Guatemala - El Salvador - Honduras - República Dominicana

Devel
CYBERSECURITY REDEFINED

CYBER SECURITY NEWS

SECURITY OPERATIONS CENTER

VULNERABILIDAD EN WP WEBHOOKS EN WORDPRESS PERMITE COPIA ARBITRARIA DE ARCHIVOS SIN AUTENTICACIÓN

21/ 08 / 2025

CONTENIDO

INTRODUCCIÓN

La vulnerabilidad **CVE-2025-8895** ha sido clasificada como crítica, con una puntuación de **9.8 según CVSS 3.1**. Su vector de ataque permite la explotación a través de la red (AV:N) con baja complejidad (AC:L), sin requerir privilegios previos (PR:N) ni interacción del usuario (UI:N). Su impacto es severo, ya que afecta de forma alta la confidencialidad, integridad y disponibilidad de los sistemas. Esta falla está asociada al tipo **CWE-22: Path Traversal**.

VULNERABILIDAD EN WP WEBHOOKS EN WORDPRESS PERMITE COPIA ARBITRARIA DE ARCHIVOS SIN AUTENTICACIÓN

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

ID de alerta:	DSOC-CERT_2025_08_21_2
Clasificación de alerta:	Noticia
Tipo de Impacto:	Alta
TLP (Clasificación de información):	**CLEAR**
Fecha de publicación:	21/08/2025
Es día cero (0 day):	No

RESUMEN

La vulnerabilidad CVE-2025-8895 ha sido clasificada como crítica, con una puntuación de 9.8 según CVSS 3.1. Su vector de ataque permite la explotación a través de la red (AV:N) con baja complejidad (AC:L), sin requerir privilegios previos (PR:N) ni interacción del usuario (UI:N). Su impacto es severo, ya que afecta de forma alta la confidencialidad, integridad y disponibilidad de los sistemas. Esta falla está asociada al tipo CWE-22: Path Traversal.

¿En qué consiste el fallo?

El problema radica en que una ruta responsable de copiar archivos dentro del plugin no valida de forma adecuada las entradas proporcionadas por el usuario. Esto posibilita que un atacante no autenticado solicite el rastreo hacia directorios superiores (mediante ../ o equivalentes codificados) y copie archivos sensibles del servidor. Por ejemplo, se puede extraer el contenido de wp-config.php, que contiene credenciales de la base de datos, y guardarlo como un archivo de texto accesible por navegador.

¿Por qué es una amenaza tan elevada?

- Sin necesidad de iniciar sesión: Cualquier atacante puede explotar esta falla desde Internet.
- Acceso a información crítica: Permite el acceso a credenciales de bases de datos, llaves privadas, backups expuestos, entre otros.
- Automatización del ataque: Los atacantes suelen escanear miles de sitios en busca de esta vulnerabilidad, lo que la hace altamente peligrosa.

¿Qué medidas deben tomar los administradores de WordPress?

1. Actualización inmediata del plugin

- Actualiza WP Webhooks a la versión 3.3.6 o superior, que corrige esta vulnerabilidad.

2. Si no puedes actualizar aún:

- Desactiva temporalmente el plugin desde el panel de administración de WordPress.
- Bloquea el acceso a los endpoints del plugin mediante reglas en tu servidor web o firewall:
  - Apache (en .htaccess):
  - RewriteEngine On
  - RewriteCond %{REQUEST_URI} ^/wp-content/plugins/wp-webhooks/ [NC]
  - RewriteRule .* – [F,L]
- Nginx:
  - location ~* /wp-content/plugins/wp-webhooks/ { return 403; }

- Aplica un parche virtual vía WAF / ModSecurity bloqueando patrones de “path traversal” (../, %2e%2e%2f, etc.) que apunten a rutas del plugin.

3. Revisión post-explotación

- Inspecciona los logs del servidor (Apache/Nginx/WAF) buscando peticiones con secuencias sospechosas como ../.
- Busca archivos nuevos o modificados fuera de lugar, especialmente archivos .php, archivos de configuración o copias de wp-config.php.

- Si sospechas que hubo acceso, rota las credenciales (base de datos, API, etc.), elimina archivos maliciosos y considera restaurar desde un backup limpio.

4. Fortalecimiento continuo

- Fortalece los permisos del servidor (ej. wp-config.php inaccesible públicamente, permisos mínimos en directorios).
- Implementa monitoreo continuo de logs y alertas para peticiones sospechosas.
- Revisa periódicamente permisos de archivos, presencia de webshells o scripts extraños.

Conclusión

La vulnerabilidad CVE-2025-8895 representa un riesgo urgente para cualquier sitio que ejecute WordPress con el plugin WP Webhooks versión 3.3.5 o inferior. Su naturaleza remota, sin necesidad de autenticación y con potencial de acceso a datos confidenciales, exige acciones inmediatas: actualización, mitigación y revisión exhaustiva.

NOTICIA COMPLETA

https://devel.group/blog/vulnerabilidad-en-wp-webhooks-en-wordpress-permite-copia-arbitraria-de-archivos-sin-autenticacion/

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