

Hackers aprovechan el error de Magento para robar datos de pago de sitios web de comercio electrónico

Nueva Vulnerabilidad en “Magento”, ahora “Adobe commerce”, la plataforma de comercio electrónico perteneciente a “Adobe”, que permite robar datos de los pagos efectuados en la página web.


Las Versiones Afectadas:

Versiones afectadas		
Producto	Versión	Plataforma
Adobe Commerce	2.4.6-p3 y versiones anteriores 2.4.5-p5 y versiones anteriores 2.4.4-p6 y versiones anteriores 2.4.3-ext-5 y versiones anteriores* 2.4.2-ext-5 y versiones anteriores* 2.4.1-ext-5 y versiones anteriores* 2.4.0-ext-5 y versiones anteriores* 2.3.7-p4-ext-5 y versiones anteriores*	Todas
Magento Open Source	2.4.6-p3 y versiones anteriores 2.4.5-p5 y versiones anteriores 2.4.4-p6 y versiones anteriores	Todas

La vulnerabilidad fue publicada como “CVE-2024-20720”, con una puntuación CVSS 9.1, en la cual se detalla que se explota una falla critica por la cual se inyecta un “backdoor” para robar los datos, el cual se ejecuta cada vez que un usuario ejecuta una compra.

Severity CVSS Version 3.x CVSS Version 2.0

CVSS 3.x Severity and Metrics:

 **CNA:** Adobe Systems Incorporated **Base Score:** 9.1 CRITICAL **Vector:** CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:C/C:H/I:H/A:H

Solución

Adobe categoriza estas actualizaciones de acuerdo con los siguientes [niveles de prioridad](#) y recomienda que los usuarios actualicen los programas a las versiones más recientes.

Producto	Versión actualizada	Plataforma	Nivel de prioridad	Instrucciones de instalación
Adobe Commerce	2.4.6-p4 para 2.4.6-p3 y versiones anteriores 2.4.5-p6 para 2.4.5-p5 y versiones anteriores 2.4.4-p7 para 2.4.4-p6 y versiones anteriores 2.4.3-ext-6 para 2.4.3-ext-5 y versiones anteriores* 2.4.2-ext-6 para 2.4.2-ext-5 y versiones anteriores* 2.4.1-ext-6 para 2.4.1-ext-5 y versiones anteriores* 2.4.0-ext-6 para 2.4.0-ext-5 y versiones anteriores* 2.3.7-p4-ext-6 para 2.3.7-p4-ext-5 y versiones anteriores*	Todas	3	Notas de la versión 2.4.x
Magento Open Source	2.4.6-p4 para 2.4.6-p3 y versiones anteriores 2.4.5-p6 para 2.4.5-p5 y versiones anteriores 2.4.4-p7 para 2.4.4-p6 y versiones anteriores	Todas	3	

Nota: * Estas versiones solo son aplicables a los clientes que participan en el [Programa de asistencia ampliada](#)

La vulnerabilidad se encuentra remediada a través de los parches de seguridad de la aplicación publicados el 13/02/2024.

Actualización de seguridad disponible para Adobe Commerce | APSB24-03

ID del boletín	Fecha de publicación	Prioridad
APSB24-03	13 de febrero de 2024	3

Se pudo establecer que la mayoría de los ataques provenían de las siguientes IPs, recomendamos generar una regla de firewall con las siguientes IPs:

Attribution

We observed the following attacker IPs:

- 45.146.54.58
- 45.146.54.59
- 45.146.54.61
- 45.146.54.67
- 216.73.163.170
- 216.73.163.182