Guatemala - El Salvador - Honduras - República Dominicana

Devel
CYBERSECURITY REDEFINED

CYBER SECURITY NEWS

SECURITY OPERATIONS CENTER

CVE-2025-7441: VULNERABILIDAD CRÍTICA EN EL PLUGIN STORYCHIEF DE WORDPRESS PERMITE CARGA ARBITRARIA DE ARCHIVOS

18/ 08 / 2025

CONTENIDO

INTRODUCCIÓN

Recientemente una nueva vulnerabilidad identificada como CVE-2025-7441 con una puntuación CVSS de 9.8 se encontró, investigadores encontraron que afecta el plugin StoryChief de la plataforma WordPress, la vulnerabilidad permite que cibercriminales no autenticados suban archivos maliciosos y potencialmente ejecuten código remoto en sitios vulnerables.

CVE-2025-7441: VULNERABILIDAD CRÍTICA EN EL PLUGIN STORYCHIEF DE WORDPRESS PERMITE CARGA ARBITRARIA DE ARCHIVOS

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

ID de alerta:	DSOC-CERT_2025_08_18_2
Clasificación de alerta:	Noticia
Tipo de Impacto:	Alta
TLP (Clasificación de información):	**CLEAR**
Fecha de publicación:	18/08/2025
Es día cero (0 day):	No

RESUMEN

Recientemente una nueva vulnerabilidad identificada como CVE-2025-7441 con una puntuación CVSS de 9.8 se encontró, investigadores encontraron que afecta el plugin StoryChief de la plataforma WordPress, la vulnerabilidad permite que cibercriminales no autenticados suban archivos maliciosos y potencialmente ejecuten código remoto en sitios vulnerables.

¿Cómo funciona?

El plugin StoryChief es utilizado comúnmente para automatizar la publicación de contenidos en WordPress, este presento una falla en su endpoint REST API /wp-json/storychief/webhook.

El endpoint no tiene una validación adecuada del tipo de archivos que se suben, lo que permite a cibercriminales cargar cualquier tipo de archivo.

La falla se encuentra en el archivo includes/tolos.php.

Versiones afectadas

El plugin en todas las versiones hasta e incluyendo la 1.0.42 estas afectadas.

Hasta lo que se sabe por parte de los investigadores no se ha reportado ningún exploit público o prueba de concepto activa (PoC).

RECOMENDACIONES

- Aplica reglas severas de validación de tipo de archivo (extensiones y MIME), aunque es una solución temporal.
- Busca archivos recientemente subidos en carpetas inusuales y analiza el registro de accesos al endpoint REST.
- Instala plugins de seguridad (p. ej., Wordfence), limita accesos al endpoint con firewalls o reglas IP, y deshabilita cualquier endpoint REST API innecesario o accesible públicamente.
- Asegura copias recientes de tu sitio y datos críticos. Tener un plan de rollback es esencial si ocurre una intrusión exitosa.

NOTICIA COMPLETA

https://devel.group/blog/cve-2025-7441-vulnerabilidad-critica-en-el-plugin-storychief-de-wordpress-permite-carga-arbitraria-de-archivos/

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