La empresa Sansec ha advertido sobre una vulnerabilidad crítica en la API REST de Magento que podría permitir a atacantes sin autenticación subir archivos ejecutables arbitrarios, logrando ejecución de código y secuestro de cuentas.

La falla ha sido denominada PolyShell por Sansec, ya que el ataque se basa en ocultar código malicioso haciéndolo pasar por una imagen. Hasta el momento, no hay pruebas de que este problema haya sido explotado en entornos reales. La vulnerabilidad de carga de archivos sin restricciones afecta a todas las versiones de Magento Open Source y Adobe Commerce hasta la versión 2.4.9-alpha2.

La firma de seguridad neerlandesa explicó que el origen del problema radica en que la API REST de Magento permite la carga de archivos como parte de las opciones personalizadas de los productos en el carrito.

«Cuando una opción de producto tiene el tipo 'file', Magento procesa un objeto file_info incrustado que contiene datos codificados en base64, un tipo MIME y un nombre de archivo,» indicó. *«El archivo se guarda en el directorio pub/media/custom_options/quote/ del servidor.»*

Dependiendo de la configuración del servidor web, esta debilidad podría facilitar la ejecución remota de código mediante la subida de archivos PHP o el secuestro de cuentas a través de ataques XSS almacenados.

Sansec también señaló que Adobe corrigió el problema en la rama preliminar 2.4.9 como parte del boletín APSB25-94, pero las versiones actuales en producción aún no cuentan con un parche independiente.

«Aunque Adobe proporciona una configuración de servidor web de ejemplo que reduciría considerablemente el impacto, la mayoría de las tiendas utilizan configuraciones personalizadas ofrecidas por sus proveedores de hosting,» añadió la compañía.

Para reducir posibles riesgos, se recomienda a las tiendas de comercio electrónico adoptar las siguientes medidas:

Restringir el acceso al directorio de carga («pub/media/custom_options/»).
Verificar que las reglas de nginx o Apache HTTP Server bloqueen el acceso a dicho directorio.
Analizar las tiendas en busca de web shells, puertas traseras u otros tipos de malware.

«Bloquear el acceso no impide la subida de archivos, por lo que los atacantes aún podrían cargar código malicioso si no se utiliza un WAF especializado,» advirtió Sansec.

Este escenario coincide con una campaña activa detectada por Netcraft, que ha identificado la compromisión y alteración (defacement) de miles de sitios de comercio electrónico basados en Magento en distintos sectores y regiones. La actividad, iniciada el 27 de febrero de 2026, consiste en que los atacantes suben archivos de texto plano a directorios web accesibles públicamente.

«Los atacantes han desplegado archivos txt de defacement en aproximadamente 15,000 hostnames distribuidos en 7,500 dominios, incluyendo infraestructuras de marcas globales reconocidas, plataformas de comercio electrónico y servicios gubernamentales,» señaló la investigadora de seguridad Gina Chow.

Por ahora, no está claro si estos ataques aprovechan una vulnerabilidad específica de Magento o errores de configuración, ni si son obra de un único actor malicioso. La campaña ha afectado infraestructuras de marcas reconocidas a nivel mundial como Asus, FedEx, Fiat, Lindt, Toyota y Yamaha, entre otras.