

## **BOLETÍN DE ALERTA**

**Boletín Nro.:** 2023-55

**Fecha de publicación:** 12/12/2023

**Tema:** Vulnerabilidad crítica en el plugin Backup Migration de WordPress.

### **Productos afectados:**

- versiones del plugin Backup Migration hasta la versión 1.3.6 están afectadas por esta vulnerabilidad.

### **Descripción:**

Se ha descubierto una vulnerabilidad crítica en el plugin Backup Migration de WordPress, el cual cuenta con más de 90,000 instalaciones. Esta vulnerabilidad permite a los atacantes ejecutar código de forma remota y comprometer por completo los sitios web vulnerables. La vulnerabilidad fue identificada como CVE-2023-6553, con una puntuación asignada de 9.8 CVSS.

### **Impacto:**

La vulnerabilidad permitiría a un actor malicioso no autenticado tomar el control total de los sitios web objetivo mediante la ejecución remota de código a través de la inyección de código PHP en el archivo /includes/backup-heart.php. Esto significa que los actores maliciosos pueden ejecutar código arbitrario en el servidor en el contexto de seguridad de la instancia de WordPress.

### **Solución:**

El equipo de desarrollo del plugin Backup Migration ha lanzado un parche para abordar esta vulnerabilidad. El fabricante recomienda a los administradores de WordPress que actualicen a la versión parcheada 1.3.8 del plugin para proteger sus sitios web contra posibles ataques.

### **Información adicional:**

- <https://www.bleepingcomputer.com/news/security/50k-wordpress-sites-exposed-to-rce-attacks-by-critical-bug-in-backup-plugin/>