Una vulnerabilidad de *cross-site scripting* (XSS) en un sistema de recorridos virtuales ha sido aprovechada por ciberdelincuentes para inyectar código malicioso en cientos de páginas web. Su objetivo es alterar los resultados de búsqueda y potenciar una campaña masiva de anuncios fraudulentos.

El investigador de ciberseguridad Oleg Zaytsev, en un informe, indicó que el ataque, denominado *360XSS*, ha comprometido más de 350 sitios, entre ellos portales gubernamentales, páginas de gobiernos estatales en EE. UU., universidades reconocidas, cadenas hoteleras, medios de comunicación, concesionarias de automóviles y varias empresas de la lista Fortune 500.

> *«Esto no fue solo una táctica de spam. Fue un abuso a gran escala de dominios de confianza»*, explicó el investigador.

Todos los sitios web afectados comparten un elemento en común: utilizan un popular framework llamado *Krpano*, diseñado para integrar imágenes y videos en 360°, lo que permite la creación de recorridos virtuales interactivos y experiencias de realidad virtual.

Zaytsev descubrió la campaña cuando encontró un anuncio con contenido para adultos en *Google Search*, pero alojado en un dominio vinculado a la Universidad de Yale («virtualtour.quantuminstitute.yale[.]edu»).

Un aspecto distintivo de estas URL es la inclusión de un parámetro XML que redirige al visitante a una segunda dirección web legítima. Desde ahí, se ejecuta un código en Base64 que, una vez descifrado, carga la URL del anuncio desde otra fuente confiable.

El parámetro XML en la URL original, que aparece en los resultados de búsqueda, forma parte de una configuración más amplia llamada *passQueryParameters*, que se utiliza para incrustar el visor de panoramas de Krpano en páginas HTML. Su función principal es permitir el paso de parámetros HTTP desde la URL hacia el visor.

El problema de seguridad radica en que, si esta opción está activada, un atacante podría generar una URL personalizada capaz de ejecutar código malicioso en el navegador de la víctima al visitar el sitio afectado.

De hecho, una vulnerabilidad de XSS reflejado derivada de este comportamiento se identificó en Krpano a finales de 2020 (CVE-2020-24901, con una calificación CVSS de 6.1), lo que significa que esta falla ha sido de conocimiento público durante más de cuatro años.

Aunque la versión 1.20.10 de Krpano introdujo restricciones en *passQueryParameters* para limitar su uso a una lista de elementos permitidos y así mitigar ataques XSS, Zaytsev descubrió que añadir manualmente el parámetro XML a esta lista reactivaba el riesgo de vulnerabilidad.


Website with Vulnerable Krpano Instance
XSS
Bank of Assets
stolen subdomains
open redirects
cheap domains
Reflect XSS Ad Generation
https://www.example.com/virtual_tour?xml=https://<hosted_payload>&id=<campaign_id>
Index the Reflected XSS URL
Welcome to Google Search Console
Free Ad is Ready!
utah.gov
Lose Your Thigh Fat🔥 youtubeshorts exercise trending ...
Experienced midwives discuss how Lose Your Thigh Fat youtubeshorts exercise trending fitness weightloss fatloss shortvideo [kom20rZXgn-] intersects with modern ...

> *«A partir de la versión 1.20.10, la instalación estándar de Krpano ya no era vulnerable. No obstante, al configurar passQueryParameters junto con el parámetro XML, se permitía cargar configuraciones XML externas a través de la URL, lo que reintroducía la amenaza de XSS»,* señaló el investigador.
>
> *«Las versiones comprometidas que he encontrado corresponden, en su mayoría, a ediciones anteriores a la 1.20.10».*

Según Zaytsev, los atacantes han explotado esta vulnerabilidad para intervenir en más de 350 sitios y utilizarlos como plataforma para mostrar anuncios engañosos de contenido para adultos, suplementos alimenticios, apuestas en línea y noticias falsas. Además, algunas de estas páginas han sido usadas para inflar artificialmente las visualizaciones de videos en YouTube.

Esta campaña resulta particularmente preocupante porque explota la reputación de sitios web legítimos para posicionarse en los primeros lugares de los motores de búsqueda, una estrategia conocida como *SEO poisoning* o envenenamiento de los resultados de búsqueda. Esto se consigue al explotar la vulnerabilidad de XSS para manipular las páginas comprometidas.

> *«Un XSS reflejado es una vulnerabilidad interesante, pero por sí solo requiere que el usuario interactúe con el enlace malicioso. El mayor desafío es hacer que la gente haga clic en ese enlace. Utilizar los motores de búsqueda como canal de distribución para un ataque XSS es una estrategia ingeniosa y efectiva»,* explicó Zaytsev.

Tras un proceso de divulgación responsable, la versión más reciente de Krpano ha eliminado la posibilidad de configurar parámetros externos mediante XML, lo que reduce significativamente el riesgo de XSS incluso si esta opción está activada.

> *«Se ha fortalecido la seguridad de embedpano() passQueryParameters: ya no se permiten URLs externas ni de datos como valores de parámetros, y las URLs dentro del parámetro XML ahora están restringidas a la estructura de carpetas interna»,* según las notas de la versión 1.22.4 lanzada esta semana.

Por el momento, no se ha identificado quién está detrás de esta operación a gran escala. Sin embargo, el hecho de que el exploit de XSS se haya utilizado principalmente para redirecciones en lugar de ataques más agresivos, como el robo de credenciales o cookies, sugiere que podría tratarse de una empresa de publicidad con prácticas cuestionables que usa esta técnica para monetizar anuncios.

Se recomienda a los administradores de Krpano actualizar su instalación a la versión más reciente y desactivar la opción *passQueryParameters*. Además, los propietarios de sitios web afectados deberían utilizar *Google Search Console* para detectar y eliminar cualquier página comprometida.