Boletín de alerta

Boletín Nro.:

Fecha de publicación: 13/08/2026

Tema: Alerta 2026-89 Múltiples vulnerabilidades críticas en ColdFusion, Commerce/Magento y Campaign Classic

Traffic Light Protocol (TLP): Amber

Producto(s) afectado(s):

- Adobe ColdFusion
  - Adobe ColdFusion 2025 Update 11 y versiones anteriores.
- Adobe Commerce / Magento Open Source
  - Adobe Commerce:
    - 2.4.9-2026-jul y anteriores.
    - 2.4.8-2026-jul y anteriores.
    - 2.4.7-2026-jul y anteriores.
    - 2.4.6-2026-jul y anteriores.
    - 2.4.5-2026-jul y anteriores.
    - 2.4.4-2026-jul y anteriores.
  - Adobe Commerce B2B:
    - 1.5.3-2026-jul y anteriores.
    - 1.5.2-2026-jul y anteriores.
    - 1.4.2-2026-jul y anteriores.
    - 1.3.4-2026-jul y anteriores.
    - 1.3.3-2026-jul y anteriores.
  - Magento Open Source:
    - 2.4.9-2026-jul y anteriores.
    - 2.4.8-2026-jul y anteriores.
    - 2.4.7-2026-jul y anteriores.
    - 2.4.6-2026-jul y anteriores.
- Adobe Campaign Classic
  - Adobe Campaign Classic v7:
- 7.4.3 Build 9399 y versiones anteriores.

Descripción

Se ha divulgado una vulnerabilidad de seguridad identificada como **CVE-2026-17106**, denominada **CopyEscape**, que afecta al mecanismo utilizado por Docker para copiar archivos desde un contenedor hacia el sistemAdobe publicó el **11 de agosto de 2026** nuevas actualizaciones de seguridad para varios de sus productos empresariales, incluyendo **Adobe ColdFusion, Adobe Commerce, Magento Open Source y Adobe Campaign Classic**.

Las vulnerabilidades corregidas incluyen fallas críticas capaces de provocar **ejecución arbitraria de código, escalamiento de privilegios, inyección de comandos del sistema operativo, inyección de código dinámicamente evaluado, inyección SQL y denegación de servicio**.

Dentro de las actualizaciones destacan los siguientes siete identificadores:

CVE-2026-48362 (CVSS 10) – Adobe ColdFusion OS Command Injection: Un atacante remoto no autenticado podría aprovechar la neutralización incorrecta de elementos especiales utilizados dentro de comandos del sistema para conseguir ejecución de código arbitrario sobre un servidor ColdFusion vulnerable.

CVE-2026-48273 (CVSS 9.9) – Adobe ColdFusion Eval Injection: Un atacante con bajos privilegios podría introducir contenido manipulado que posteriormente sea interpretado por el entorno de ejecución de ColdFusion, provocando la ejecución de código arbitrario.

CVE-2026-71384 (CVSS 9.6) – Adobe ColdFusion Incorrect Authorization: Un atacante localizado en una red adyacente puede explotar la falla sin necesidad de contar con credenciales válidas y provocar una condición de denegación de servicio sobre la aplicación afectada.

CVE-2026-71362 (CVSS 9.1) – Adobe Commerce / Magento Incorrect Authorization: La explotación exitosa podría permitir que un atacante obtenga privilegios superiores dentro de la plataforma y acceda o modifique información que normalmente debería encontrarse restringida.

CVE-2026-71398 (CVSS 10) – Adobe Campaign Classic Incorrect Authorization: corresponde a una vulnerabilidad crítica de **autorización incorrecta** que puede provocar ejecución arbitraria de código en instalaciones vulnerables de Adobe Campaign Classic.

CVE-2026-27302 (CVSS 10) – Adobe Campaign Classic Incorrect Authorization: Una validación incorrecta de autorización permite que un atacante remoto sin credenciales pueda alcanzar funcionalidades que posteriormente deriven en ejecución arbitraria de código.

CVE-2026-48381 (CVSS 9) – Adobe Campaign Classic SQL Injection: Un atacante remoto puede introducir contenido manipulado dentro de consultas SQL procesadas por Adobe Campaign Classic.

Solución

Se recomienda instalar las actualizaciones de seguridad publicadas el 11 de agosto de 2026:

- Adobe ColdFusion
  - ColdFusion 2025 2025.0.12

    - ColdFusion 2023 2023.0.23
- Adobe Commerce
    - 2.4.9-2026-aug
    - 2.4.8-2026-aug
    - 2.4.7-2026-aug
    - 2.4.6-2026-aug
    - 2.4.5-2026-aug
    - 2.4.4-2026-aug
- • Magento Open Source
    - 2.4.9-2026-aug
    - 2.4.8-2026-aug
    - 2.4.7-2026-aug
    - 2.4.6-2026-aug
- Adobe Campaign Classic
    - 7.4.4 Build 9400

Información adicional:

- **Adobe Security Bulletin APSB26-90 – Adobe ColdFusion**
- **Adobe Security Bulletin APSB26-92 – Adobe Commerce / Magento Open Source**
- **Adobe Security Bulletin APSB26-123 – Adobe Campaign Classic**
- **Adobe Product Security Incident Response Team**