Los actores maliciosos están actualmente tratando de aprovechar una grave vulnerabilidad de seguridad encontrada en el complemento ValvePress Automatic para WordPress, la cual podría permitir la toma de control de sitios web.

Esta debilidad, identificada como CVE-2024-27956, tiene una puntuación CVSS de 9.9 sobre un máximo de 10. Afecta a todas las versiones del complemento anteriores a la 3.92.0. La cuestión ha sido resuelta en la versión 3.92.1 lanzada el 27 de febrero de 2024, aunque la información de lanzamiento no hace referencia a ello.

> *«Esta vulnerabilidad, una falla de inyección SQL (SQLi), plantea una amenaza significativa, ya que los atacantes podrían explotarla para obtener acceso no autorizado a sitios web, crear cuentas de usuario con privilegios de administrador, cargar archivos maliciosos y, potencialmente, tomar control total de los sitios afectados»*, informó WPScan en una alerta esta semana.

Según la empresa propiedad de Automattic, el problema radica en el mecanismo de autenticación de usuario del complemento, que puede ser fácilmente eludido para ejecutar consultas SQL arbitrarias contra la base de datos mediante solicitudes especialmente diseñadas.

En los ataques observados hasta ahora, CVE-2024-27956 se está utilizando para realizar consultas no autorizadas a la base de datos y crear nuevas cuentas de administrador en sitios de WordPress susceptibles (por ejemplo, nombres que comienzan con «xtw»), las cuales podrían ser luego aprovechadas para acciones de explotación posteriores.

Esto incluye la instalación de complementos que permiten cargar archivos o editar código, lo que sugiere intentos de reutilizar los sitios infectados como plataformas de lanzamiento para actividades adicionales.

> *«Una vez que un sitio de WordPress ha sido comprometido, los atacantes aseguran*

> *prolongar su acceso mediante la creación de puertas traseras y la ofuscación del código. Para evadir la detección y mantener el acceso, los atacantes también pueden cambiar el nombre del archivo vulnerable WP-Automatic, lo que dificulta que los propietarios del sitio web o las herramientas de seguridad detecten o bloqueen la cuestión»,* mencionó WPScan.

El archivo en cuestión es *«/wp-content/plugins/wp-automatic/inc/csv.php»*, el cual es renombrado a algo como *«/wp-content/plugins/wp-automatic/inc/csv65f82ab408b3.php».*

Dicho esto, es posible que los actores maliciosos estén llevando a cabo esta acción con el fin de evitar que otros atacantes aprovechen los sitios que ya están bajo su control.

CVE-2024-27956 fue divulgado públicamente por la empresa de seguridad de WordPress Patchstack el 13 de marzo de 2024. Desde entonces, se han detectado más de 5.5 millones de intentos de ataque para aprovechar la vulnerabilidad en la naturaleza.

La divulgación se produce cuando se han revelado graves errores en complementos como Email Subscribers de Icegram Express (CVE-2024-2876, puntuación CVSS: 9.8), Forminator (CVE-2024-28890, puntuación CVSS: 9.8) y User Registration (CVE-2024-2417, puntuación CVSS: 8.8) que podrían ser utilizados para extraer datos sensibles como los hash de contraseñas de la base de datos, cargar archivos arbitrarios y otorgar a un usuario autenticado privilegios de administrador.

Patchstack también ha advertido sobre un problema no resuelto en el complemento Poll Maker (CVE-2024-32514, puntuación CVSS: 9.9) que permite a los atacantes autenticados, con acceso de nivel suscriptor y superior, cargar archivos arbitrarios en el servidor del sitio afectado, lo que lleva a la ejecución remota de código.

(El artículo fue actualizado después de su publicación para corregir las versiones del complemento afectadas por CVE-2024-27956).