



BOLETÍN DE ALERTA

Boletín Nro.: 2022-09

Fecha de publicación: 18/02/2022

Tema: Vulnerabilidades críticas de ejecución remota de comandos (RCE) en plataformas Adobe Commerce y Magento.

Software afectado:

- **Adobe Commerce:** 2.3.3-p1 a 2.3.7-p2 (en todas sus plataformas), y 2.4.0 a 2.4.3-p1 (en todas sus plataformas). La versión 2.3.3 y anteriores no son vulnerables
- **Magento Open Source:** 2.3.3-p1 a 2.3.7-p2 (en todas sus plataformas), y 2.4.0 a 2.4.3-p1 (en todas sus plataformas). La versión 2.3.3 y anteriores no son vulnerables

Descripción:

Adobe ha lanzado parches de seguridad para subsanar dos vulnerabilidades críticas de ejecución remota de comandos (RCE) en sus plataformas Commerce y Magento, identificadas como [CVE-2022-24086](#) en un primer momento, y posteriormente [CVE-2022-24087](#) (identificador reservado aún).

Estas vulnerabilidades de severidad crítica tienen una puntuación de 9.8. Las mismas se deben a una incorrecta validación de entrada (*input*) durante el proceso de *checkout* en ambos productos. Un atacante podría aprovechar estas vulnerabilidades sin interacción del usuario para realizar un ataque combinado de inyección SQL e inyección de objetos PHP y así lograr una ejecución remota de código (RCE) en el dispositivo vulnerable.

Cabe destacar que, si bien no se divulgaron los detalles técnicos del ataque ni existen aún *exploits* disponibles públicamente, a nivel global ya se reportó una campaña de ataques que explotan estas vulnerabilidades afectando a más de 500 sitios web que utilizan las mencionadas plataformas.

Impacto:

Un atacante podría realizar ataques de ejecución remota de código (RCE) en los sistemas afectados.



Solución:

Recomendamos instalar las actualizaciones correspondientes de acuerdo a su producto provistas por Adobe en el siguiente enlace:

<https://support.magento.com/hc/en-us/articles/4426353041293-Security-updates-available-for-Adobe-Commerce-APSB22-12->.

Nota: es necesaria la instalación de ambos parches para subsanar el riesgo, debido a que el parche para [CVE-2022-24086](#) no es suficiente para mitigar ambas vulnerabilidades reportadas.

Para más información con relación al proceso de instalación puede acceder al siguiente enlace:

<https://support.magento.com/hc/en-us/articles/360028367731>

Información adicional:

- <https://thehackernews.com/2022/02/another-critical-rce-discovered-in.html>
- <https://securityaffairs.co/wordpress/127999/hacking/cve-2022-24086-zero-day.html>
- <https://support.magento.com/hc/en-us/articles/4426353041293-Security-updates-available-for-Adobe-Commerce-APSB22-12->
- <https://nvd.nist.gov/vuln/detail/CVE-2022-24086>
- <https://nvd.nist.gov/vuln/detail/CVE-2022-24087>