Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

Advisory NCSC-2026-0517

PRIORITEIT: NORMAAL

Kwetsbaarheden verholpen in Adobe Campaign Classic

Publicatiedatum: 26-11-2026

Toegestane verspreiding: TLP:WHITE
(Traffic Light Protocol)

Deze publicatie bevat het label TLP:WHITE en wordt door het Nationaal Cyber Security Center (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 de-len. Dit staat beschreven in de standaard First (www.first.org/tlp).

Ontvangers van TLP:WHITE mogen de informatie publiek verspreiden.

Reacties zijn welkom op info@ncsc.nl.

Feiten

Adobe heeft meerdere kwetsbaarheden verholpen in Adobe Campaign Classic (ACC).

Duiding

De kwetsbaarheden in Adobe Campaign Classic betreffen onder andere code-injectie, incorrecte autorisatie, SQL-injectie en Cross-Site Scripting (XSS).

Een aanvaller met lage privileges kan hierdoor op afstand willekeurige code uitvoeren zonder gebruikersinteractie, privileges escaleren, en toegang krijgen tot gevoelige data en functionaliteiten. De code-injectie kwetsbaarheid wijzigt de uitvoering scope binnen ACC, wat ongeautoriseerde code-uitvoering mogelijk maakt. De incorrecte autorisatie kwetsbaarheid maakt het mogelijk om normale toegangscontroles te omzeilen en verhoogde rechten te verkrijgen. De SQL-injectie kwetsbaarheden stellen een aanvaller in staat om beveiligingsmechanismen te omzeilen en data te lezen of beperkt te wijzigen zonder gebruikersinteractie. De XSS-kwetsbaarheden, zowel reflected als stored, maken het mogelijk om kwaadaardige scripts uit te voeren in de browsercontext van gebruikers, wat kan leiden tot sessiekaping of ongeautoriseerde acties binnen de applicatie.

Oplossingen

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

Referenties

- https://www.adobe.com/trust/security/products/campaign/apsb26-194.html

Kwetsbaarheden

CVE	CVSS Score
CVE-2026-123342	9.9 CRITICAL
CVE-2026-123721	9.6 CRITICAL
CVE-2026-123722	9.9 CRITICAL
CVE-2026-123723	9.9 CRITICAL
CVE-2026-123986	9.9 CRITICAL
CVE-2026-123987	9.9 CRITICAL
CVE-2026-125675	9.9 CRITICAL
CVE-2026-125676	9.9 CRITICAL
CVE-2026-125716	9.3 CRITICAL
CVE-2026-125717	9.6 CRITICAL
CVE-2026-125718	9.1 CRITICAL
CVE-2026-125723	9.0 CRITICAL

CWE's

CWE	Beschrijving
CWE-79	Improper Neutralization of Input During Web Page Generation
CWE-89	Improper Neutralization of Special Elements used in an SQL Command
CWE-94	Improper Control of Generation of Code
CWE-863	Incorrect Authorization

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.