

PHP descubre otro fallo de seguridad sin parche apenas dos días después de una actualización urgente: Cloudflare y Amazon ya detectan ataques contra los anteriores

PHP descubre un tercer fallo de seguridad mientras Cloudflare y Amazon detectan ataques contra las dos vulnerabilidades críticas corregidas el miércoles

Parece que PHP no está teniendo una buena semana. El pasado 21 de octubre sus responsables publicaban actualizaciones de emergencia para corregir dos vulnerabilidades críticas y hoy, apenas dos días después, han reconocido un tercer fallo de seguridad que todavía no tiene parche. Y todo mientras Cloudflare y Amazon ya están detectando ataques contra los dos anteriores.



Según recoge The Hacker News, el nuevo problema se ha identificado como CVE-2026-115560 y podría permitir ejecutar código malicioso en un servidor de forma remota. No obstante, PHP considera poco probable que pueda aprovecharse, por lo que ha recomendado desactivar temporalmente una función en lugar de publicar otra actualización urgente.

Los ataques contra PHP2Shell ya se cuentan por millones

El pasado miércoles se publicaron las versiones PHP 8.5.12, 8.4.27, 8.3.36 y 8.2.35 para corregir dos vulnerabilidades conocidas como PHP2Shell. Los fallos, identificados como CVE-2026-109618 y CVE-2026-109619, habían recibido una puntuación de gravedad de 9,2 sobre 10 y permitían ejecutar código malicioso sin autenticación bajo determinadas condiciones.

Y parece que los atacantes ya estaban intentando aprovecharlos antes de que se publicasen las correcciones. Amazon asegura que sus sistemas de vigilancia registraron un intento de

explotación el 17 de octubre, cuatro días antes de la divulgación de los fallos. Cloudflare, por su parte, observó decenas de miles de intentos en los primeros 45 minutos del anuncio.

La cifra no tardó demasiado en dispararse. Para las primeras horas del 22 de octubre, Cloudflare ya estaba registrando millones de intentos de ataque. Además, Sophos y Arctic Wolf han detectado que algunos delincuentes están intentando instalar una variante de Mirai, una red de dispositivos infectados que permite utilizarlos para lanzar ataques coordinados.

Eso sí, aunque los intentos son reales, todavía no se han acreditado ejecuciones de código satisfactorias en las investigaciones citadas. La situación recuerda a otros agujeros de seguridad que ya estaban siendo atacados, como sucedió con Chrome. En este caso, además, los detalles de PHP2Shell se filtraron antes de la fecha prevista y obligaron a adelantar los parches.

Un tercer fallo que PHP no tiene previsto corregir de urgencia

Cuando todavía se estaban instalando las actualizaciones del miércoles, PHP ha publicado un nuevo aviso. Esta vez el problema afecta a la gestión de sesiones y al seguimiento de las subidas de archivos, aunque sólo puede explotarse con una combinación poco habitual de configuraciones. Por ahora tampoco se conocen ataques que hayan conseguido aprovechar esta vulnerabilidad.

Para evitar problemas, The PHP Foundation recomienda establecer `session.upload_progress.enabled=0` desde la configuración del servidor hasta la siguiente actualización. La organización ha señalado que quienes ya aplicaron esta medida el miércoles no necesitan hacer nada más, puesto que

también se había recomendado como protección frente a una de las dos vulnerabilidades anteriores.

No es la primera vez que una actualización de emergencia deja problemas pendientes, aunque conviene señalar que el nuevo fallo es independiente de PHP2Shell. Por ahora, PHP no ha comunicado qué versiones están afectadas ni cuándo publicará la corrección definitiva, y tampoco ha asignado una puntuación de gravedad a CVE-2026-115560.

Hay otra cuestión para quienes utilizan versiones antiguas del lenguaje. PHP 8.1 y anteriores ya no reciben nuevas versiones oficiales, aunque se han publicado correcciones de código para 7.4, 8.0 y 8.1. Si tienes una página en WordPress o utilizas un alojamiento compartido, conviene comprobar que tu proveedor ha instalado los parches correspondientes.

Por ahora, los responsables de PHP mantienen que el nuevo fallo tiene unas condiciones de explotación demasiado específicas como para justificar otra actualización urgente. La próxima corrección llegará con una versión ordinaria, cuya fecha todavía no se ha anunciado. Mientras tanto, los administradores deberán mantener desactivada la función afectada y comprobar que sus servidores están protegidos frente a PHP2Shell.

Fuente: larazon.