

Alert Bulletin

Bulletin N.:

Publication Date: 13/08/2026

Subject: Alert 2026-89 Multiple critical vulnerabilities in ColdFusion, Commerce/Magento and Campaign Classic

Traffic Light Protocol (TLP): Amber

Affected product(s):

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

Description

A security vulnerability identified as **CVE-2026-17106**, named **CopyEscape**, has been disclosed that affects the mechanism used by Docker to copy files from a container to the system. Adobe published on **August 11, 2026** new security updates for several of its enterprise products, including **Adobe ColdFusion, Adobe Commerce, Magento Open Source, and Adobe Campaign Classic**.

The fixed vulnerabilities include critical flaws capable of causing **arbitrary code execution, privilege escalation, operating system command injection, dynamically evaluated code injection, SQL injection, and denial of service**.

Within the updates, the following seven identifiers stand out:

CVE-2026-48362 (CVSS 10) – Adobe ColdFusion OS Command Injection: A remote unauthenticated attacker could exploit the improper neutralization of special elements used within system commands to achieve arbitrary code execution on a vulnerable ColdFusion server.

CVE-2026-48273 (CVSS 9.9) – Adobe ColdFusion Eval Injection: An attacker with low privileges could introduce manipulated content that is subsequently interpreted by the ColdFusion runtime environment, causing arbitrary code execution.

CVE-2026-71384 (CVSS 9.6) – Adobe ColdFusion Incorrect Authorization: An attacker located on an adjacent network can exploit the flaw without needing valid credentials and cause a denial-of-service condition on the affected application.

CVE-2026-71362 (CVSS 9.1) – Adobe Commerce / Magento Incorrect Authorization: Successful exploitation could allow an attacker to obtain elevated privileges within the platform and access or modify information that should normally be restricted.

CVE-2026-71398 (CVSS 10) – Adobe Campaign Classic Incorrect Authorization: corresponds to a critical **incorrect authorization** vulnerability that can cause arbitrary code execution on vulnerable Adobe Campaign Classic installations.

CVE-2026-27302 (CVSS 10) – Adobe Campaign Classic Incorrect Authorization: An improper authorization validation allows a remote attacker without credentials to reach functionalities that subsequently lead to arbitrary code execution.

CVE-2026-48381 (CVSS 9) – Adobe Campaign Classic SQL Injection: A remote attacker can introduce manipulated content within SQL queries processed by Adobe Campaign Classic.

Solution

It is recommended to install the security updates published on August 11, 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

Additional information:

- [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](#)