**GOVERNMENT OF THE REPUBLIC OF VANUATU**

PRIME MINISTER'S OFFICE

CERTVU
DEPARTMENT OF COMMUNICATIONS & DIGITAL TRANSFORMATION

PM B 9108 Port Vila, Vanuatu
Tel: (678) 33380

**GOUVERNEMENT DE LA REPUBLIQUE DU VANUATU**

BUREAU DU PREMIER MINISTRE

CERTVU

DEPARTMENT DE COMMUNICATION ET DE TRANSFORMATION NUMERIQUE

SPP 9108 Port Vila, Vanuatu
Tel: (678) 33380

13 August 2026

**Advisory 189: Adobe ColdFusion, Commerce, and Campaign Classic Critical Vulnerabilities**

**Release Date:** 12th August 2026
**Impact:** CRITICAL
**TLP:** CLEAR

The Department of Communications and Digital Transformation (DCDT) through CERT Vanuatu (CERTVU), provides the following advisory.

This alert is relevant to Organizations and System/Network administrators that utilize the above products. This alert is intended to be understood by technical users and systems administrators.

# What is it?

Adobe released security updates addressing seven vulnerabilities across ColdFusion (APSB26-90), Commerce (APSB26-92), and Campaign Classic (APSB26-123). Three of the seven carry the maximum CVSS score of 10.0, and the ColdFusion and Campaign Classic updates both carry Adobe's Priority 1 rating, indicating a heightened risk of imminent exploitation.
The most severe issues are an OS command injection flaw in ColdFusion (CVE-2026-48362, CVSS 10.0) and two incorrect authorization flaws in Campaign Classic (CVE-2026-71398 and CVE-2026-27302, both CVSS 10.0) that could each lead to arbitrary code execution. Adobe reports no evidence of in-the-wild exploitation as of publication, but recommends installing the updates within 72 hours given the severity and exploitability of these flaws.

# What are the systems affected?

Affected systems span three separate Adobe products; organisations should check each one independently rather than assuming a single patch covers all three.

Adobe ColdFusion 2025 (Update 11 and earlier) - (Affected, CVE-2026-48362, CVE-2026-48273, CVE-2026-71384)
Adobe ColdFusion 2023 (Update 22 and earlier) - (Affected, same CVEs)
Adobe Commerce - (Affected, CVE-2026-71362)
Adobe Campaign Classic v7 on-premise and hybrid on-premise components - (Affected, CVE-2026-71398, CVE-2026-27302, CVE-2026-48381)
Adobe-hosted Campaign Classic cloud instances - (Already remediated, no customer action required)

Any organisation running on-premises ColdFusion, Commerce, or Campaign Classic should treat this as urgent, given the maximum-severity ratings and Priority 1 classification on two of the three products.

# What does this mean?

These seven vulnerabilities cluster into four root-cause groups rather than a single attack chain, since they affect three separate products. Each is exploitable independently.

**OS Command Injection - ColdFusion (CVE-2026-48362, CVSS 10.0)**
ColdFusion improperly handles input that is passed through to operating system-level commands, allowing an attacker to execute arbitrary commands on the underlying server.

**Eval Injection - ColdFusion (CVE-2026-48273, CVSS 9.9)**
Untrusted input reaches a code-evaluation function within ColdFusion, letting an attacker run arbitrary code in the application's context without needing to inject an operating system command directly.

**Incorrect Authorization and SQL Injection - Campaign Classic (CVE-2026-71398, CVE-2026-27302, CVE-2026-48381)**
Authorization checks are improperly enforced on certain Campaign Classic functions, and a separate SQL injection flaw allows unsanitized input to reach a database query. Both routes can lead to arbitrary code execution on affected on-premise instances.

**Denial of Service and Privilege Escalation (CVE-2026-71384 ColdFusion, CVE-2026-71362 Commerce)**
Incorrect authorization in ColdFusion can be abused to **disrupt application availability**, while a similar flaw in Commerce allows a lower-privileged user to escalate to permissions beyond their intended access level.

# Mitigation process

CERTVU recommends the following:

### 1. Apply Adobe Security Updates Immediately

Update ColdFusion to 2025.0.12 or 2023.0.23 per APSB26-90; update Commerce per APSB26-92; and update on-premise or hybrid Campaign Classic deployments to ACC v7 7.4.4 build 9400 per APSB26-123. Adobe-hosted Campaign Classic cloud instances have already been remediated and require no customer action. Given the Priority 1 rating on ColdFusion and Campaign Classic, apply these updates within 72 hours rather than waiting for a scheduled maintenance window.

*Adobe Security Bulletin APSB26-90 (ColdFusion)*

**2. Reduce Exposure in the Interim**

Restrict administrative and management interfaces for all three products to trusted internal networks or a VPN, and review application and database logs for anomalous OS command execution, code evaluation, or SQL query patterns around the disclosure window. Note that this is the second maximum-severity Campaign Classic disclosure in two weeks - CERTVU Advisory 178 covered CVE-2026-48449 on 2 August 2026 - so any organisation running on-premise Campaign Classic should treat patching that product as an ongoing priority rather than a one-time fix.

# Reference


1. https://helpx.adobe.com/security/products/coldfusion/apsb26-90.html
2. https://helpx.adobe.com/security/products/magento/apsb26-92.html
3. https://helpx.adobe.com/security/products/campaign/apsb26-123.html
4. https://thehackernews.com/2026/08/adobe-patches-three-cvss-100-coldfusion.html


.