BOLETÍN DE ALERTA

Boletín Nro.: 2022-33
Fecha de publicación: 08/08/2022
Tema: Vulnerabilidad de Cross-Site Request Forgery (CSRF) detectada en plugin Ecwid de WordPress

Productos afectados:

- *Ecwid Ecommerce Shopping Cart*, version 6.10.23 y anteriores.

Descripción:

Se ha reportado una vulnerabilidad que afecta al plugin *Ecwid Ecommerce Shopping de Wordpress*, que permitiría a un atacante realizar *Cross-Site Request Forgery* (*CSRF*).

La vulnerabilidad identificada como CVE-2022-2432, de severidad "alta", sin una puntuación asignada aún. Esta vulnerabilidad se debe a una incorrecta validación de datos de entrada a través de la función *ecwid_update_plugin_params*.

Impacto:

La explotación exitosa de esta vulnerabilidad permitiría a un atacante realizar *Cross-Site Request Forgery* (*CSRF*) y modificar el *ecwid_store_id,* que identifica de manera única la tienda.

Solución:

WordPress recomienda actualizar a la última versión 6.10.24 o superior disponible de *Ecwid Ecommerce Shopping Cart,* a través del siguiente enlace:

- https://wordpress.org/plugins/ecwid-shopping-cart/#description

Información adicional:

- https://www.wordfence.com/blog/2022/08/cross-site-request-forgery-vulnerability-patched-in-ecwid-ecommerce-shopping-cart-plugin/
- https://www.redpacketsecurity.com/ecwid-ecommerce-shopping-cart-plugin-for-wordpress-cross-site-request-forgery-cve-2022-2432/
- https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-2432
- https://patchstack.com/database/vulnerability/ecwid-shopping-cart/wordpress-ecwid-ecommerce-shopping-cart-plugin-6-10-23-cross-site-request-forgery-csrf-vulnerability-leading-to-settings-options-update