Un paseo por el lado del cliente

JavaScript es esencial para ofrecer experiencias de usuario impactantes. Sin embargo, su uso hace que los sitios web sean vulnerables a las amenazas del lado del cliente y al robo de datos del usuario final.

Los ataques de robo de información web, Magecart y formjacking pueden tener consecuencias perjudiciales para las marcas, desde multas hasta erosión de la confianza y pérdida de ingresos.

Dónde se origina la infección

Explotación de las vulnerabilidades propias

Configuración incorrecta de la seguridad, vulnerabilidades del marco, etc.

Ataques a la cadena de suministro de terceros

Inyección de código malicioso a través de un proveedor externo autorizado

Cómo se roban los datos de los usuarios finales

Un usuario final navega online

Aplicación web

El usuario final introduce **información confidencial** en la página de pago

Con la inyección de **scripts maliciosos** se roban los datos

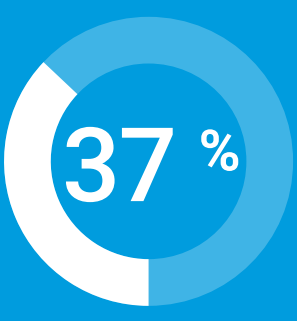
JavaScript se ve **comprometido**

Los datos se recopilan y **se filtran** en el dominio controlado por el atacante

El uso de JavaScript de terceros sitúa a las marcas en posición de vulnerabilidad

Porcentaje de JavaScript en sitios web procedentes de fuentes ajenas

Retail y comercio[1]



Servicios financieros[2]

Una amenaza para empresas de todos los tamaños

El 81 % de los grandes retailers online afirma que en su organización se detectó un comportamiento sospechoso de los scripts en 2022[3]

Un impacto devastador

4,45M $	Coste medio total de una filtración de datos a nivel mundial en 2023[4]
9,48M $	Coste medio total de una filtración de datos en EE. UU. en 2023[4]

El cumplimiento de PCI requiere ahora seguridad en el lado del cliente

PCI Security Standards Council

A fin de evitar sanciones, cualquier organización que procese datos de tarjetas de pago debe cumplir los nuevos **requisitos de seguridad de PCI DSS v4.0 para JavaScript antes de 2025**[5]

Requisito 6.4.3 | **Requisito 11.6.1**

Akamai Client-Side Protection & Compliance

Akamai Client-Side Protection & Compliance protege contra las amenazas de JavaScript, optimiza los flujos de trabajo de PCI DSS v4.0 y mantiene la seguridad de los datos de los usuarios finales. Proporciona visibilidad de las vulnerabilidades de JavaScript y analiza el comportamiento de los scripts para detectar la actividad dañina y maliciosa. Además, ofrece alertas útiles que permiten a los equipos de seguridad protegerse rápidamente contra los ataques del lado del cliente y mitigarlos.

Para obtener más información, visite nuestra página de productos o póngase en contacto con el equipo de ventas de Akamai.

1. Análisis de las tendencias de las amenazas: Ataques en el sector del comercio | SOTI de Akamai 2023
2. Lo que está en juego con la innovación: Tendencias de ataque a los servicios financieros | SOTI de Akamai 2023
3. De bots malintencionados a scripts maliciosos: La eficacia de las defensas especializadas | 2023
4. IBM Cost of a Data Breach Report (Informe de IBM sobre el coste de la vulneración de datos) | 2023
5. PCI DSS v4.0 | 2022

 | Publicado en diciembre de 2023