BOLETÍN DE ALERTA

Boletín Nro.: 2021-11

Fecha de publicación: 17/05/2021

Tema: Vulnerabilidad crítica en WordPress.

Fecha de actualización: 17/05/2021

Sistemas afectados:

- WordPress entre las versiones 3.7 y 5.7.

Descripción:

WordPress corrigió una vulnerabilidad crítica de falla de inyección de objetos presente en múltiples versiones de PHPMailer, a la que se le ha dado un identificador de CVE-2020-36326.

La falla se introdujo luego de una corrección incorrecta a una vulnerabilidad previa (CVE-2018-19296), que buscaba corregir un problema de funcionalidad en el que PHPMailer.

A continuación se expone la lista de vulnerabilidades de gravedad crítica y alta:

- **CVE-2020-36326** de severidad crítica con una puntuación de 9.8. PHPMailer 6.1.8 a 6.4.0 permite la inyección de objetos a través de la deserialización de Phar mediante **addAttachment** con un nombre de ruta UNC. Es importante recalcar que esto es similar a la vulnerabilidad CVE-2018-19296, pero surgió debido a una 6.1.8 solución incorrecta al bug de PHPMailer (siempre consideraba ilegibles los nombres de ruta UNC, incluso en contextos seguros) . Como efecto secundario no intencionado, esta corrección eliminó el código que bloqueaba la explotación de “addAttachment”.
- **CVE-2018-19296** de severidad alta con una puntuación de 8.8. PHPMailer antes de 5.2.27 y 6.x antes de 6.0.6 es vulnerable a un ataque de inyección de objetos.

Impacto:

La explotación exitosa de la vulnerabilidad podría permitir a un atacante remoto no autenticado realizar diferentes tipos de ataques, como inyección de código, inyección de SQL, recorrido de ruta y denegación de servicio de la aplicación, según el contexto.

Solución:

- Actualice automáticamente desde el menú **Panel de control > Actualizaciones** en el área de administración de su sitio o visite

  https://wordpress.org/download/release-archive/.

- Para obtener instrucciones paso a paso sobre la instalación y actualización de WordPress: Actualización de WordPress.

Información adicional:

- https://nvd.nist.gov/vuln/detail/CVE-2020-35938
- https://nvd.nist.gov/vuln/detail/CVE-2018-6195
- https://wordpress.org/support/wordpress-version/version-5-7-2/
- https://www.searchenginejournal.com/critical-wordpress-vulnerability/406932/#close
- https://www.hebergementwebs.com/sej/wordpress-5-7-2-fixes-critical-vulnerability
- https://patchstack.com/database/vulnerability/wordpress/wordpress-5-7-object-injection-in-phpmailer-vulnerability-cve-2020-36326