Una vulnerabilidad de día cero en un plugin de WordPress llamado BackupBuddy está siendo explotada activamente, según reveló la compañía de seguridad de WordPress, Wordfence.

> *«Esta vulnerabilidad hace posible que usuarios no autenticados descarguen archivos arbitrarios del sitio afectado que pueden incluir información confidencial»,* dijo.

BackupBuddy permite a los usuarios hacer una copia de seguridad de toda su instalación de WordPress desde el tablero, incluyendo los archivos de temas, páginas, publicaciones, widgets, usuarios y archivos multimedia, entre otros.

Se estima que el complemento tiene alrededor de 140,000 instalaciones activas, con la vulnerabilidad (CVE-2022-31474, puntaje CVSS: 7.5) que afecta a las versiones 8.5.8.0 a 8.7.4.1. Se abordó en la versión 8.7.5 lanzada el 2 de septiembre de 2022.

El problema tiene su raíz en la función llamada *«Copia de directorio local»* que está diseñada para almacenar una copia local de las copias de seguridad. Según Wordfence, la vulnerabilidad es el resultado de la implementación insegura, que permite que un atacante no autenticado descargue cualquier archivo arbitrario en el servidor.

Se ocultaron detalles adicionales sobre la falla a la luz del abuso colectivo en estado salvaje y su facilidad de explotación.

> *«Esta vulnerabilidad podría permitir que un atacante vea el contenido de cualquier archivo en su servidor que pueda ser leído por su instalación de WordPress. Esto podría incluir el archivo wp-config.php de WordPress, y según la configuración de su servidor, archivos confidenciales como /etc/passwd»,* dijo el desarrollador del

> plugin, iThemes.

Wordfence dijo que la selección de CVE-2022-31474 comenzó el 26 de agosto de 2022 y que ha bloqueado casi cinco millones de ataques en el período intermedio. La mayoría de las intrusiones intentaron leer los siguientes archivos:

- /etc/passwd
- /wp.config.php
- .mi.cnf
- .accesshash

Se recomienda a los usuarios del plugin BackupBuddy que actualicen a la última versión. Si los usuarios determinan que pudieron haber sido comprometidos, se recomienda restablecer la contraseña de la base de datos, cambiar las «salts» de WordPress y rotar las claves API almacenadas en wp-config.php.