



NCSC-2026-0331

Kwetsbaarheden verholpen in Adobe Campaign Classic

NCSC Security Advisory

Prioriteit: Normaal

Gepubliceerd op: 27-08-2026

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 betreffen een Server-Side Request Forgery (SSRF) en OS Command Injection in Adobe Campaign Classic. De SSRF-kwetsbaarheid maakt het mogelijk voor een aanvaller om verzoeken op de server te manipuleren, wat kan leiden tot het uitvoeren van willekeurige code zonder gebruikersinteractie. De OS Command Injection kwetsbaarheden stellen een aanvaller in staat om willekeurige besturingssysteemcommando's uit te voeren met de rechten van de huidige gebruiker, eveneens zonder dat hiervoor gebruikersinteractie nodig is. Afhankelijk van de gebruikersrechten kan dit leiden tot volledige compromittering van het systeem waarop Adobe Campaign Classic draait.

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/apsb26-134.html>

Kwetsbaarheden

CVE	CVSS Score
➤ CVE-2026-76193	10.0 CRITICAL
➤ CVE-2026-76195	10.0 CRITICAL
➤ CVE-2026-76197	10.0 CRITICAL

CWE's

CWE	Beschrijving
➤ CWE-78	Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')

[> CWE-918](#)

Server-Side Request Forgery (SSRF)

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.