Se ha revelado una importante vulnerabilidad de seguridad en el plugin *«Abandoned Cart Lite for WooCommerce»* de WordPress, instalado en más de 30,000 sitios web.

> *«Esta falla de seguridad permite que un atacante obtenga acceso a las cuentas de usuarios que han abandonado sus carritos, que suelen ser clientes, pero también puede afectar a otros usuarios de nivel alto cuando se cumplen ciertas condiciones»*, advirtió Wordfence de Defiant en un comunicado.

Identificada como CVE-2023-2986, esta debilidad ha sido calificada con una gravedad de 9.8 sobre 10 en el sistema de puntuación CVSS. Afecta a todas las versiones del plugin, incluyendo las versiones anteriores a la 5.14.2.

La raíz del problema radica en una vulnerabilidad de omisión de autenticación causada por insuficientes medidas de cifrado aplicadas cuando se notifica a los clientes que han abandonado sus carritos de compra en sitios de comercio electrónico sin completar la compra.

En concreto, la clave de cifrado está codificada en el plugin, lo que permite que actores malintencionados inicien sesión como un usuario con un carrito abandonado.

> *«Sin embargo, existe la posibilidad de que, al aprovechar la vulnerabilidad de omisión de autenticación, un atacante pueda obtener acceso a una cuenta de usuario administrador u otra cuenta de alto nivel si han estado probando la funcionalidad del carrito abandonado»,* afirmó el investigador de seguridad István Márton.

Tras una divulgación responsable el 30 de mayo de 2023, el desarrollador del plugin, Tyche Softwares, solucionó la vulnerabilidad el 6 de junio de 2023 con la versión 5.15.0. La versión actual de Abandoned Cart Lite for WooCommerce es la 5.15.2.

Este hallazgo se produce mientras Wordfence reveló otra vulnerabilidad de omisión de autenticación que afecta al plugin *«Booking Calendar | Appointment Booking | BookIt»* de StylemixThemes (CVE-2023-2834, puntuación CVSS: 9.8), el cual cuenta con más de 10,000 instalaciones en WordPress.

> *«Esto se debe a una verificación insuficiente del usuario proporcionado durante la reserva de una cita a través del plugin. Esto permite que atacantes no autenticados inicien sesión como cualquier usuario existente en el sitio, como un administrador, si tienen acceso al correo electrónico»*, explicó Márton.

Esta vulnerabilidad, que afecta a las versiones 2.3.7 y anteriores, se solucionó en la versión 2.3.8, lanzada el 13 de junio de 2023.