

Se detectaron dos vulnerabilidades críticas en PHP, una tecnología ampliamente utilizada para el funcionamiento de sitios, aplicaciones y servicios web. Las fallas fueron identificadas como CVE-2026-109618 y CVE-2026-109619 y presentan una gravedad de 9,2 sobre 10.

¿Qué pasó?

Las vulnerabilidades afectan al propio entorno de ejecución de PHP y, bajo determinadas condiciones, pueden permitir que un atacante ejecute código de manera remota en un servidor vulnerable sin necesidad de autenticarse previamente.

Esto significa que el riesgo no depende necesariamente de una falla en el sitio o la aplicación. Incluso una aplicación correctamente desarrollada puede quedar expuesta si funciona sobre una versión vulnerable de PHP.

¿Por qué es importante?

PHP es una tecnología utilizada detrás de numerosos sitios web, portales, aplicaciones y servicios online. Por ese motivo, una vulnerabilidad presente en su núcleo puede alcanzar a diferentes tipos de sistemas que dependen de esta tecnología para funcionar.

Las fallas no implican que todos los sitios que utilizan PHP hayan sido comprometidos, pero sí hacen necesario identificar los sistemas potencialmente afectados y actualizar las versiones vulnerables.

¿Qué versiones están afectadas?

Las versiones corregidas publicadas por PHP el 21 de octubre de 2026 son:

- PHP 8.5.12
- PHP 8.4.27
- PHP 8.3.36
- PHP 8.2.35

Las ramas PHP 8.1 y anteriores se encuentran fuera del soporte oficial del proyecto PHP y no cuentan con una nueva versión oficial equivalente que resuelva estas vulnerabilidades. Para

esos entornos se recomienda avanzar hacia una rama soportada o aplicar las actualizaciones proporcionadas por el proveedor o la distribución correspondiente.

¿Qué hacer?

Si administrás un sitio, aplicación o servicio web:

- Verificá la versión de PHP utilizada por el sistema.
- Actualizá a una de las versiones corregidas o aplicá el paquete de seguridad correspondiente proporcionado por tu proveedor.
- Comprobá que la actualización se haya aplicado correctamente en todos los entornos que utilicen PHP.

Si no administrás directamente el servidor, consultá con tu proveedor de hosting o con el equipo técnico responsable para confirmar que la actualización haya sido realizada.

Actualizar es la principal medida de protección

Las mitigaciones temporales pueden reducir determinados escenarios de riesgo, pero no reemplazan la actualización de PHP. La recomendación principal es aplicar las versiones corregidas y mantener los sistemas y componentes actualizados.

Desde BA-CSIRT, el Centro de Ciberseguridad del Gobierno de la Ciudad de Buenos Aires, recomendamos verificar los entornos que utilizan PHP y aplicar las actualizaciones de seguridad correspondientes lo antes posible.