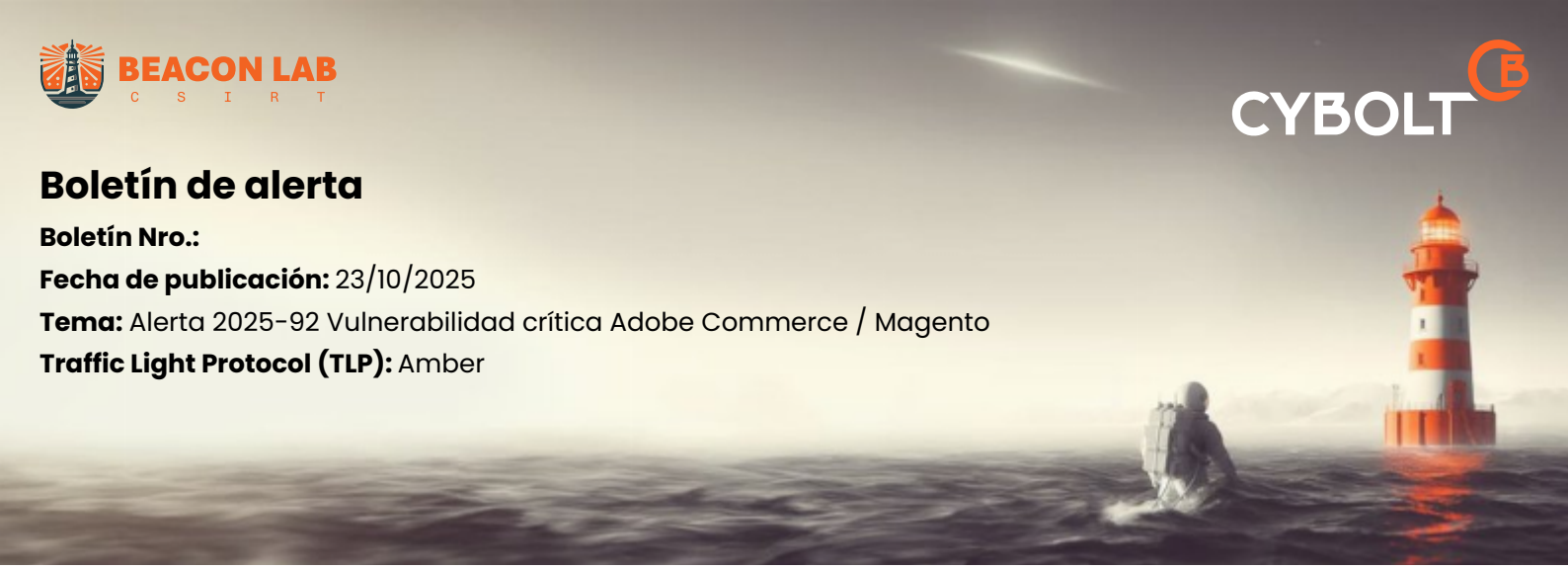


Boletín de alerta

Boletín Nro.:
Fecha de publicación: 23/10/2025
Tema: Alerta 2025-92 Vulnerabilidad crítica Adobe Commerce / Magento
Traffic Light Protocol (TLP): Amber

Producto(s) afectado(s):

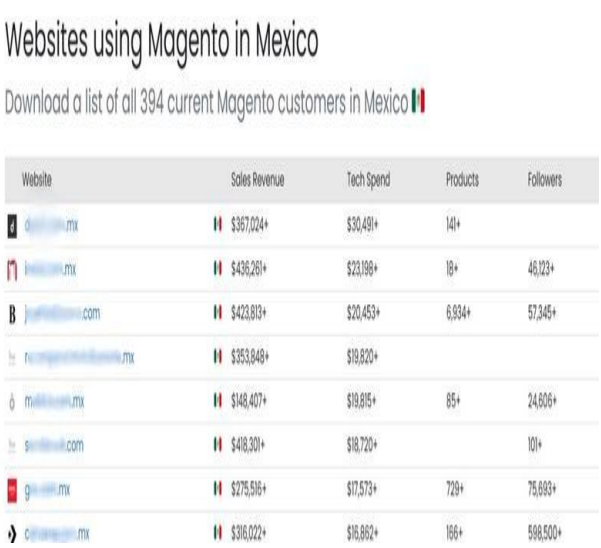
- **Adobe Commerce / Magento Open Source**:
  - 2.4.9-alpha2 y anteriores;
  - 2.4.8-p2 y anteriores; 2.4.7-p7 y anteriores;
  - 2.4.6-p12 y anteriores; 2.4.5-p14 y anteriores;
  - 2.4.4-p15 y anteriores.

Descripción

Recientemente, el equipo de seguridad de Adobe identificó la **CVE-2025-54236**, apodada *SessionReaper*, una vulnerabilidad de Improper Input Validation en el componente ServiceInputProcessor del Web API / Commerce REST API de Adobe Commerce / Magento. Adobe publicó un boletín y un hotfix el 9 de septiembre de 2025, clasificando esta vulnerabilidad con una severidad crítica de CVSS 9.1, ya que permite el secuestro de sesiones de cuentas de clientes sin interacción del usuario al permitir solicitudes API especialmente formadas que evaden las validaciones y controles de seguridad previstos.

La raíz del problema está en la validación insuficiente de entradas (posibles casos de nested deserialization y procesamiento anidado en entradas del API) que permiten modificar el flujo de sesión o inyectar parámetros que permiten suplantar/recuperar sesiones. Desde su publicación se han reportado explotaciones y actividad maliciosa contra tiendas Magento/Adobe Commerce, como ataques masivos y cuentas comprometidas, por lo que el riesgo operativo para comercios en producción es alto y la ventana de exposición es real mientras existan instancias sin parchear. Además, se han publicado PoC experimentales que muestran métodos de explotación tanto en LAN como con técnicas de coacción de conexión a distancia.

En México se identifican casi 400 sitios de comercio electrónico que utilizan Adobe Commerce (Magento), muchos de ellos operando tiendas en línea activas y potencialmente expuestas si no han aplicado los parches más recientes frente a esta vulnerabilidad.



Comercios electrónicos utilizando AdobeCommerce (Magento) en México

Recomendaciones:

- **Bloquear el acceso al Commerce REST API** desde Internet (si la tienda no lo requiere públicamente) o limitarlo mediante ACLs / IP allowlists.
- **Implementar reglas WAF** que bloqueen patrones maliciosos conocidos hacia los endpoints del API (filtrar payloads sospechosos, bloquear parámetros anómalos). Muchos proveedores WAF han publicado reglas de emergencia tras la divulgación; aplicar rápidamente.
- **Rotar/invalidar tokens y cookies de sesión** y forzar reautenticación si se sospecha compromiso.
- **Revisar y endurecer la validación de entrada** en integraciones y extensiones personalizadas que interactúen con el ServiceInputProcessor.

Solución:

Aplicar el parche oficial de Adobe inmediatamente: Adobe publicó un boletín y parches/hotfixes para las ramas afectadas. Mismo que se puede encontrar en el siguiente enlace

- https://helpx.adobe.com/security/products/magento/apsb25-88.html

Información adicional:

- Why nested deserialization is STILL harmful – Magento RCE (CVE-2025-54236) › Searchlight Cyber
- Over 250 Magento Stores Hit Overnight as Hackers Exploit New Adobe Commerce Flaw
- NVD – CVE-2025-54236