Hackers desconocidos están explotando activamente una vulnerabilidad de seguridad parcheada recientemente en el complemento del creador de sitios web Elementor Pro para WordPress.

La vulnerabilidad, descrita como un caso de control de acceso roto, afecta a las versiones 3.11.6 y anteriores. Fue abordador por los mantenedores del complemento en la versión 3.11.7 lanzada el 22 de marzo.

«Se mejoró la aplicación de la seguridad del código en los componentes de WooCommerce», dijo la compañía con sede en Tel Aviv en sus notas de lanzamiento. Se estima que el plugin premium se utiliza en más de 12 millones de sitios web.

La explotación exitosa de la vulnerabilidad de alta gravedad permite que un hacker autenticado complete una toma de control de un sitio de WordPress que tiene habilitado WooCommerce.

> *«Esto hace posible que un usuario malicioso active la página de registro (si está habilitada) y establezca el rol de usuario predeterminado en administrador para que pueda crear una cuenta que tenga privilegios de administrador al instante»,* dijo Patchstack en una alerta del 30 de marzo de 2023.

> *«Después de esto, es probable que redirijan el sitio a otro dominio malicioso o carguen un complemento malicioso o una puerta trasera para explotar más el sitio».*

El investigador de seguridad de NinTechNet, Jerome Bruandet, obtuvo el crédito por descubrir e informar sobre la vulnerabilidad el 18 de marzo de 2023.

Patchstack dijo además de que la vulnerabilidad está siendo abusada actualmente desde

distintas direcciones IP con la intención de cargar archivos PHP y ZIP arbitrarios.

Se recomienda a los usuarios del plugin Elementor Pro que actualicen a 3.11.7 o 3.12.0, que es la última versión, lo antes posible para mitigar posibles amenazas.

El aviso llega más de un año después de que se descubriera que el complemento Essential Addons for Elementor contenía una vulnerabilidad crítica que podría resultar en la ejecución de código arbitrario en sitios web comprometidos.

La semana pasada, WordPress emitió actualizaciones automáticas para corregir otro error crítico en el plugin de pagos WooCommerce, que permitía a los hackers no autenticados obtener acceso de administrador a sitios vulnerables.