



NCSC-2026-0278

Kwetsbaarheden verholpen in Adobe Campaign Classic

NCSC Security Advisory

Prioriteit: Normaal

Gepubliceerd op: 06-08-2026

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).

Ontvangers van TLP:WHITE mogen de informatie publiek verspreiden.

Uw reacties zijn welkom op info@ncsc.nl

Feiten

Adobe heeft meerdere kwetsbaarheden verholpen in Adobe Campaign Classic.

Duiding

De kwetsbaarheden in Adobe Campaign Classic omvatten een Server-Side Request Forgery (SSRF) die privilege-escalatie mogelijk maakt zonder gebruikersinteractie, een onjuiste neutralisatie van speciale elementen in de template engine die leidt tot uitvoering van willekeurige code, en meerdere SQL-injectieproblemen die het uitvoeren van willekeurige SQL-commando's mogelijk maken. Daarnaast is er een onjuiste autorisatiecontrole die privilege-escalatie toestaat, een Eval Injection kwetsbaarheid die uitvoering van willekeurige code door laaggeprivilegieerde aanvallers mogelijk maakt, en een ontwerpprincipe-overschrijding die het omzeilen van beveiligingsmaatregelen en ongeautoriseerde lees toegang tot gevoelige informatie mogelijk maakt. Al deze kwetsbaarheden kunnen worden misbruikt zonder enige gebruikersinteractie, wat de kans op geautomatiseerde of remote aanvallen vergroot.

NB: Dit is geen update van de eerdere advisory NCSC-2026-0273 (<https://advisories.ncsc.nl/2026/ncsc-2026-0273.html>). Deze advisory betreft nieuw gevonden kwetsbaarheden.

Oplossingen

Adobe heeft updates uitgebracht om de kwetsbaarheden in Adobe Campaign Classic te verhelpen. Zie bijgevoegde referenties voor meer informatie.

Referenties

➤ <https://helpx.adobe.com/security/products/campaign/apsb26-120.html>

Kwetsbaarheden

CVE	CVSS Score
➤ CVE-2026-48331	10.0 CRITICAL
➤ CVE-2026-48323	10.0 CRITICAL
➤ CVE-2026-48330	10.0 CRITICAL
➤ CVE-2026-48326	9.9 CRITICAL

> CVE-2026-48333	9.8 CRITICAL
> CVE-2026-48317	9.6 CRITICAL
> CVE-2026-48399	7.5 HIGH

CWE's

CWE	Beschrijving
> CWE-89	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')
> CWE-95	Improper Neutralization of Directives in Dynamically Evaluated Code ('Eval Injection')
> CWE-657	Violation of Secure Design Principles
> CWE-863	Incorrect Authorization
> CWE-918	Server-Side Request Forgery (SSRF)
> CWE-1336	Improper Neutralization of Special Elements Used in a Template Engine

Getroffen producten

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.