP2Shell	2026-109618/19	Cloudflare WAF	23/10/2026

MAPA DEL DOCUMENTO

Índice

01	Resumen ejecutivo	03
02	Contexto de la vulnerabilidad	04
03	Alcance y requisitos previos	05
04	Procedimiento de configuración	06
	Paso 1 · Acceso a la zona	06
	Paso 2 · Configuración de seguridad	06
	Paso 3 · Conjunto de reglas administradas	07
	Paso 4 · Anulación de las 7 reglas PHP2Shell	08
	Paso 5 · Despliegue y confirmación	09
05	Verificación y monitorización	10
06	Falsos positivos y reversión	11
07	Medidas complementarias	12
08	Anexo · Referencias	12

Control del documento

CÓDIGO	CYL-PROC-WAF-2026-014	
TIPO	Procedimiento técnico de mitigación	
VERSIÓN	1.0 · 23/10/2026	
CLASIFICACIÓN	Confidencial · Uso interno y cliente	
AUDIENCIA	Equipos de SOC/MDR, sistemas y administradores de Cloudflare	
VULNERABILIDAD	PHP2Shell · CVE-2026-109618 / CVE-2026-109619	
VERSIÓN	FECHA	DESCRIPCIÓN DEL CAMBIO
1.0	23/10/2026	Versión inicial: configuración del WAF de Cloudflare frente a PHP2Shell.

01 Resumen ejecutivo

El 21 de octubre de 2026 el proyecto PHP publicó parches de emergencia para **PHP2Shell**, dos vulnerabilidades críticas en el núcleo de PHP (**CVE-2026-109618** y **CVE-2026-109619**) que permiten la **ejecución remota de código sin autenticación** con los privilegios del proceso del servidor web. Afectan a cualquier instalación de PHP que sirva peticiones web (PHP-FPM, Apache con mod_php, php-cgi, FrankenPHP, LiteSpeed), con independencia de la aplicación desplegada (WordPress, Drupal, Joomla o desarrollos propios).

Cloudflare desplegó, horas antes de la divulgación pública, **7 reglas específicas** en su conjunto de reglas administradas (WAF) que bloquean los patrones de explotación conocidos. Ya se observa explotación activa y mutación de cargas para evadir las firmas.

Este procedimiento describe cómo **activar el Conjunto de reglas administradas de Cloudflare** y forzar las **7 reglas PHP2Shell en modo Bloquear**, minimizando el impacto sobre el tráfico legítimo cuando el conjunto no estaba activo previamente.

IMPORTANTE · EL WAF NO SUSTITUYE AL PARCHÉ

Las reglas del WAF son una **capa de contención temporal**. La única corrección definitiva es actualizar PHP a **8.5.12, 8.4.27, 8.3.36 u 8.2.35** (o a un paquete de distribución con el parche retroportado). Actualizar el CMS o sus plugins no corrige la vulnerabilidad.

2

CVE CRÍTICAS
RCE SIN AUTENTICACIÓN

7

REGLAS WAF
PHP2SHELL EN BLOQUEO

5

PASOS DE
CONFIGURACIÓN

~15'

TIEMPO ESTIMADO
POR ZONA

Acciones prioritarias recomendadas

01

0-24H · INMEDIATO

Activar el conjunto de reglas administradas y poner las 7 reglas PHP2Shell en **Bloquear** en todas las zonas con aplicaciones PHP.

02

0-72H · URGENTE

Actualizar el runtime de PHP en servidores, contenedores y hosting gestionado expuestos a Internet.

03

CONTINUO · MONITORIZACIÓN

Revisar eventos de seguridad filtrando por los ID de regla y ajustar excepciones ante falsos positivos.

02 Contexto de la vulnerabilidad

Ambos fallos se originan en que PHP deja la memoria en un estado corrupto cuando una petición termina de forma anómala. Fueron descubiertos por investigadores de Calif, OpenAI y Wiz, que demostraron RCE sin autenticación contra WordPress, Drupal y Joomla.

IDENTIFICADOR	DESCRIPCIÓN	SEVERIDAD
CVE-2026-109618	Encadenamiento de debilidades que provoca corrupción de memoria por agotamiento (<i>out-of-memory</i>) y permite ejecución remota de código con la cuenta del proceso web.	CRÍTICA
CVE-2026-109619	Estado global obsoleto (<i>stale global state</i>) que permite <i>use-after-free</i> en heap sin autenticación, divulgación de memoria del proceso y ejecución remota de código.	CRÍTICA

Versiones afectadas y corregidas

RAMA	VULNERABLE	CORREGIDA
8.5	< 8.5.12	8.5.12
8.4	< 8.4.27	8.4.27
8.3	< 8.3.36	8.3.36
8.2	< 8.2.35	8.2.35
7.4 – 8.1	Todas	Backport en código fuente / proveedor LTS
≤ 7.3	Todas	Migrar a versión soportada

Superficie expuesta

SAPI / DESPLIEGUE	RIESGO
Apache + mod_php	MÁXIMO
PHP-FPM	ALTO
php-cgi	ALTO
FrankenPHP	ALTO
LiteSpeed (LSAPI)	ALTO

En mod_php existe un exploit demostrado que se dispara **antes de ejecutar código de la aplicación**.

Cronología relevante

20/10	AVISO PREVIO El equipo de PHP anuncia la publicación inminente de parches de seguridad críticos.
21/10	03:02 UTC · CLOUDFLARE Cloudflare despliega las 7 reglas en sus conjuntos administrados (Free y de pago) y observa los primeros intentos de explotación.
21/10	DIVULGACIÓN PÚBLICA Publicación de PHP 8.5.12, 8.4.27, 8.3.36 y 8.2.35 y de los avisos de seguridad.

03 Alcance y requisitos previos

Alcance

Aplica a todas las zonas (dominios) gestionadas en Cloudflare que publiquen aplicaciones o servicios basados en PHP, o en las que no se tenga certeza de la tecnología del origen. Cubre la configuración del WAF a nivel de zona desde el panel de Cloudflare.

Cobertura por plan de Cloudflare

PLAN	CONJUNTO DE REGLAS	ACCIÓN REQUERIDA
Free	Cloudflare Managed Free Ruleset	Protección desplegada automáticamente. Solo verificar (sección 05).
Pro · Business · Enterprise	Cloudflare Managed Ruleset	Aplicar este procedimiento: activar el conjunto y confirmar las 7 reglas en Bloquear.
Todos	Managed Response Firewall Default	Regla de respuesta <i>Default block for High confidence Signatures</i> activa por defecto.

Requisitos previos

☐	Acceso al panel de Cloudflare con rol Super Administrator, Administrator o Firewall / WAF Admin sobre la zona.	ACCESO
☐	Inventario de zonas con backend PHP y responsable técnico de cada aplicación identificado.	INVENTARIO
☐	Ventana de cambio aprobada o procedimiento de cambio de emergencia activado (riesgo crítico con explotación activa).	GESTIÓN
☐	Comprobación del estado inicial del Conjunto de reglas administradas (activo / inactivo) y de las anulaciones existentes.	LÍNEA BASE
☐	Canal de comunicación con el cliente/negocio para notificar posibles bloqueos de tráfico legítimo.	COMUNICACIÓN

Estrategia según el estado inicial

ESCENARIO A · CONJUNTO YA ACTIVO

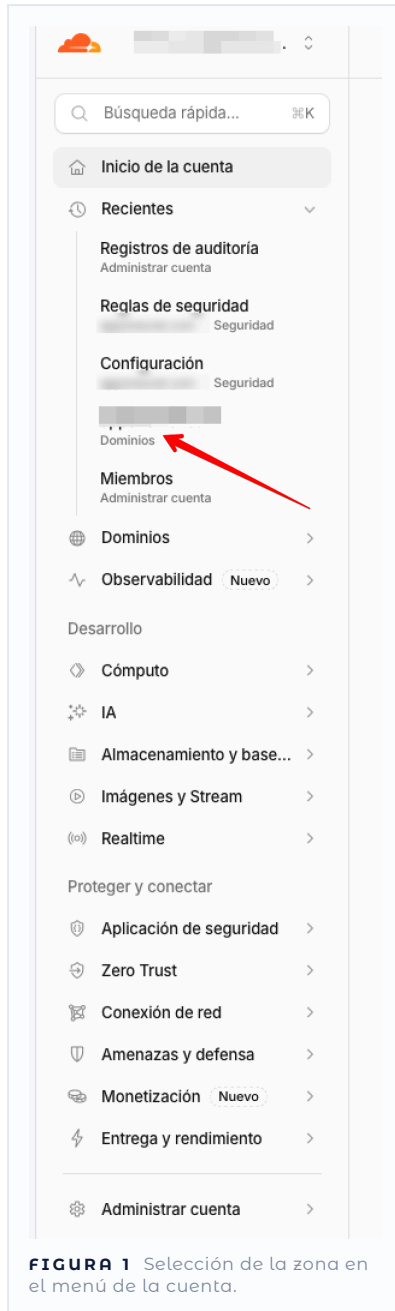
Mantener la configuración existente y verificar que **ninguna anulación** desactiva o rebaja la acción de las 7 reglas PHP2Shell. Forzarlas a **Bloquear** si fuese necesario.

ESCENARIO B · CONJUNTO NO ACTIVO

Activar el conjunto (≈ 837 reglas) con la acción del conjunto en **Registro (Log)** para no impactar en producción, y anular **solo las 7 reglas PHP2Shell** a **Bloquear**.

El número total de reglas del conjunto administrado puede variar con las actualizaciones de Cloudflare. Si la acción *Registro* no está disponible en el plan contratado, mantener la acción predeterminada del conjunto y reforzar la monitorización de eventos durante las primeras 48 h.

04 Procedimiento de configuración



PASO 01

Acceder a la zona

Inicio de la cuenta → Dominios → <dominio>

Iniciar sesión en `dash.cloudflare.com` y seleccionar la cuenta correspondiente. Desde el menú lateral, abrir **Dominios** (o la entrada reciente) y seleccionar el **dominio a proteger**.

Repetir el procedimiento completo para cada zona del inventario con backend PHP.

consejo

Utilizar la **Búsqueda rápida** (⌘K / Ctrl+K) para localizar la zona directamente cuando la cuenta gestione muchos dominios.

PASO 02

Abrir la configuración de seguridad

<dominio> → Seguridad → Configuración

Dentro de la zona, desplegar el menú **Seguridad** y pulsar **Configuración**. Esta vista reúne las herramientas de detección y protección de la zona, incluido el WAF administrado.



PASO
03

Activar el Conjunto de reglas administradas de Cloudflare

[Seguridad](#) → [Configuración](#) → [Conjunto de reglas administradas de Cloudflare](#)

Localizar el bloque **Conjunto de reglas administradas de Cloudflare** (puede filtrarse por el grupo *Exploits de aplicaciones web*) y comprobar el interruptor de **Estado**:

- **Activo:** aplicar el **Escenario A**. Pulsar **Ver conjunto de reglas** para revisar las anulaciones existentes y continuar en el Paso 4.
- **Inactivo:** aplicar el **Escenario B**. Activar el interruptor; al desplegar el conjunto, establecer la acción del conjunto en **Registro** (*Log*) y guardar.

Configuración [Ver documentación](#)

Configuración y herramientas utilizadas para personalizar y mejorar las detecciones de Cloudflare y la postura de seguridad de tu dominio.

Q Buscar configuraciones, descripciones o herramientas de detección [Filtrar por grupos](#)

Abuso de API 8 configuraciones

Nombre	Configuraciones	Estado
Certificados de cliente ⓘ		
Emita nuevos certificados de cliente y administre los existentes en certificados de cliente. Los certificados de cliente pueden utilizarse para aplicar el cifrado de seguridad mutua de la capa de transporte (mutual Transport Layer Security, mTLS). Crear certificado		
Conjunto de reglas administradas de Cloudflare ⓘ		☒
Este conjunto de reglas, creado y mantenido por Cloudflare, ofrece una protección rápida y eficaz para todas sus aplicaciones. Cloudflare recomienda habilitar las reglas cuyas etiquetas correspondan a su paquete tecnológico. Crear una regla de excepción Ver conjunto de reglas Exploits de aplicaciones web Ataques DDoS Tráfico de bots		
Descubrimiento de activos web ⓘ		☒
Descubre automáticamente los activos web de tu aplicación para mapear tu área de superficie de ataque y recibir información adicional. Siempre activo		
Etiquetas de endpoint ⓘ		
Etiqueta los endpoints para organizarlos por caso de uso Administrar etiquetas		
Reglas de fallback personalizadas		
Tome medidas contra las solicitudes a endpoints que no estén guardadas en el panel de activos web. El uso de detecciones fallback puede protegerle contra endpoints heredados o zombis que podría desconocer. Crear regla de fallback personalizada		

↓ [Mostrar todas las 8 configuraciones en Abuso de API](#)

FIGURA 3 Conjunto de reglas administradas de Cloudflare con el estado activado.

ESCENARIO B · POR QUÉ MODO REGISTRO

Activar de golpe el conjunto completo (≈ 837 reglas) en bloqueo sobre una aplicación que nunca lo ha tenido puede generar **falsos positivos** y cortes de servicio. En modo Registro el resto de reglas solo registra eventos, lo que permite analizarlos y promoverlas a bloqueo de forma controlada en una fase posterior.

Las **7 reglas PHP2Shell** sí deben quedar en **Bloquear** desde el primer momento mediante anulación individual (Paso 4).

PASO
04

Anular las 7 reglas PHP2Shell a Bloquear

[Ver conjunto de reglas](#) → [Buscar / filtrar por etiqueta](#) → [Anulaciones de reglas](#)

Desde **Ver conjunto de reglas** (o editando la regla de implementación *Execute* del conjunto en **Reglas de seguridad** → **Reglas administradas**), buscar las reglas de PHP2Shell filtrando por las etiquetas **cve-2026-109618** o por la descripción **PHP Remote Code Execution Attack**.

Seleccionar las **7 reglas**, establecer **Acción: Bloquear** y **Estado: Habilitado**, y pulsar **Aplicar configuración del conjunto de reglas**. El resultado debe coincidir con la Figura 4.

Anulaciones de reglas

Descripción/id. de la regla	Etiqueta	Acción	Habilitado
PHP Remote Code Execution Attack (... c1d409ad838f47f59446f21cc438d5dd	php cve-2026-109619 cve-2026-109618 remote-code-execution	Bloquear	Habilitado
PHP Remote Code Execution Attack (... f9a45927414245e3a64bb12d0a0c2f64	php cve-2026-109619 cve-2026-109618 remote-code-execution	Bloquear	Habilitado
PHP Remote Code Execution Attack (... 771c654ae1154d4daa72f4e1545d163c	php cve-2026-109619 cve-2026-109618 remote-code-execution	Bloquear	Habilitado
PHP Remote Code Execution Attack (... 217005865f0145f392300bac212afcc9	php cve-2026-109619 cve-2026-109618 remote-code-execution	Bloquear	Habilitado
PHP Remote Code Execution Attack (... 38efdb17ea594501bb55a1d71867b12e	php cve-2026-109619 cve-2026-109618 remote-code-execution	Bloquear	Habilitado
PHP Remote Code Execution Attack (... 4148ae686fdb4d01be673fab9d9c073d	php cve-2026-109619 cve-2026-109618 remote-code-execution	Bloquear	Habilitado
PHP Remote Code Execution Attack (... 1389aa259617437392ce149c48143645	php cve-2026-109619 cve-2026-109618 remote-code-execution	Bloquear	Habilitado

FIGURA 4 Anulaciones de reglas: las 7 reglas PHP2Shell en acción Bloquear y estado Habilitado.

PASO 04 · REFERENCIA

Reglas a anular · Cloudflare Managed Ruleset (Pro / Business / Enterprise)

Cloudflare ha indicado que las descripciones de estas reglas pueden cambiar (inicialmente se publicaron como *Generic Rules – Anomalous Execution 1-7*); **identificarlas siempre por su ID**.

#	ID DE LA REGLA	ETIQUETAS	ACCIÓN	ESTADO
01	c1d409ad838f47f59446f21cc438d5dd	php cve-2026-109618 cve-2026-109619	BLOQUEAR	HABILITADO
02	f9a45927414245e3a64bb12d0a0c2f64	php cve-2026-109618 cve-2026-109619	BLOQUEAR	HABILITADO
03	771c654ae1154d4daa72f4e1545d163c	php cve-2026-109618 cve-2026-109619	BLOQUEAR	HABILITADO
04	217005865f0145f392300bac212afcc9	php cve-2026-109618 cve-2026-109619	BLOQUEAR	HABILITADO
05	38efdb17ea594501bb55a1d71867b12e	php cve-2026-109618 cve-2026-109619	BLOQUEAR	HABILITADO
06	4148ae686fdb4d01be673fab9d9c073d	php cve-2026-109618 cve-2026-109619	BLOQUEAR	HABILITADO
07	1389aa259617437392ce149c48143645	php cve-2026-109618 cve-2026-109619	BLOQUEAR	HABILITADO
ID DEL CONJUNTO (PLANES DE PAGO)			efb7b8c949ac4650a09736fc376e9aee	
ID DEL CONJUNTO (PLAN FREE)			77454fe2d30c4220b5701f6fdbfb893ba	
REGLA DE RESPUESTA (TODOS LOS PLANES)			afffe22785674c80a31875c848d2242a	

PRECEDENCIA

Las **excepciones** (*skip*) se evalúan antes que las anulaciones. Revisar que no exista una regla de excepción que omita el conjunto administrado para rutas o hosts PHP de la zona.

**PASO
05****Desplegar y confirmar la configuración**

[Reglas de seguridad](#) → [Reglas administradas](#)

Guardar/implementar los cambios y comprobar en **Reglas de seguridad**, filtrando por **Reglas administradas**, que la regla de implementación del conjunto aparece **habilitada** y que sus anulaciones reflejan:

- Acción del conjunto: **predeterminada** (Escenario A) o **Registro** (Escenario B).
- Las **7 reglas PHP2Shell** en **Bloquear · Habilitado**.
- Ninguna anulación o excepción adicional que deshabilite estas reglas.

Documentar en el ticket de cambio la zona, la fecha/hora, el escenario aplicado y el operador.

05 Verificación y monitorización

Tras el despliegue, validar que la protección está operativa y vigilar la actividad asociada. La ausencia de eventos **no implica** que las reglas estén inactivas: confirmar siempre también la configuración (Paso 5).

Revisión de eventos de seguridad

- 01** **ACCESO**
Abrir **Seguridad** → **Análisis** → **Eventos** de la zona.
- 02** **FILTRO**
Agregar filtro → campo **ID de regla** → operador **es igual a** → introducir cada uno de los 7 ID (o filtrar por servicio *Reglas administradas*).
- 03** **VENTANA**
Utilizar intervalos cortos (últimas 24 h) y ampliar progresivamente.
- 04** **ANÁLISIS**
Expandir cada evento para revisar petición, ruta, IP origen, ASN, país y acción aplicada (**Bloquear**).

Lista de comprobación post-implantación

- | | | |
|--------------------------|---|---------|
| ☐ | Conjunto de reglas administradas de Cloudflare activo en la zona. | CONFIG. |
| ☐ | Las 7 reglas PHP2Shell en Bloquear · Habilitado , verificadas por ID. | CONFIG. |
| ☐ | Sin excepciones que omitan el conjunto en hosts o rutas PHP. | CONFIG. |
| ☐ | Aplicación accesible y funcional tras el cambio (prueba de humo de login, formularios y subida de ficheros). | NEGOCIO |
| ☐ | Eventos de bloqueo revisados; IPs atacantes correladas en SIEM/MDR y, si procede, bloqueadas. | SOC |
| ☐ | En Escenario B: revisión de eventos en modo Registro a las 48-72 h para planificar el paso a bloqueo del conjunto completo. | SOC |
| ☐ | Ticket de cambio actualizado con evidencias (capturas de anulaciones y de eventos). | GESTIÓN |

DETECCIÓN DE COMPROMISO PREVIO

Si se registran bloqueos de estas reglas, o la zona estuvo expuesta sin protección antes del 21/10/2026, revisar en el origen: procesos hijos inesperados del usuario del servidor web, ficheros PHP nuevos o modificados en directorios web/subida, y conexiones salientes anómalas. Escalar al equipo de DFIR ante cualquier indicio.

06 Falsos positivos y reversión

Gestión de falsos positivos

Si alguna de las 7 reglas bloquea tráfico legítimo, **no desactivar el conjunto completo ni las reglas**. Aplicar la medida más acotada posible:

- 01 IDENTIFICAR**
Localizar en Eventos el ID de regla, la ruta, el método y los parámetros implicados.
- 02 ACOTAR**
Crear una **regla de excepción** (*Crear una regla de excepción*) que omita **únicamente ese ID** para la ruta / host / IP de origen concretos (p. ej., integraciones de confianza).
- 03 COMPENSAR**
Priorizar el parcheo de PHP en ese origen y documentar el riesgo aceptado con fecha de caducidad de la excepción.

Plan de reversión

SITUACIÓN	ACCIÓN DE REVERSIÓN
Escenario B con impacto generalizado	Mantener las 7 anulaciones en Bloquear y verificar que la acción del conjunto está en Registro. Si el impacto persiste, revisar los eventos por ID antes de cualquier desactivación.
Falso positivo de una regla PHP2Shell	Excepción acotada por ID de regla y ruta (ver arriba). Nunca deshabilitar las 7 reglas de forma global.
Error de configuración	Restaurar la configuración de la línea base documentada (estado inicial del conjunto y anulaciones) y repetir desde el Paso 3.

APROBACIÓN

Cualquier desactivación total de las reglas PHP2Shell en una zona con PHP sin parchear supone **exponer un RCE crítico con explotación activa** y requiere aprobación expresa del responsable de seguridad del cliente, registrada en el ticket.

Roles y responsabilidades

ROL	RESPONSABILIDAD
Operador SOC / MDR	Ejecución de los pasos 1-5, verificación y monitorización de eventos.
Responsable de la aplicación	Pruebas funcionales, validación de falsos positivos y parcheo del runtime PHP.
Responsable de seguridad	Aprobación del cambio, excepciones y aceptación de riesgos.

07 Medidas complementarias

- 01

CORRECCIÓN DEFINITIVA

Actualizar PHP a **8.5.12 / 8.4.27 / 8.3.36 / 8.2.35**, reconstruir y redespregar contenedores y verificar la versión efectiva (`php -v` y SAPI en uso). Exigir el parche a los proveedores de hosting gestionado.
- 02

MITIGACIÓN PARCIAL · CVE-2026-109618

`memory_limit=-1` (vía `php_admin_value`), `post_max_size` a 8M (sin subidas) o 32M, y límites de contenedor/cgroup que terminen solo el worker afectado.
- 03

MITIGACIÓN PARCIAL · CVE-2026-109619

`session.upload_progress.enabled=0` ; en PHP 8.5, `fatal_error_backtraces=0` ; reiniciar todos los workers y corregir errores fatales alcanzables por un atacante.
- 04

REDUCCIÓN DE EXPOSICIÓN

Restringir el acceso a servicios no parchados (allowlist, Zero Trust) o retirarlos temporalmente; limitar subidas y su tamaño.

08 Anexo · Referencias

FUENTE	CONTENIDO
BleepingComputer	PHP ships emergency patches for critical PHP2Shell flaws (21/10/2026).
Endor Labs	PHP2Shell: critical vulnerabilities in PHP (CVE-2026-109618, CVE-2026-109619).
PPC Land	Cloudflare blocks PHP2Shell exploits 9 hours before PHP flaws went public.
Techdows	Cloudflare PHP2Shell WAF rule: how to turn it on and why it is not a fix.
Cloudflare Docs	WAF Managed Rules · Overrides y excepciones de conjuntos administrados.

Información vigente a 23/10/2026. Cloudflare puede añadir o modificar reglas a medida que evolucionen las cargas de ataque; revisar periódicamente las etiquetas `cve-2026-109618` `cve-2026-109619` en el conjunto administrado.