BOLETÍN DE ALERTA

Boletín Nro.: 2021-06

Fecha de publicación: 04/03/2021

Tema: Vulnerabilidad en plugin Contact Form 7 para WordPress

Versión afectada:

- Contact Form 7 5.3.1 y versiones anteriores

Descripción

Un equipo de seguridad ha reportado una vulnerabilidad que afecta al plugin **Contact Form 7** en su versión 5.3.1 y las anteriores.. Contact Form 7 es uno de los complementos de WordPress más populares que permite a sus usuarios agregar múltiples formularios de contacto en su sitio.

La vulnerabilidad, identificada como CVE-2020-35489, permite la carga arbitraria de archivos sin restricciones, lo cual un atacante puede aprovechar para cargar archivos de cualquier tipo, evitando todas las restricciones impuestas con respecto a los tipos de archivos permitidos que se pueden cargar. La vulnerabilidad está clasificada como de **gravedad máxima**, con calificación CVSS **10**.

En un sitio web que usa la versión vulnerable de Contact Form 7 y almacena los archivos en el propio servidor, un atacante puede aprovechar esta vulnerabilidad para cargar contenido malicioso como webshells. La vulnerabilidad solo es explotable cuando el formulario tiene habilitada la carga de archivos.

Impacto:

La explotación exitosa de esta vulnerabilidad puede derivar en el control total del servidor que aloja el sitio web afectado y/o en el que se almacenan los archivos de este sitio web.

Solución y m**itigación**

1. Actualice a la última versión, Contact-form-7 versión 7.5.4. Se debe tener en cuenta que el plugin requiere Wordpress 5.5 o superior. En caso de contar con una versión anterior de Wordpress, ésta debe ser actualizada también.
    a. Para actualizar el plugin, acceda a su > panel de administración > Plugin > Plugin instalado > Actualizar.
2. Deshabilitar la opción de subida de archivo en el formulario.

Referencias

- https://contactform7.com/2020/12/17/contact-form-7-532/
- https://www.getastra.com/blog/911/plugin-exploit/contact-form-7-unrestricted-file-upload-vulnerability/