Hasta 200.000 sitios web de WordPress corren el riesgo de sufrir ataques continuos que aprovechan una vulnerabilidad crítica sin parchear en el complemento Ultimate Member.

El fallo, registrado como CVE-2023-3460 (puntuación CVSS: 9,8), afecta a todas las versiones del complemento Ultimate Member, incluida la versión más reciente (2.6.6) que se lanzó el 29 de junio de 2023.

Ultimate Member es un complemento popular que facilita la creación de perfiles de usuario y comunidades en sitios de WordPress. También proporciona características de gestión de cuentas.

> *«Este es un problema muy grave: los atacantes no autenticados pueden explotar esta vulnerabilidad para crear nuevas cuentas de usuario con privilegios administrativos, lo que les da el poder de tomar el control total de los sitios afectados»,* dijo la empresa de seguridad de WordPress WPScan en una alerta.

Aunque no se han revelado detalles sobre el fallo debido a su explotación activa, se origina en una lógica de lista negra insuficiente utilizada para modificar el valor de metadatos de usuario *«wp_capabilities»* de un nuevo usuario y obtener acceso completo al sitio.

> *«Aunque el complemento tiene una lista predefinida de claves prohibidas que un usuario no debería poder actualizar, existen formas sencillas de eludir los filtros implementados, como aprovechar diferentes casos, barras y codificación de caracteres en el valor de la clave de metadatos suministrada en versiones vulnerables del complemento»,* dijo Chloe Chamberland, investigadora de Wordfence.

El problema salió a la luz después de que se informara de la aparición de cuentas de administrador fraudulentas en los sitios afectados, lo que llevó a los desarrolladores del

complemento a lanzar correcciones parciales en las versiones 2.6.4, 2.6.5 y 2.6.6. Se espera que se lance una nueva actualización en los próximos días.

> *«Una vulnerabilidad de escalada de privilegios utilizada a través de UM Forms. Se sabe que esta vulnerabilidad, que ha sido detectada en la naturaleza, permite que desconocidos creen usuarios de WordPress con nivel de administrador»,* dijo Ultimate Member en sus notas de lanzamiento.

Sin embargo, WPScan señaló que las soluciones parciales son insuficientes y descubrió numerosos métodos para evadirlos, lo que significa que el problema aún puede ser aprovechado activamente.

En los ataques observados, se aprovecha la vulnerabilidad para registrar nuevas cuentas con los nombres apadmins, se_brutal, segs_brutal, wpadmins, wpengine_backup y wpenginer, con el fin de cargar complementos y temas maliciosos a través del panel de administración del sitio.

Se recomienda a los usuarios de Ultimate Member desactivar el complemento hasta que se disponga de un parche adecuado que cierre por completo la brecha de seguridad. También se sugiere realizar una auditoría de todos los usuarios de nivel administrador en los sitios web para determinar si se han agregado cuentas no autorizadas.