# BOLETÍN DE ALERTA

**Boletín Nro.**: 2020-13
**Fecha de publicación**: 13/05/2020
**Tema**: Vulnerabilidades de CSRF en el plugin Page Builder de Wordpress.

**Sistemas afectados**:

- Page Builder en sus versiones 2.10.15 y anteriores.

**Descripción**:

Recientemente fueron abordadas en una actualización de seguridad **dos vulnerabilidades críticas** en el plugin **Page Builder** de **Wordpress**. La **primera** se trata de un fallo en la característica **Live Editor** utilizada para realizar cambios y actualizaciones en el contenido publicado, dichos cambios son enviados a través de un parámetro **POST** y seguidamente se realiza una validación en las funciones de metadatos para asegurar que los usuarios tengan permiso de edición, sin embargo durante este proceso de validación no existen protecciones **nonce** (cadena única generada por el servidor), con esto algunos widgets con "**Custom HTML**" incluido podrían ser utilizados para la inyección de **JavaScript malicioso** dentro de la "**live page**", si una vista previa de la "**live page**" diseñada con el widget comprometido es accedida por el administrador del sitio, esto llevaría a una vulnerabilidad del tipo **CSRF(Cross Site Request Forgery)** y también a un **XSS (Cross-Site Scripting) reflexivo.**

Por otro lado, el segundo fallo fue detectado en la función **action_builder_content**, esta es utilizada para transmitir el contenido desde el **Live Editor**, al editor estándar de **Wordpress** con el fin de realizar alguna actualización o publicación sin antes verificar que el usuario cuenta con los permisos requeridos, sin embargo durante este proceso no existe **validación** alguna de la fuente de la solicitud, llevando a una vulnerabilidad del tipo **CSRF(Cross-Site Request Forgery).**

Un atacante remoto podría explotar estas vulnerabilidades engañando al administrador del sitio, con el fin de que el mismo ingrese a un enlace o archivo malicioso y seguidamente ejecutar código malicioso.

**Impacto:**

Estas vulnerabilidades podrían permitir a un atacante ejecutar código malicioso en el navegador del administrador del sitio, crear un nuevo usuario administrador e inclusive inyectar una puerta trasera en el sitio web víctima.

**Solución y prevención:**

- Estas vulnerabilidades fueron abordadas en la versión **2.10.16** de **Page Builder,** se recomienda aplicar las actualizacion lo mas pronto posible desde la página oficial de Wordpress**.**
- Instalar un **WAF (Web Application Firewall)** que filtre las peticiones **HTTP** que contengan código malicioso.

**Información adicional:**

- https://www.wordfence.com/blog/2020/05/vulnerabilities-patched-in-page-builder-by-siteorigin-affects-over-1-million-sites/
- https://www.bleepingcomputer.com/news/security/wordpress-plugin-bugs-can-let-hackers-take-over-almost-1m-sites/
- https://www.zdnet.com/article/wordpress-plugin-page-builder-by-siteorigin-patched-against-code-execution-attacks/