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

3 August 2026

Advisory 178: Adobe Campaign Classic Critical Vulnerability – Arbitrary Code Execution (CVE-2026-48449, CVSS 10.0)

Release Date: 29th July 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 has released security updates addressing two vulnerabilities in Adobe Campaign Classic (ACC), its enterprise marketing automation platform. The most severe, CVE-2026-48449 (CWE-863, Incorrect Authorization), carries the maximum CVSS v3.1 base score of 10.0 and could result in arbitrary code execution in the context of the current user without requiring any user interaction. A second flaw, CVE-2026-48448 (CWE-89, SQL Injection), scores 8.6 and could allow arbitrary file system read. Adobe states it is not aware of either vulnerability being exploited in the wild. Separately, Adobe has also released updates for Adobe Bridge addressing eight Critical-rated vulnerabilities that could lead to privilege escalation and arbitrary code execution.

What are the systems affected?

The following products and versions are affected:

- Adobe Campaign Classic (ACC) v7: 7.4.3 build 9397 and earlier, on Windows and Linux

- Adobe Bridge (versions affected by the eight vulnerabilities listed below; see Adobe's Bridge security bulletin APSB26-89 for exact version ranges)

This bulletin applies only to fully on-premise deployments of Adobe Campaign Classic and to the on-premise components of hybrid deployments. Adobe-hosted (cloud) instances of Campaign Classic have already been remediated by Adobe and require no customer action.

The eight Adobe Bridge vulnerabilities fixed in this cycle are:

- CVE-2026-48395 (CVSS 8.6) — Untrusted search path vulnerability leading to arbitrary code execution
- CVE-2026-48396 (CVSS 8.6) — Incorrect authorization vulnerability leading to arbitrary code execution
- CVE-2026-48390 (CVSS 8.6) — Incorrect authorization vulnerability leading to privilege escalation
- CVE-2026-48391 (CVSS 8.2) — Untrusted search path vulnerability leading to arbitrary code execution
- CVE-2026-48374 (CVSS 7.8) — Path traversal vulnerability leading to arbitrary code execution
- CVE-2026-48392 (CVSS 7.8) — Out-of-bounds write vulnerability leading to arbitrary code execution
- CVE-2026-48393 (CVSS 7.8) — Out-of-bounds write vulnerability leading to arbitrary code execution
- CVE-2026-48394 (CVSS 7.8) — Out-of-bounds write vulnerability leading to arbitrary code execution

What does this mean?

Typical exploitation flow for CVE-2026-48449:

1. Incorrect authorization identified
    - An attacker locates a Campaign Classic on-premise instance where authorization checks on a given function or endpoint are improperly enforced.
2. Unauthenticated or low-privilege access leveraged
    - The flaw does not require any user interaction, meaning an attacker can attempt exploitation directly against a reachable instance without needing a victim to click or open anything.
3. Arbitrary code execution
    - Successful exploitation allows arbitrary code execution in the context of the current user, and given the maximum CVSS score, the scope is rated as changed (impacting confidentiality, integrity, and availability).
4. Compounding risk via SQL injection
    - The companion flaw, CVE-2026-48448, allows arbitrary file system reads via SQL injection and could be used to gather further information to support an attack chain.

This vulnerability requires:

- No authentication
- No user interaction
- Low attack complexity

Mitigation process

CERTVU recommends the following:

1. **Apply Security Updates Immediately**
    - Update on-premise Adobe Campaign Classic v7 installations to build 7.4.3 build 9398 or later without delay, given the maximum CVSS 10.0 severity of CVE-2026-48449. Adobe-hosted (cloud) instances have already been remediated and require no customer action.
2. **Patch Adobe Bridge**
    - Update Adobe Bridge to the version specified in Adobe's security bulletin APSB26-89 to address the eight Critical-rated vulnerabilities affecting that product.
3. **Restrict Network Exposure**
    - Where patching cannot be completed immediately, restrict network access to Campaign Classic on-premise instances to trusted administrative networks only, as an interim defense-in-depth control.
4. **Review for Prior Compromise**
    - Review application, database, and file-access logs on affected Campaign Classic and Bridge installations for any signs of unauthorized activity predating the patch, and treat any positive finding as a potential compromise requiring incident response.

Reference

1. https://helpx.adobe.com/security/products/campaign/apsb26-114.html
2. https://helpx.adobe.com/security/products/bridge/apsb26-89.html
3. https://thehackernews.com/2026/08/adobe-campaign-classic-cvss-100-flaw.html
4. https://cwe.mitre.org/data/definitions/863.html