Si utilizas WordPress y no has actualizado tu sitio a la última versión 5.0.3, sería muy buena idea hacerlo ahora, pues investigadores de seguridad cibernética en RIPS Technologies GmbH aseguran que las versiones anteriores cuentan con una grave vulnerabilidad.

Según las investigaciones, la vulnerabilidad crítica de ejecución remota de código afecta a todas las versiones anteriores del software de administración de contenido lanzadas en los últimos seis años.

Este fallo de seguridad fue reportado al equipo de seguridad de WordPress a finales del año pasado. La vulnerabilidad puede ser explotada por un atacante con privilegios bajos con una cuenta mínimamente de autor, con la que aprovecha dos vulnerabilidades separadas, la Travesía de Ruta e Inclusión de Archivos Locales, que residen en el núcleo de WordPress.

El requisito de al menos una cuenta de autor reduce la gravedad de la vulnerabilidad en cierta forma, pues solo puede ser aprovechada por algún colaborador deshonesto o algún atacante que se las arregle para obtener las credenciales del autor.

> *«Un atacante que obtiene acceso a una cuenta con al menos privilegios de autor en un sitio de WordPress de destino puede ejecutar un código PHP arbitrario en el servidor subyacente, lo que lleva a una toma de control remota completa»,* afirma Scannell.

Según Simon Scannell, investigador de RIPS Technologies GmbH, el ataque aprovecha la forma en que el sistema de gestión de imágenes de WordPress maneja las entradas Post Meta que se utilizan para almacenar la descripción, el tamaño, el creador y demás información meta de las imágenes cargadas.

En los siguientes videos puedes ver cómo funciona la vulnerabilidad:

Scannell descubrió que una cuenta de autor malintencionada o comprometida puede modificar cualquier entrada asociada con una imagen y establecerla en valores arbitrarios, lo

que lleva a la vulnerabilidad de la ruta de acceso.

> *«La idea es configurar _wp_attached_file en evil.jpg?Shell.php, lo que llevaría a una solicitud HTTP a la siguiente URL: https://targetserver.com/wp-content/uploads/evil.jpg?shell.php»,* explica Scannell.
>
> Y, *«todavía es posible colocar la imagen resultante en cualquier directorio utilizando una carga útil como evil.jpg? /../../ evil.jpg».*

La falla de trayectoria en combinación con una falla de inclusión de archivo local en el directorio de temas podría permitir al atacante ejecutar código arbitrario en el servidor de destino.

El ataque, como se muestra en el video de prueba de concepto compartido por el investigador, se puede ejecutar en pocos segundos para obtener un control completo sobre un blog de WordPress vulnerable.

Según Scannell, el ataque de ejecución de código se convirtió en no explotable en las versiones de WordPress 5.0.1 y 4.9.9 luego de que se introdujera un parche para otra vulnerabilidad que impedía que usuarios no autorizados establecieran entradas arbitrarias de Post Meta.

Sin embargo, el defecto Path Traversal aún no está parcheado ni siquiera en la última versión de WordPress y puede ser explotado por hackers si algún complemento de terceros instalado maneja incorrectamente las entradas Post Meta.

Scannell confirmó que la próxima versión de WordPress incluirá una solución para abordar completamente el problema demostrado por los investigadores.

Mientras tanto, será mejor que tengas cautela con tus colaboradores, pues nunca se sabe

quién podría aprovechar esto para mal.