



# NCSC-2026-0393

## Kwetsbaarheden verholpen in Adobe Campaign Classic

NCSC Security Advisory

Prioriteit: Normaal

Gepubliceerd op: 24-09-2026

**TLP:WHITE**

### Toegestane verspreiding van TLP:WHITE

(Traffic Light Protocol)

Deze handreiking bevat het label TLP:WHITE en wordt door het NCSC verspreid. Het NCSC gebruikt het Traffic Light Protocol (TLP) om eenduidig te definiëren wat er met de informatie mag gebeuren. Wanneer informatie is voorzien van een TLP-aanduiding weet u met wie u deze informatie mag delen. Dit staat beschreven in de standaard First ([www.first.org/tlp](http://www.first.org/tlp)).

Ontvangers van TLP:WHITE mogen de informatie publiek verspreiden.

Uw reacties zijn welkom op [info@ncsc.nl](mailto:info@ncsc.nl)

## Feiten

Adobe heeft 18 kritieke kwetsbaarheden verholpen in Adobe Campaign Classic.

## Duiding

De kwetsbaarheden betreffen onder meer code- en OS-command-injectie, SQL-injectie, onvoldoende autorisatie, onvoldoende invoervalidatie en Server-Side Request Forgery (SSRF). Alle 18 kwetsbaarheden zijn als kritiek aangemerkt en tien kunnen zonder authenticatie op afstand worden misbruikt. Succesvol misbruik kan onder meer leiden tot het uitvoeren van willekeurige code, privilege-escalatie, het omzeilen van beveiligingsmaatregelen, het uitlezen van bestanden en Denial-of-Service.

De kwetsbaarheden met kenmerk CVE-2026-82004, CVE-2026-73369, CVE-2026-84412, CVE-2026-89275, CVE-2026-75723, CVE-2026-75699, CVE-2026-75703 en CVE-2026-75721 hebben een CVSS-score van 10,0 en kunnen zonder authenticatie en gebruikersinteractie op afstand worden misbruikt. Voor zeven hiervan noemt Adobe willekeurige code-uitvoering als mogelijke impact. Voor CVE-2026-75703 noemt Adobe Denial-of-Service als impact.

## Oplossingen

Adobe heeft beveiligingsupdates uitgebracht om de kwetsbaarheden te verhelpen. Gebruikers van Adobe Campaign Classic wordt geadviseerd te updaten naar versie 7.4.4 build 9402. Adobe-hosted omgevingen zijn reeds bijgewerkt. Zie bijgevoegde referenties voor meer informatie.

## Referenties

➤ <https://helpx.adobe.com/security/products/campaign/apsb26-142.html>

## Kwetsbaarheden

| CVE                              | CVSS Score    |
|----------------------------------|---------------|
| ➤ <a href="#">CVE-2026-73369</a> | 10.0 CRITICAL |
| ➤ <a href="#">CVE-2026-75699</a> | 10.0 CRITICAL |
| ➤ <a href="#">CVE-2026-75703</a> | 10.0 CRITICAL |
| ➤ <a href="#">CVE-2026-75721</a> | 10.0 CRITICAL |
|                                  |               |

|                  |               |
|------------------|---------------|
| > CVE-2026-75723 | 10.0 CRITICAL |
| > CVE-2026-75728 | 9.1 CRITICAL  |
| > CVE-2026-82003 | 8.5 HIGH      |
| > CVE-2026-82004 | 10.0 CRITICAL |
| > CVE-2026-82008 | 9.9 CRITICAL  |
| > CVE-2026-82010 | 9.9 CRITICAL  |
| > CVE-2026-82011 | 9.1 CRITICAL  |
| > CVE-2026-82013 | 9.9 CRITICAL  |
| > CVE-2026-82443 | 9.6 CRITICAL  |
| > CVE-2026-83660 | 9.9 CRITICAL  |
| > CVE-2026-84412 | 10.0 CRITICAL |
| > CVE-2026-89275 | 10.0 CRITICAL |
| > CVE-2026-89276 | 9.9 CRITICAL  |
| > CVE-2026-82009 | 9.1 CRITICAL  |

CWE's

| CWE       | Beschrijving                                                                               |
|-----------|--------------------------------------------------------------------------------------------|
| > CWE-78  | Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection') |
| > CWE-89  | Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')       |
| > CWE-94  | Improper Control of Generation of Code ('Code Injection')                                  |
| > CWE-863 | Incorrect Authorization                                                                    |
| > CWE-918 | Server-Side Request Forgery (SSRF)                                                         |

## Getroffen producten

### Adobe

-hosted instances of  
Campaign Classic

Adobe Campaign  
Classic

## Disclaimer

The Netherlands Cyber Security Center (henceforth: NCSC-NL) maintains this page to enhance access to its information and security advisories. The use of this security advisory is subject to the following terms and conditions: NCSC-NL makes every reasonable effort to ensure that the content of this page is kept up to date, and that it is accurate and complete. Nevertheless, NCSC-NL cannot entirely rule out the possibility of errors, and therefore cannot give any warranty in respect of its completeness, accuracy or continuous keeping up-to-date. The information contained in this security advisory is intended solely for the purpose of providing general information to professional users. No rights can be derived from the information provided therein. NCSC-NL and the Kingdom of the Netherlands assume no legal liability or responsibility for any damage resulting from either the use or inability of use of this security advisory. This includes damage resulting from the inaccuracy of incompleteness of the information contained in the advisory. This security advisory is subject to Dutch law. All disputes related to or arising from the use of this advisory will be submitted to the competent court in The Hague. This choice of means also applies to the court in summary proceedings.