



BOLETÍN DE ALERTA

Boletín Nro.: 2021-21

Fecha de publicación: 13/09/2021

Tema: Actualización crítica de seguridad y mantenimiento de WordPress.

Productos afectados:

- WordPress, versiones entre la 5.4 y la 5.8.

Descripción:

El equipo de desarrollo de WordPress ha anunciado el lanzamiento de la versión 5.8.1 que corresponde a una actualización de seguridad y mantenimiento, la cual soluciona 3 problemas de seguridad críticos y además 60 correcciones de fallos y errores.

Los problemas de seguridad que han sido reportados y que soluciona esta nueva actualización, afectan a las versiones comprendidas entre la 5.4 y la 5.8, por lo que se han publicado actualizaciones desde la versión 5.4. Los problemas de seguridad que solventa esta nueva actualización son:

- Vulnerabilidad por exposición de datos en el REST API de WordPress.
- Vulnerabilidad de tipo Cross-site Scripting en el editor de bloques.
- Actualización de la librería 'Lodash' para incorporar diversas actualizaciones de seguridad de la misma.

Impacto:

La explotación exitosa de las vulnerabilidades puede resultar en un compromiso completo del sitio vulnerable.



Solución:

El proceso de actualización de WordPress a la versión 5.8.1, se puede realizar de las siguientes formas:

- Descargar la actualización desde la página [oficial de WordPress](#).
- Desde el propio gestor de contenido, en el aviso que aparecerá en el panel principal o accediendo al área de administración del sitio, en el menú **Escritorio**, **Actualizaciones** y haciendo clic en **Actualizar ahora**.

Observación: en los sitios web compatibles con actualizaciones automáticas en segundo plano, el proceso de actualización se realizará de forma automática.

Al tratarse de una actualización de seguridad recomendamos encarecidamente aplicar dicha actualización.

Información adicional:

- <https://es.wordpress.org/2021/09/09/wordpress-5-8-1-actualizacion-de-seguridad-y-mantenimiento/>
- <https://us-cert.cisa.gov/ncas/current-activity/2021/09/10/wordpress-releases-security-update>