Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

NCSC-2026-0363

Kwetsbaarheden verholpen in Adobe Experience Manager

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

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 meerdere kwetsbaarheden verholpen in Adobe Experience Manager.

Duiding

Adobe Experience Manager bevat meerdere Cross-Site Scripting (XSS) kwetsbaarheden, waaronder DOM-based en stored XSS. Deze kwetsbaarheden stellen een aanvaller in staat om kwaadaardige JavaScript-code te injecteren en uit te voeren binnen de browsers van gebruikers die een speciaal vervaardigde webpagina bezoeken of met deze pagina's interacteren. De stored XSS kwetsbaarheden ontstaan door onvoldoende input sanitatie en output encoding in formuliercomponenten, waardoor persistent scriptinvoeging mogelijk is. Daarnaast is er een Incorrect Authorization kwetsbaarheid die het mogelijk maakt voor aanvallers met lage privileges om arbitrary code uit te voeren zonder gebruikersinteractie, door onjuiste autorisatiecontroles binnen de applicatie. Ook is er een Improper Input Validation kwetsbaarheid die het mogelijk maakt om beveiligingsmaatregelen te omzeilen en beperkte schrijfrechten te verkrijgen via malafide URL's of webpagina's. Deze kwetsbaarheden kunnen leiden tot ongeautoriseerde acties binnen de context van de sessie van het slachtoffer.

Oplossingen

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

Referenties

- https://helpx.adobe.com/security/products/experience-manager/apsb26-98.html

Kwetsbaarheden

CVE	CVSS Score
CVE-2025-64542	5.4 MEDIUM
CVE-2025-64584	5.4 MEDIUM
CVE-2025-64588	5.4 MEDIUM
CVE-2025-64589	5.4 MEDIUM
CVE-2025-64610	5.4 MEDIUM

CVE-2025-64618	5.4 MEDIUM
CVE-2025-64830	5.4 MEDIUM
CVE-2025-64838	5.4 MEDIUM
CVE-2025-64854	5.4 MEDIUM
CVE-2025-64866	5.4 MEDIUM
CVE-2025-64868	5.4 MEDIUM
CVE-2026-19232	9.9 CRITICAL
CVE-2026-19479	5.4 MEDIUM
CVE-2026-19612	5.4 MEDIUM
CVE-2026-19644	5.4 MEDIUM
CVE-2026-19713	5.4 MEDIUM
CVE-2026-27222	5.5 MEDIUM
CVE-2026-27227	5.4 MEDIUM
CVE-2026-27238	7.8 HIGH
CVE-2026-27258	5.5 MEDIUM
CVE-2026-71356	5.4 MEDIUM
CVE-2026-71357	5.4 MEDIUM
CVE-2026-71388	5.4 MEDIUM
CVE-2026-71440	5.4 MEDIUM
CVE-2026-71565	5.4 MEDIUM
CVE-2026-72626	5.4 MEDIUM
CVE-2026-72627	5.4 MEDIUM
CVE-2026-75629	5.4 MEDIUM

CVE-2026-75635	5.4 MEDIUM
CVE-2026-75636	5.4 MEDIUM
CVE-2026-75637	5.4 MEDIUM
CVE-2026-75639	5.4 MEDIUM
CVE-2026-75640	5.4 MEDIUM
CVE-2026-75642	5.4 MEDIUM
CVE-2026-75643	5.4 MEDIUM
CVE-2026-75644	5.4 MEDIUM
CVE-2026-75646	5.4 MEDIUM
CVE-2026-75647	5.4 MEDIUM
CVE-2026-75651	5.4 MEDIUM
CVE-2026-75652	5.4 MEDIUM
CVE-2026-75657	5.4 MEDIUM
CVE-2026-75659	5.4 MEDIUM
CVE-2026-75660	5.4 MEDIUM
CVE-2026-75661	5.4 MEDIUM
CVE-2026-75666	5.4 MEDIUM
CVE-2026-75667	5.4 MEDIUM
CVE-2026-75668	5.4 MEDIUM
CVE-2026-75669	5.4 MEDIUM
CVE-2026-75670	5.4 MEDIUM
CVE-2026-75671	5.4 MEDIUM
CVE-2026-75672	5.4 MEDIUM

CVE-2026-75674	5.4 MEDIUM
CVE-2026-75675	5.4 MEDIUM
CVE-2026-75677	5.4 MEDIUM
CVE-2026-75678	5.4 MEDIUM
CVE-2026-75679	5.4 MEDIUM
CVE-2026-75680	5.4 MEDIUM
CVE-2026-75681	5.4 MEDIUM
CVE-2026-75683	5.4 MEDIUM
CVE-2026-75685	5.4 MEDIUM
CVE-2026-75687	5.4 MEDIUM
CVE-2026-75690	5.4 MEDIUM
CVE-2026-75691	5.4 MEDIUM
CVE-2026-75692	5.4 MEDIUM
CVE-2026-75693	5.4 MEDIUM
CVE-2026-75694	5.4 MEDIUM
CVE-2026-75695	5.4 MEDIUM
CVE-2026-75696	5.4 MEDIUM
CVE-2026-75700	5.4 MEDIUM
CVE-2026-75701	5.4 MEDIUM
CVE-2026-75702	5.4 MEDIUM
CVE-2026-75704	5.4 MEDIUM
CVE-2026-75705	5.4 MEDIUM
CVE-2026-75706	5.4 MEDIUM

CVE-2026-75707	5.4 MEDIUM
CVE-2026-75708	5.4 MEDIUM
CVE-2026-75709	5.4 MEDIUM
CVE-2026-75710	5.4 MEDIUM
CVE-2026-75711	5.4 MEDIUM
CVE-2026-75712	5.4 MEDIUM
CVE-2026-75713	5.4 MEDIUM
CVE-2026-75714	5.4 MEDIUM
CVE-2026-75715	5.4 MEDIUM
CVE-2026-75716	5.4 MEDIUM
CVE-2026-75717	5.4 MEDIUM
CVE-2026-75718	5.4 MEDIUM
CVE-2026-75719	5.4 MEDIUM
CVE-2026-75720	5.4 MEDIUM
CVE-2026-75722	5.4 MEDIUM
CVE-2026-75724	5.4 MEDIUM
CVE-2026-75725	5.4 MEDIUM
CVE-2026-75726	3.5 LOW
CVE-2026-75727	5.4 MEDIUM
CVE-2026-75729	5.4 MEDIUM
CVE-2026-75730	5.4 MEDIUM
CVE-2026-75731	5.4 MEDIUM
CVE-2026-75733	5.4 MEDIUM

CVE-2026-75734	**5.4 MEDIUM**
CVE-2026-75735	**5.4 MEDIUM**
CVE-2026-75736	**5.4 MEDIUM**
CVE-2026-75737	**5.4 MEDIUM**
CVE-2026-75738	**5.4 MEDIUM**
CVE-2026-75739	**5.4 MEDIUM**
CVE-2026-75740	**5.4 MEDIUM**
CVE-2026-75741	**5.4 MEDIUM**
CVE-2026-75742	**5.4 MEDIUM**
CVE-2026-79905	**5.4 MEDIUM**

CWE's

CWE	Beschrijving
CWE-79	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')
CWE-863	Incorrect Authorization

Getroffen producten

Adobe
AEM Cloud Service (CS)
Adobe Experience Manager 6.5
Adobe Experience Manager 6.5 LTS

Disclaimer