Guatemala - El Salvador - Honduras - República Dominicana

Devel
CYBERSECURITY REDEFINED

CYBER SECURITY NEWS

SECURITY OPERATIONS CENTER

DOS NUEVAS VULNERABILIDADES PERMITEN ACCESO ADMINISTRATIVO SIN CREDENCIALES EN WORDPRESS

26/ 08 / 2025

CONTENIDO

INTRODUCCIÓN 3
RESUMEN 5
RECOMENDACIONES 5
NOTICIA COMPLETA 5
CONTACTOS DE SOPORTE 6

INTRODUCCIÓN

Recientemente, se publicaron dos nuevas vulnerabilidades críticas en plugins de WordPress que permiten accesos no autorizados a cuentas administrativas. Ambas vulnerabilidades tienen una puntuación CVSS de 9.8 y han sido identificadas con los ID CVE-2025-7624 y CVE-2025-5821.

DOS NUEVAS VULNERABILIDADES PERMITEN ACCESO ADMINISTRATIVO SIN CREDENCIALES EN WORDPRESS

A continuación, se encuentra en cuadro de identificación de la amenaza.

ID de alerta:	DSOC-CERT_2025_08_26_1
Clasificación de alerta:	Noticia
Tipo de Impacto:	Alta
TLP (Clasificación de información):	**CLEAR**
Fecha de publicación:	26/08/2025
Es día cero (0 day):	No

RESUMEN

Recientemente, se publicaron dos nuevas vulnerabilidades críticas en plugins de WordPress que permiten accesos no autorizados a cuentas administrativas. Ambas vulnerabilidades tienen una puntuación CVSS de 9.8 y han sido identificadas con los ID CVE-2025-7624 y CVE-2025-5821.

CVE-2025-7624

Esta vulnerabilidad afecta al complemento Simpler Checkout para WordPress, utilizado junto con WooCommerce en las versiones 0.7.0 a 1.1.9, inclusive.

El fallo se encuentra en la función simplerwc_woocommerce_order-created(). Permite que un cibercriminal no autenticado inyecte un ID de pedido y sea autenticado como el usuario vinculado, incluso como administrador si el pedido proviene de una cuenta con privilegios elevados.

CVE-2025-5821

Esta vulnerabilidad afecta al complemento Case Theme User para WordPress e incluye todas las versiones hasta la 1.0.3.

El fallo en la función Facebook_ajax_login_callback()permite que un atacante no autenticado se conecte como usuario administrativo, siempre que tenga una cuenta existente y conozca la dirección de correo electrónico del administrador.

RECOMENDACIONES

El impacto para ambas vulnerabilidades es alto, por lo cual se recomienda una actualización inmediata para no incurrir en un incidente.

- Actualiza los plugins a sus versiones seguras y parcheadas lo antes posible.
- Revisa el historial de inicios de sesión, solicitudes sospechosas y cambios en cuentas administrativas.
- Implementa un WAF (Web Application Firewall) para bloquear solicitudes sospechosas con ID.
- Asegura copias de respaldo y revisa tus planos de respuesta ante incidentes.
- Implementa autenticación multifactor (MFA) para cuentas críticas.

NOTICIA COMPLETA

https://devel.group/blog/dos-nuevas-vulnerabilidades-permiten-acceso-administrativo-sin-credenciales-en-wordpress/

CONTACTOS DE SOPORTE

Correo electrónico: cti@develsecurity.com

Teléfonos directos:

Guatemala: +(502) 2307 5757

El Salvador: +(503) 2249 4252

Honduras: +(504) 2283 5904

República Dominicana: +1 829 734 2040

WhatsApp: +(502) 5124 9536

Sitio Web: https://devel.group