BOLETÍN DE ALERTA

Boletín Nro.: 2022-27
Fecha de publicación: 22/06/2022
Tema: Vulnerabilidad en el plugin *Elementor Website Builder* de *Wordpress*

La vulnerabilidad está presente en versiones anteriores a:

- *Elementor Website Builder 3.5.6.*

Descripción:

Se ha reportado un nuevo aviso de seguridad sobre una vulnerabilidad del tipo *DOM-based Reflected Cross-Site Scripting (XSS)* que afecta al plugin *Elementor Website Builder* de *WordPress*, que permitiría a un atacante realizar ejecución de código *JavaScript* en el sistema afectado.

La vulnerabilidad identificada como CVE-2022-29455 de severidad crítica. Esta se debe a una falla en la comprobación de código del parámetro "*type=video*" específicamente dentro del parámetro "videoParams" en el complemento *Elementor Website Builder* de *Wordpress.*

Actualmente para esta vulnerabilidad, existen PoC publicados en internet.

Impacto:

La explotación exitosa de la misma permitiría a un atacante realizar las siguientes acciones:

- Ejecución de código *JavaScript.*
- Captura de cookies.
- SOAP Bypass.
- CORS Bypass.
- Defacement.

Detección:

Verificar si se posee instalada la versión vulnerable del plugin *Elementor Website Builder:*

1. Escanear el sitio web con el siguiente script:

```
Wget https://raw.githubusercontent.com/projectdiscovery/nuclei-templates/3581482df1bfe1aef4e7fff96e183f9ef0e5bf13/cves/2022/CVE-2022-29455.yaml
```

```
nuclei -t ./CVE-2022-29455.yaml -u https://...
```

2. Verificar el sitio web a través de la herramienta *Elementor XSS Tester*.

Mitigación:

WordPress recomienda actualizar a la última versión 3.5.6 disponible de *Elementor Website Builder*, siguiendo los pasos del siguiente enlace:

- https://elementor.com/help/how-to-update-elementor-and-elementor-pro/

Información adicional:

- https://rotem-bar.com/hacking-65-million-websites-greater-cve-2022-29455-elementor
- https://nvd.nist.gov/vuln/detail/CVE-2022-29455
- https://www.rotem-bar.com/elementor
- https://elementor.com/help/how-to-update-elementor-and-elementor-pro/