BOLETÍN DE ALERTA

Boletín Nro.: 2023-21
Fecha de publicación: 17/05/2023
Tema: Múltiples vulnerabilidades en *plugins* de WordPress

El software afectado es:

- *Plugin* Essential Addons for Elementor, versiones 5.4.0 al 5.7.1.
- *Plugin* RegistrationMagic, versión 5.2.1.0 y anteriores.
- *Plugin* Advanced Custom Fields de WordPress, versiones anteriores a 6.1.6.

Descripción:

Se han reportado nuevos avisos de seguridad sobre múltiples vulnerabilidades explotadas activamente que afectan a varios *plugins* del CMS WordPress, que permitirían a un atacante realizar ataques del tipo *cross-site scripting* (*XSS*), escalamiento de privilegios, entre otros. Actualmente para el CVE-2023-30777 existe prueba de concepto (*PoC*) públicada.

- CVE-2023-32243, de severidad "Crítica", con una puntuación asignada de 9.8. Esta vulnerabilidad explotada activamente se debe a una falla de validación de una clave de restablecimiento de contraseña en la función *reset_password* del *plugin* **Essential Addons for Elementor de WordPress.** Esto permitiría a un atacante no autenticado realizar escalamiento de privilegios conociendo el correo electrónico o el nombre de usuario de una cuenta, restablecer la contraseña de la cuenta correspondiente al sitio web afectado.
- CVE-2023-2499, de severidad "Crítica", con una puntuación asignada de 9.8. Esta vulnerabilidad de omisión de autenticación se debe a una falla en la verificación del inicio sesión social de Google (SSO) a través del *plugin* **RegistrationMagic** de WordPress. Esto permitiría a un atacante no autenticado a través del correo electrónico de una cuenta, iniciar sesión con cualquier usuario incluidos los administradores, realizar cambios no autorizados, robar información confidencial y potencialmente tomar el control del sitio web afectado.
- CVE-2023-30777, de severidad "Alta", con una puntuación asignada de 7.1. Esta vulnerabilidad del tipo *cross-site scripting* (*XSS*) explotada activamente se debe a una falla de validación de datos de entradas del usuario en el *plugin* **Advanced Custom Fields** de WordPress. Esto permitiría a un atacante a través de solicitudes *HTTP* especialmente diseñadas enviadas al sitio web, ejecutar código JavaScript en el navegador de las víctimas a través del sitio web afectado.

Impacto:

La explotación exitosa de estas vulnerabilidades podría permitir a un atacante ejecutar código JavaScript en el navegador de las víctimas y obtener privilegios elevados, realizar escalamiento de privilegios, robar información confidencial y potencialmente tomar el control del sitio web afectado.

Solución:

Recomendamos instalar las actualizaciones correspondientes a cada plugin provistas por WordPress en los siguientes enlaces:

- **CVE-2023-32243: Plugin Essential Addons for Elementor 5.7.2**
- **CVE-2023-2499: Plugin RegistrationMagic 5.2.1.1**
- **CVE-2023-30777**: **Plugin Advanced Custom Fields de WordPress 6.1.6**

Información adicional:

- https://www.bleepingcomputer.com/news/security/hackers-target-wordpress-plugin-flaw-after-poc-exploit-released/
- https://www.bleepingcomputer.com/news/security/wordpress-elementor-plugin-bug-let-attackers-hijack-accounts-on-1m-sites/
- https://securityonline.info/authentication-bypass-flaw-cve-2023-2499-in-wordpress-plugin-with-over-10000-installations/
- https://www.cert.gov.py/noticias/vulnerabilidad-de-escalamiento-de-privilegios-en-plugin-de-wordpress-3/
- https://www.cert.gov.py/noticias/vulnerabilidad-de-cross-site-scripting-xss-en-plugin-de-wordpress-6/
- https://nvd.nist.gov/vuln/detail/CVE-2023-32243
- https://nvd.nist.gov/vuln/detail/CVE-2023-30777
- https://nvd.nist.gov/vuln/detail/CVE-2023-2499
- https://wordpress.org/plugins/advanced-custom-fields/#developers
- https://wordpress.org/plugins/essential-addons-for-elementor-lite/
- https://wordpress.org/plugins/custom-registration-form-builder-with-submission-manager/