Si tienes un sitio web de comercio electrónico creado en WordPress y utilizas el plugin WooCommerce, debes tener mucho cuidado con una vulnerabilidad que no ha sido parcheada, que podría permitir que los hackers pongan en peligro tu tienda online.

Una compañía de seguridad de WordPress, llamada *«Vulnerabilidades de complementos»,* ha estado protestando contra los moderadores del foro de soporte oficial de WordPress, dejando de lado los detalles de la vulnerabilidad de prueba de concepto de una falla crítica en un plugin de WordPress muy utilizado.

Cabe recalcar que la vulnerabilidad informada no reside en el núcleo de WordPress o en el propio complemento de WooCommerce.

La vulnerabilidad existe en el plugin llamado WooCommerce Checkout Manager, que amplía la funcionalidad de WooComeerce al permitir que los sitios de comercio electrónico personalicen los formularios en sus páginas web de pago y que actualmente están siendo utilizados por más de 60,000 sitios web.

Dicha vulnerabilidad se basa en un problema de *«carga arbitraria de archivos»* que puede ser explotado por atacantes remotos no autenticados si los sitios vulnerables tienen la opción *«Categorizar archivos subidos»* habilitada dentro de la configuración del plugin WooCommerce Checkout Manager.

> *«Desde el aspecto más técnico, la vulnerabilidad se produce dentro del archivo 'includes/admin.php' en la línea 2084 en la que la aplicación está moviendo los archivos dados a un directorio utilizando 'move_uploaded_file' sin una verificación previa adecuada de los archivos permitidos»,* escribió la plataforma de seguridad WebARX.

Si se explota, la falla podría permitir a los hackers ejecutar código de script del lado del servidor en el contexto del proceso del servidor web y poner en peligro la aplicación para acceder o modificar datos u obtener acceso administrativo.


Prueba de concepto

La versión 4.2.6 de WooCommerce Checkout Manager, que es el último complemento disponible en el momento de la escritura, es vulnerable a este problema.

Si tu sitio de WordPress utiliza este complemento, se recomienda deshabilitar la opción «Clasificar archivos cargados» en la configuración o deshabilitar el plugin completo hasta que esté disponible una nueva versión parcheada.

Esta no es la primera vez que la compañía llamada Plugin Vulnerabilities revele de forma inapropiada una falla no parcheada en público.

La compañía ha estado continuamente revelando vulnerabilidades en distintos complementos de WordPress desde que tuvieron problemas con los moderadores del foro de WordPress.

Desde hace al menos dos años, el equipo que está detrás de Plugin Vulnerabilities ha estado publicando deliberadamente detalles sobre las vulnerabilidades recién descubiertas directamente en el foto de soporte de WordPress, en lugar de informarlas directamente a los respectivos autores de los plugins, violando así las reglas del foro.

Como respuesta al comportamiento inapropiado, los moderadores de WordPress.org incluyeron en la lista negra a Plugin Vulnerabilities de su foro oficial luego de múltiples advertencias y la prohibición de todas sus cuentas.

Sin embargo, esto no impidió que Plugin Vulnerabilities, que desde entonces comenzaron a revelar detalles sobre las nuevas vulnerabilidades de plugins de WordPress sin parches en su propio sitio web, pusieran en riesgo todo el ecosistema, los sitios web y sus usuarios.