Se ha revelado una vulnerabilidad de seguridad en el popular plugin de WordPress, Essential Addons for Elementor, que podría explotarse potencialmente para lograr privilegios elevados en los sitios afectados.

La vulnerabilidad, rastreada como CVE-2023-32243, ha sido abordada por los mantenedores del complemento en la versión 5.7.2 que se envió el 11 de mayo de 2023. Essential Addons for Elementor tiene más de un millón de instalaciones activas.

> *«Este plugin sufre una vulnerabilidad de escalada de privilegios no autenticados y permite que cualquier usuario no autenticado aumente sus privilegios a los de cualquier usuario en el sitio de WordPress»,* dijo Rafie Muhammad, investigador de Patchstack.

La explotación exitosa de la vulnerabilidad podría permitir que un atacante restablezca la contraseña de cualquier usuario arbitrario, siempre que la parte malintencionada conozca su nombre de usuario. Se cree que la deficiencia existe desde la versión 5.4.0

Esto puede tener serias ramificaciones, ya que la vulnerabilidad podría convertirse en un arma para restablecer la contraseña asociada con una cuenta de administrador y tomar el control total del sitio web.

> *«Esta vulnerabilidad ocurre porque esta función de restablecimiento de contraseña no valida una clave de restablecimiento de contraseña y, en cambio, cambia de forma directa la contraseña del usuario dado»*, dijo Muhammad.

La divulgación se produce más de un año después de que Patchstack revelara otra vulnerabilidad grave en el mismo complemento que podría haber sido objeto de abuso para ejecutar código arbitrario en sitios web comprometidos.

Los hallazgos también siguen al descubrimiento de una nueva ola de ataques dirigidos a sitios de WordPress desde finales de marzo de 2023 que tiene como objetivo inyectar el malware SocGholish (también conocido como FakeUpdates).

SocGholish es un marco de malware de JavaScript persistente que funciona como un proveedor de acceso inicial para facilitar la entrega de malware adicional a los hosts infectados. El malware se ha distribuido a través de descargas ocultas que se hacen pasar por una actualización del navegador web.

Se descubrió que la última campaña detectada por Sucuri aprovecha las tácticas de compresión usando una biblioteca de software llamada zlib para ocultar el malware, reducir su huella y evitar la detección.

> *«Los malos actores están continuamente desarrollando sus tácticas, técnicas y procedimientos para evadir la detección y prolongar la vida de sus campañas de malware»*, dijo el investigador de Sucuri, Denis Sinegubko.

> *«El malware SocGholish es un excelente ejemplo de esto, ya que los atacantes han alterado su enfoque en el pasado para inyectar scripts maliciosos en sitios web de WordPress comprometidos».*

No es solo SocGholish, Malwarebytes, en un informe técnico de esta semana, detalló una campaña de publicidad maliciosa que sirve a los visitantes de sitios web para adultos con anuncios emergentes que simulan una actualización falsa de Windows para eliminar el cargador *«in2al5d p3in4er»* (también conocido como Invalid Printer).

> *«El esquema está muy bien diseñado ya que se basa en el navegador web para mostrar una animación de pantalla completa que se parece mucho a lo que esperarías de Microsoft»,* dijo Jérôme Segura, director de inteligencia de amenazas de Malwarebytes.

El cargador, que fue documentado por Morphisec el mes pasado, está diseñado para verificar la tarjeta gráfica del sistema para determinar si se está ejecutando en una máquina virtual o en un entorno de espacio aislado y, en última instancia, lanzar el malware de robo de información Aurora.

La campaña, según Malwarebytes, se ha cobrado 585 víctimas en los últimos dos meses, y el actor de amenazas también está vinculado a otras estafas de soporte técnico y un panel de comando y control del bot Amadey.

Complementos esenciales para la vulnerabilidad del complemento de Elementor

Wordfence, en su propio aviso, dijo que la vulnerabilidad crítica en el plugin Essential Addons for Elementor se está explotando activamente en la naturaleza, y que bloqueó 200 ataques dirigidos a la falla en las últimas 24 horas, por lo que es imperativo que los usuarios se muevan rápidamente para actualizar a la última versión.