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

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

WordPress, el CMS más usado del mundo, vuelve a estar en el punto de mira de los ciberdelincuentes. Recientemente, se han revelado dos vulnerabilidades críticas en plugins populares que permiten acceder a cuentas administrativas sin necesidad de credenciales. Ambas fallas tienen una puntuación de 9.8 en la escala CVSS, lo que las sitúa en el nivel más alto de riesgo.

Las vulnerabilidades han sido catalogadas como CVE-2025-7624 y CVE-2025-5821, y afectan a plugins utilizados en tiendas online y sitios que implementan sistemas de registro de usuarios.

CVE-2025-7624 – Falla en Simpler Checkout

- Plugin afectado: Simpler Checkout para WordPress (junto con WooCommerce).
- Versiones vulnerables: de la 0.7.0 a la 1.1.9, inclusive.
- Descripción técnica: el fallo se encuentra en la función simplerwc_woocommerce_order_created().
    - Un atacante no autenticado puede inyectar un ID de pedido falso y hacerse pasar por el usuario asociado.
    - Si el pedido pertenece a un administrador, el atacante obtiene privilegios completos sobre el sitio.

Impacto potencial

- Control total del sitio web.
- Alteración o robo de datos de clientes (incluyendo información sensible de pedidos).
- Inyección de código malicioso para propagar malware o redirigir tráfico a páginas fraudulentas.

CVE-2025-5821 – Falla en Case Theme User

- Plugin afectado: Case Theme User.
- Versiones vulnerables: todas hasta la 1.0.3 inclusive.
- Descripción técnica: el fallo está en la función facebook_ajax_login_callback().
    - Permite que un atacante no autenticado se conecte como administrador.
    - Solo requiere conocer el correo electrónico del administrador y tener una cuenta registrada en el sitio.

Impacto potencial

- Acceso directo al panel de administración.
- Creación o eliminación de usuarios.
- Instalación de plugins maliciosos.
- Robo o borrado de información crítica.

¿Por qué es grave?

WordPress impulsa más del 40% de los sitios web en Internet, y su seguridad depende en gran medida de los plugins de terceros. Esto convierte a los plugins en uno de los puntos más atacados por los cibercriminales.

Un fallo en un solo plugin puede afectar a miles de páginas en todo el mundo. En este caso, ambos errores permiten el bypass total de autenticación, es decir, acceder como administrador sin necesidad de contraseña ni interacción del usuario.

RECOMENDACIONES

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

- Actualiza inmediatamente los plugins afectados:
  - Simpler Checkout: actualizar a una versión superior a la 1.1.9 en cuanto esté disponible.
  - Case Theme User: actualizar a una versión superior a la 1.0.3.
  - Si no hay parches aún, lo más seguro es desactivar temporalmente los plugins.
- Audita los registros de tu sitio: revisa inicios de sesión sospechosos y cambios en cuentas administrativas.
- Cambia las contraseñas de administradores y usuarios con privilegios elevados.
- Habilita autenticación multifactor (MFA) para todas las cuentas críticas.
- Usa un firewall de aplicaciones web (WAF) para filtrar intentos de explotación automatizados.
- Haz copias de seguridad regulares de tu sitio y base de datos, para poder restaurar en caso de compromiso.

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