Cómo Comprobar Si Tu Web Es Vulnerable Al Nuevo Fallo De WordPress

El pasado 20 de noviembre, *WordPress* ha anunciado una **vulnerabilidad critica de cross-site scripting** en el sistema de gestión de contenido más popular y ampliamente usado en la Internet. Inicialmente fue descubierto por Jouko Pynnonen, con la compañía de Finnish IT Klikki Oy, la vulnerabilidad podría permitir a usuarios anónimos **comprometer sitios web que usan versiones anteriores** a la 3.9.3 en WordPress.

Se trata de una vulnerabilidad bastante grave, ya que *afecta a millones de sitios web* a través de Internet y podría permitir a un usuario hacerse con el control completo de estos sitios web y, potencialmente, el sistema operativo subyacente. Según las estadísticas de WordPress, alrededor del **86 por ciento de todos los sitios de WordPress** estaban usando una versión vulnerable a partir del 20 de noviembre de 2014. Los sitios Explotados entonces se podrían utilizar para atacar a otros usuarios, o si el sistema operativo se veía afectado, la máquina podría ser utilizada como parte de una **botnet**. Los informes indican que esta vulnerabilidad está siendo activamente explotada y que el código de explotación se ha hecho disponible en Internet para que otros puedan usar y modificar.

Detalles Técnicos

El medio de ataque principal de esta vulnerabilidad es mediante la adición de **código JavaScript malicioso para ciertos campos de texto**, concretamente la posición de cajas contenidas en los artículos y blogs de WordPress. El código JavaScript malicioso entonces se desencadena cuando un usuario ve el comentario sea a través de una entrada de blog, página o en la sección «Comentarios» del panel de administración. El JavaScript se ejecuta con los mismos privilegios del usuario que lo desencadenó. Como tal, el escenario más impactante es cuando el comentario es visto por el administrador del sitio web.

La vulnerabilidad se introduce a través de una **función de formateo de texto llamada wptexturize()**. Esta función está activada por defecto y es utilizada por WordPress para modificar el texto fijado o comentarios para presentar una salida más legible y visualmente atractiva. El proceso de texturización puede ser subvertido, sin embargo, mediante la adición de una mezcla especialmente diseñado de cuadrados y ángulos para el comentario.

¿Cómo saber si eres vulnerable?

Si eres usuario de WordPress, de seguro te gustara saber si eres vulnerable a este peligroso fallo. La **versión de WordPress** de tu sitio deben ser visible en la sección administrativa, ya sea en el encabezado o pie de página, dependiendo de la versión.

También es posible que desee considerar el uso de una *herramienta de análisis* como Qualys FreeScan, que le puede dar un panorama general de su seguridad y recomendaciones para soluciones eficaces. En última instancia, es importante verificar si su sitio se ha visto comprometida y luego actualizar tus sitios de inmediato para disminuir el impacto potencial de esta vulnerabilidad.

Para más detalles sobre los pasos de la vulnerabilidad y mitigación de esta, puedes visitar el articulo que lanzó WordPress.