Han surgido informes sobre una nueva vulnerabilidad crítica de seguridad que afecta a PHP, la cual podría ser explotada para ejecutar código de forma remota en determinadas condiciones.

La vulnerabilidad, identificada como CVE-2024-4577, se ha descrito como una vulnerabilidad de inyección de argumentos CGI que impacta todas las versiones de PHP instaladas en el sistema operativo Windows.

De acuerdo con un investigador de seguridad de DEVCORE, esta falla permite eludir las protecciones establecidas para otra vulnerabilidad, CVE-2012-1823.

> *«Al implementar PHP, el equipo no se percató de la función de Best Fit en la conversión de codificación del sistema operativo Windows»,* comentó el investigador de seguridad Orange Tsai.
>
> *«Este error permite a atacantes no autenticados eludir la protección anterior de CVE-2012-1823 mediante secuencias de caracteres específicas. Se puede ejecutar código arbitrario en servidores PHP remotos a través de un ataque de inyección de argumentos.»*

Después de una divulgación responsable el 7 de mayo de 2024, se ha lanzado una solución para la vulnerabilidad en las versiones de PHP 8.3.8, 8.2.20 y 8.1.29.

DEVCORE ha advertido que todas las instalaciones de XAMPP en Windows son vulnerables por defecto cuando están configuradas para usar las configuraciones regionales de chino tradicional, chino simplificado o japonés.

La empresa taiwanesa también recomienda a los administradores que abandonen el obsoleto CGI de PHP y opten por una solución más segura como Mod-PHP, FastCGI o PHP-FPM.

> *«Esta vulnerabilidad es increíblemente sencilla, pero eso también es lo que la hace interesante. ¿Quién habría pensado que un parche, revisado y probado como seguro durante los últimos 12 años, podría ser eludido debido a una característica menor de Windows?»*, dijo Tsai.

La Fundación Shadowserver, en una publicación compartida en X, informó que ya ha detectado intentos de explotación de la vulnerabilidad en sus servidores honeypot dentro de las 24 horas posteriores a la divulgación pública.

watchTowr Labs informó que logró desarrollar un exploit para CVE-2024-4577 y ejecutar código de forma remota, lo que hace imperativo que los usuarios apliquen rápidamente los parches más recientes.

> *«Un error desagradable con un exploit muy simple»,* comentó la investigadora de seguridad Aliz Hammond.
>
> *«Se insta a aquellos que utilicen una configuración afectada bajo una de las configuraciones regionales afectadas – chino (simplificado o tradicional) o japonés – a actualizar lo antes posible, ya que la vulnerabilidad tiene una alta probabilidad de ser explotada en masa debido a la baja complejidad del exploit.»*