BOLETÍN DE ALERTA

Boletín Nro.: 2023-31
Fecha de publicación: 16/06/2023
Tema: Vulnerabilidad de *insecure direct object reference* (*IDOR*) en *plugin* de WordPress

El producto afectado es:

- *Plugin* WooCommerce Stripe Payment Gateway, versión 7.4.0 y anteriores.

Descripción:

Se ha reportado un nuevo aviso de seguridad sobre una vulnerabilidad que afecta al *plugin* WooCommerce Stripe Payment Gateway de WordPress, que permitiría a un atacante realizar divulgación de información sensible del sistema afectado.

La vulnerabilidad identificada como CVE-2023-34000, de severidad "Alta" y con puntuación asignada de 7.5. Esta vulnerabilidad del tipo *insecure direct object reference* (*IDOR*) se debe a una falla de seguridad en el control de acceso de las funciones *javascript_params* y *payment_fields* del *plugin* WooCommerce Stripe Payment Gateway de WordPress. Esto permitiría a un atacante no autenticado a través de la falta de comprobación de un pedido realizado por el usuario, obtener acceso no autorizado a información personal sensible como nombre, dirección y la dirección de correo electrónico de las órdenes de compras realizadas en el sitio web afectado.

Impacto:

La explotación exitosa de la vulnerabilidad podría permitir a un atacante realizar divulgación de información personal sensible.

Solución:

Recomendamos acceder a las actualizaciones provistas por el fabricante en el siguiente enlace:

- https://wordpress.org/plugins/woocommerce-gateway-stripe/

Información adicional:

- https://patchstack.com/articles/unauthenticated-idor-to-pii-disclosure-vulnerability-in-woocommerce-stripe-gateway-plugin?_s_id=cve
- https://www.securityweek.com/hundreds-of-thousands-of-ecommerce-sites-impacted-by-critical-plugin-vulnerability/
- https://nvd.nist.gov/vuln/detail/CVE-2023-34000
- https://wordpress.org/plugins/woocommerce-gateway-stripe/