Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

NCSC-2026-0391

Kwetsbaarheden verholpen in Adobe Connect en Adobe Connect Android Mobile App

NCSC Security Advisory
Prioriteit: Normaal
Gepubliceerd op: 23-09-2026

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).

Ontvangers van TLP:WHITE mogen de informatie publiek verspreiden.

Uw reacties zijn welkom op info@ncsc.nl

Feiten

Adobe heeft 9 kwetsbaarheden verholpen in Adobe Connect en de Adobe Connect Android Mobile App. De kwetsbaarheden zijn verholpen in Adobe Connect 12.12 en Adobe Connect Android Mobile App 4.5.

Duiding

De kwetsbaarheden betreffen verschillende beveiligingsproblemen in Adobe Connect, waaronder SQL-injectie, Cross-Site Scripting (XSS), onvoldoende invoervalidatie, path traversal en onvoldoende certificaatvalidatie. De kwetsbaarheden hebben CVSS-scores variërend van middel tot kritiek. Van de in totaal 9 kwetsbaarheden zijn zeven door Adobe als kritiek aangemerkt. Succesvol misbruik kan onder meer leiden tot het uitvoeren van willekeurige code, privilege-escalatie, het uitlezen van bestanden en het omzeilen van beveiligingsmaatregelen.

Van de zeven kwetsbaarheden die als kritiek zijn aangemerkt, hebben zes een CVSS-score van 9,3 of hoger. De kwetsbaarheid met kenmerk CVE-2026-75682 heeft met een CVSS-score van 9,9 de hoogste score en betreft een SQL-injectiekwetsbaarheid waarmee een laaggeprivilegieerde kwaadwillende willekeurige code kan uitvoeren.

De kwetsbaarheden met kenmerk CVE-2026-75684, CVE-2026-75689 en CVE-2026-75697 betreffen opgeslagen XSS-kwetsbaarheden die kunnen leiden tot privilege-escalatie. CVE-2026-75686 betreft onvoldoende invoervalidatie en CVE-2026-75698 een reflected XSS-kwetsbaarheid en succesvol misbruik kan leiden tot het uitvoeren van willekeurige code. Voor deze vijf kwetsbaarheden is geen authenticatie vereist, maar wel gebruikersinteractie.

CVE-2026-34689 betreft een path-traversalkwetsbaarheid met een CVSS-score van 8,6 waarmee een niet-geauthenticeerde kwaadwillende zonder gebruikersinteractie bestanden kan uitlezen.

Adobe meldt niet op de hoogte te zijn van actief misbruik van de kwetsbaarheden.

Oplossingen

Adobe heeft beveiligingsupdates uitgebracht om de kwetsbaarheden te verhelpen. Gebruikers van Adobe Connect wordt geadviseerd te updaten naar versie 12.12. Voor de Adobe Connect Android Mobile App is versie 4.5 beschikbaar. Zie bijgevoegde referenties voor meer informatie.

Referenties

- https://helpx.adobe.com/security/products/connect/apsb26-150.html

Kwetsbaarheden

CVE	CVSS Score
CVE-2026-75682	9.9 CRITICAL
CVE-2026-75684	9.3 CRITICAL
CVE-2026-75686	9.3 CRITICAL
CVE-2026-75689	9.3 CRITICAL
CVE-2026-75697	9.3 CRITICAL
CVE-2026-75698	9.3 CRITICAL
CVE-2026-34689	8.6 HIGH
CVE-2026-83964	6.2 MEDIUM
CVE-2026-48361	6.1 MEDIUM

CWE's

CWE	Beschrijving
CWE-79	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')
CWE-22	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')
CWE-89	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')
CWE-295	Improper Certificate Validation

Getroffen producten

Adobe
Adobe Connect
Adobe Connect Android Mobile App

Disclaimer