

Boletín de alerta

Boletín Nro.: 117

Fecha de publicación: 21/10/2026

Tema: Alerta 2026-117 Dos vulnerabilidades críticas en PHP

Traffic Light Protocol (TLP): White

Actualización: 21/10/2026 11:30 AM CDMX

Producto(s) afectado(s):

ACTUALIZACIÓN: ya esta la actualización de parte del equipo de PHP

<https://www.php.net/downloads.php?source=Y>

Rama de PHP	Estado de afectación	Versión corregida
PHP 8.5.x	Pendiente de confirmación oficial del rango afectado	Pendiente de publicación
PHP 8.4.x	Pendiente de confirmación oficial del rango afectado	Pendiente de publicación
PHP 8.3.x	Pendiente de confirmación oficial del rango afectado	Pendiente de publicación
PHP 8.2.x	Pendiente de confirmación oficial del rango afectado	Pendiente de publicación
PHP 8.1 y anteriores	Alcance pendiente de confirmación; ramas fuera del soporte oficial de PHP	Sin corrección anunciada; verificar también el soporte del proveedor

El estado de afectación procede del aviso preventivo de PHP; la situación de soporte de las ramas antiguas consta en su listado de versiones sin soporte

Descripción

El equipo de seguridad de PHP anunció una actualización de emergencia para corregir dos vulnerabilidades críticas, identificadas por investigadores como CVE-2026-109618 y CVE-2026-109619, relacionadas con ejecución remota de código. PHP asignó a ambas una puntuación CVSS v4.0 de 9.2 y programó la publicación para el 21 de octubre de 2026 a las 14:00 UTC —11:00, UTC-3—, aunque podría adelantarla ante divulgación de detalles o evidencia de explotación.

Al momento de la consulta, el aviso oficial todavía no especificaba las versiones afectadas, los requisitos de explotación ni las versiones corregidas. Se insta a preparar el despliegue urgente y mantener vigilancia sobre los canales oficiales.

Las dos vulnerabilidades permiten ejecución remota de código (RCE) y un equipo de investigación ya habría reproducido CVE-2026-109618. Parte de la información se filtró antes de la divulgación prevista, pero el fabricante mantiene pendientes los detalles técnicos completos.

A continuación, se detallan ambas vulnerabilidades:

Identificador	Impacto reportado	Puntuación oficial anunciada	Información pendiente
CVE-2026-109618	Ejecución remota de código; Se reporta haber reproducido la falla.	CVSS v4.0: 9.2	Causa técnica, configuraciones afectadas, requisitos y versiones corregidas.
CVE-2026-109619	Ejecución remota de código reportada por investigadores.	CVSS v4.0: 9.2	Causa técnica, configuraciones afectadas, requisitos y versiones corregidas.

El **riesgo** principal es que la publicación de los parches o de una prueba de concepto (POC) funcional reduzca rápidamente la barrera para desarrollar y automatizar intentos de explotación: los atacantes podrían analizar los cambios, adaptar herramientas y realizar escaneos masivos contra servicios PHP expuestos a Internet. Dado el potencial de ejecución remota de código de CVE-2026-109618 y CVE-2026-109619, una demora en la remediación podría facilitar el compromiso de servidores, el robo de información o la instalación de puertas traseras.

Aunque todavía no se conocen todos los requisitos de explotación ni puede asegurarse que cualquier instalación sea vulnerable, debe anticiparse una ventana de respuesta corta y preparar la actualización inmediata de los sistemas afectados, sin esperar a observar ataques en la propia organización.

Mitigación Temporal

La recomendación compartida por el conocido investigador Kostas^[1] consiste en deshabilitar el seguimiento del progreso de cargas mediante la siguiente directive en el archivo php.ini (si estas en php 8.2) :

```
session.upload_progress.enabled = Off
```

Debe presentarse como una medida provisional de reducción de exposición, no como una solución validada para ambas CVE. La propia publicación expresa dudas sobre su cobertura; PHP aún no confirma en su aviso oficial que este ajuste bloquee las dos vulnerabilidades.

Consideraciones de implementación

- Aplicar el cambio en la configuración utilizada por el servicio web correspondiente, no únicamente en la configuración de PHP para línea de comandos.
- Recargar o reiniciar el servicio que ejecuta PHP, según la arquitectura: PHP-FPM o Apache cuando utiliza PHP como módulo. No corresponde reiniciar ambos indiscriminadamente.
- Verificar el valor efectivo mediante un mecanismo de diagnóstico restringido y retirarlo al finalizar; no publicar páginas `phpinfo()` accesibles desde Internet.
- Probar las funciones de carga de archivos. La directiva controla el seguimiento de progreso, no la habilitación general de las cargas; pueden dejar de funcionar las barras de progreso que dependen de esta característica.

La documentación de PHP identifica esta opción como habilitada por defecto y de tipo `INI_PERDIR`; no debe intentarse aplicar la medida mediante un `ini_set()` dentro del código de la aplicación.

La distinción de la captura entre versiones anteriores y posteriores a PHP 8.2 tampoco constituye una matriz oficial de afectación ni garantiza que las versiones antiguas reciban una corrección.

Solución

El proveedor ha publicado parches de seguridad para mitigar el problema, puede encontrarlos en el siguiente enlace:

<https://www.php.net/downloads.php?source=Y>

Si utiliza un hosting como proveedor de servicios web, como Hostinger y demás, ellos suelen realizar las actualizaciones de forma automática del core de PHP. Favor contactar con el equipo de soporte correspondiente y validar la versión.

Información adicional:

- PHP — anuncio oficial de la actualización de emergencia:
<https://www.php.net/index.php#2026-10-20-1php>
- BleepingComputer — aviso y declaraciones de investigadores:
<https://www.bleepingcomputer.com/news/security/php-warns-admins-of-two-critical-flaws-emergency-patches-coming-tomorrow/bleepingcomputer>
- WatchTower — seguimiento de CVE-2026-109618 y CVE-2026-109619:
<https://watchtower.com/intelligence/php-cve-2026-109618-faq/watchtower>
- PHP — documentación de `session.upload_progress.enabled`:
<https://www.php.net/manual/en/session.configuration.php#ini.session.upload-progress.enabled>
- <https://www.php.net/downloads.php?source=Y>

[1] <https://x.com/Kostastsale/status/2112774685792571463>