



TLP: CLEAR

CALIFORNIA CYBERSECURITY INTEGRATION CENTER



CYBER ADVISORY

Thursday, July 30, 2026

CAL-CSIC-202607-A-015

Maximum-Severity Vulnerability found within Adobe Campaign Classic for Windows and Linux

Unauthenticated Attacker

Internal Pivoting

Full System Compromise

Update Available

The California Cybersecurity Integration Center (Cal-CSIC) has become aware of a maximum-severity vulnerability found in Adobe Campaign Classic (ACC) for Windows and Linux. Adobe Campaign Classic is a marketing infrastructure platform and is used for data modeling, workflow automation and delivery management. CVE-2026-48449 carries a maximum CVSS 3.1 score of 10.0.¹

CVE-2026-48449 is an Incorrect Authorization vulnerability. It allows an unauthenticated attacker with network access to exploit an authorization bypass within the platform. Successful exploitation of this CVE allows the unauthenticated attacker to execute arbitrary code within the current context of the user that can lead to full system compromise. The attacker would have access to customer databases, PII, email infrastructure, and further pivot towards connected Customer Relationship Managers (CRMs) like Salesforce and SAP.² This CVE does not require credentials or user interaction.

Adobe has acknowledged the vulnerability and has issued a security advisory with update guidance that addresses CVE-2026-48449.³ There is currently no known exploitation in the wild regarding this vulnerability. The Cal-CSIC recommends following the Fortinet's update guidance as soon as possible.

For additional details regarding CVE-2026-48449 please use this link:

CVE-2026-48449 Security Advisory:

<https://helpx.adobe.com/security/products/campaign/apsb26-114.html>

WARNING: This document is the property of the California Cybersecurity Integration Center (CAL-CSIC) and follows Traffic Light Protocol (TLP) standards. Except for **TLP: CLEAR**, all TLP designations require recipients to control, store, handle, transmit, and dispose of this product accordingly. Do not release to the public, media, or unauthorized personnel without prior CAL-CSIC approval. This document may contain information exempt from public release under the California Public Records Act (Govt. Code Sec. 7920.000 et seq.). CAL-CSIC does not guarantee the completeness or accuracy of the information.

TLP: CLEAR

Affected Products and Versions

Product	Affected Version	Updated Version
Adobe Campaign Classic	ACC v7: 7.4.3 build 9397 and earlier	ACC v7: 7.4.3 build 9398

Cal-CSIC services are provided at no cost to assist organizations in strengthening their cybersecurity defenses. If you need assistance or wish to verify this communication, please contact us at (833) REPORT-1, or (916) 636-2997. Visit our website for more details: [California Cybersecurity Integration Center | California Governor's Office of Emergency Services](#)

References

¹ OpenCVE; "CVE-2026-48449"; <https://app.openCVE.io/cve/CVE-2026-48449>; accessed 30 July 2026

² ThreatAft; "Adobe Campaign Classic RCE — CVE-2026-48449 (CVSS 10); <https://threataft.com/articles/adobe-campaign-cve-2026-48449>; accessed 30 July 2026

³ Adobe; "Adobe Security Bulletin"; <https://helpx.adobe.com/security/products/campaign/apsb26-114.html>; accessed 30 July 2026

WARNING: This document is the property of the California Cybersecurity Integration Center (CAL-CSIC) and follows Traffic Light Protocol (TLP) standards. Except for **TLP: CLEAR**, all TLP designations require recipients to control, store, handle, transmit, and dispose of this product accordingly. Do not release to the public, media, or unauthorized personnel without prior CAL-CSIC approval. This document may contain information exempt from public release under the California Public Records Act (Govt. Code Sec. 7920.000 et seq.). CAL-CSIC does not guarantee the completeness or accuracy of the information.

TLP: CLEAR