



NCSC-2026-0390

Kwetsbaarheden verholpen in Adobe Experience Manager Forms JEE

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 6 kwetsbaarheden verholpen in Adobe Experience Manager (AEM) Forms op Java Enterprise Edition (JEE), waaronder AEM 6.5 Forms en AEM 6.5 LTS Forms.

Duiding

De kwetsbaarheden betreffen verschillende beveiligingsproblemen, waaronder onjuiste autorisatie, onvoldoende invoervalidatie, Server-Side Request Forgery (SSRF), Cross-Site Scripting (XSS) en Cross-Site Request Forgery (CSRF). Alle zes kwetsbaarheden zijn als kritiek aangemerkt en twee kunnen zonder authenticatie op afstand worden misbruikt. Succesvol misbruik kan onder meer leiden tot het uitvoeren van willekeurige code, privilege-escalatie en het omzeilen van beveiligingsmaatregelen.

CVE-2026-75745 heeft met een CVSS-score van 9,8 de hoogste score en kan zonder authenticatie en gebruikersinteractie op afstand worden misbruikt voor het uitvoeren van willekeurige code. Adobe meldt niet op de hoogte te zijn van actief misbruik.

Oplossingen

Adobe heeft beveiligingsupdates uitgebracht om de kwetsbaarheden te verhelpen. Zie bijgevoegde referenties voor meer informatie.

Referenties

➤ <https://helpx.adobe.com/security/products/aem-forms/apsb26-151.html>

Kwetsbaarheden

CVE	CVSS Score
➤ CVE-2026-75745	10.0 CRITICAL
➤ CVE-2026-81995	9.1 CRITICAL
➤ CVE-2026-82000	9.6 CRITICAL
➤ CVE-2026-81999	8.7 HIGH
➤ CVE-2026-75744	8.1 HIGH
➤ CVE-2026-75743	7.1 HIGH

CWE's

CWE	Beschrijving
> CWE-79	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')
> CWE-352	Cross-Site Request Forgery (CSRF)
> CWE-863	Incorrect Authorization
> CWE-918	Server-Side Request Forgery (SSRF)

Getroffen producten

Adobe
AEM 6.5 Forms
AEM 6.5 Forms JEE
AEM 6.5 LTS Forms
AEM 6.5 LTS Forms JEE

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.