CYBER ADVISORY

Thursday, June 11, 2026 **CAL-CSIC-202606-A-007**

Maximum-Severity Vulnerabilities Impacting Adobe Campaign Classic

Arbitrary Code Execution	No User Interaction Required	Change of Scope	Patch Available

The Cybersecurity Integration Center (CSIC) has become aware of two maximum-severity vulnerabilities impacting Adobe Campaign Classic. CVE-2026-47938 and CVE-2026-48303 both carry a CVSS 3.1 score of 10.0.[1] [2]

CVE-2026-47938 is a Server-Side Request Forgery (SSRF) vulnerability. The vulnerability initially resulted in arbitrary code execution in the context of the current user. However, the scope has changed in that vulnerability would result in privilege escalation and chain into Remote Code Execution. Successful exploitation of this vulnerability would allow an attacker to pivot from the Adobe application server to internal networks.[3]

CVE-2026-48303 is an Incorrect Authorization vulnerability that enables a remote, unauthenticated attacker to bypass authorization logic to execute arbitrary code in the context of the current user – meaning that the attacker's code would inherit the exact same permissions and access rights as the user account running the application. The impacts of this vulnerability are dependent on the privilege level of the compromised account. This vulnerability does not require user interaction to execute, so a remote attacker could successfully exploit the flaw through exposed web interfaces or APIs. Compromised service accounts with mis-authorized actions can lead to a fully system compromise.[4]

There have not been reports of confirmed exploitation in the wild for both CVE-2026-47938 and CVE-2026-48303. There are currently no publicly available Proof-of-Concepts for either vulnerability. Adobe has issued a security bulletin for these vulnerabilities and has released a patch to fix these vulnerabilities.

The Cal-CSIC recommends following Adobe's patching guidance.[5] For additional details for both CVE-2026-47938 and CVE-2026-48303, please use this link:

https://helpx.adobe.com/security/products/campaign/apsb26-66.html

Affected Product(s) and Version(s)

Product	Version
Adobe Campaign Classic (Windows, Linux)	ACC v7 7.4.3 Build 9394 and earlier

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-2026-47938"; https://app.opencve.io/cve/CVE-2026-47938; accessed 09 June 2026
[2] OpenCVE; "CVE-2026-48303"; https://app.opencve.io/cve/CVE-2026-47938; accessed 09 June 2026
[3] CVEFeed; "CVE-2026-47938"; https://cvefeed.io/vuln/detail/CVE-2026-47938; accessed 09 June 2026
[4] CVEFeed; "CVE-2026-48303"; https://cvefeed.io/vuln/detail/CVE-2026-48303; accessed 09 June 2026
[5] Adobe; "Adobe Security Bulletin"; https://helpx.adobe.com/security/products/campaign/apsb26-66.html; accessed 09 June 2026