Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

Advisory NCSC-2026-0518

PRIORITEIT: NORMAAL

Kwetsbaarheden verholpen in Adobe Experience Manager

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 Experience Manager.

Duiding

De kwetsbaarheden betreffen verschillende vormen van Cross-Site Scripting (XSS), waaronder DOM-based, stored en reflected XSS. Hierbij kan een aanvaller kwaadaardige JavaScript-code uitvoeren binnen de browser van een slachtoffer, bijvoorbeeld door het bezoeken en interactie met speciaal vervaardigde webpagina's of het invullen van gemanipuleerde formuliervelden. Dit kan leiden tot ongeautoriseerde acties binnen de sessie van het slachtoffer.

Daarnaast zijn er kwetsbaarheden die betrekking hebben op incorrecte autorisatie, waardoor aanvallers met beperkte rechten beveiligingsmechanismen kunnen omzeilen en beperkte schrijfrechten verkrijgen zonder gebruikersinteractie. Verder is er een kwetsbaarheid in de template engine die het mogelijk maakt voor een aanvaller met hoge rechten om beveiligingsmechanismen te omzeilen en ongeautoriseerde lees- en schrijfrechten te verkrijgen zonder gebruikersinteractie. Ook is er een kwetsbaarheid in de controle van codegeneratiemechanismen, waardoor een aanvaller met beperkte rechten zonder gebruikersinteractie willekeurige code kan uitvoeren en zo de scope van zijn privileges kan wijzigen.

Oplossingen

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

Referenties

- https://www.adobe.com/trust/security/products/experience-manager/apsb26-104.html

Kwetsbaarheden

CVE	CVSS Score
CVE-2026-48401	5.4 MEDIUM
CVE-2026-48403	5.4 MEDIUM
CVE-2026-71355	5.4 MEDIUM
CVE-2026-75630	5.4 MEDIUM
CVE-2026-75641	5.4 MEDIUM
CVE-2026-75648	5.4 MEDIUM
CVE-2026-75653	5.4 MEDIUM
CVE-2026-75654	5.4 MEDIUM
CVE-2026-75662	5.4 MEDIUM
CVE-2026-75664	5.4 MEDIUM
CVE-2026-75673	5.4 MEDIUM
CVE-2026-75688	5.4 MEDIUM
CVE-2026-119018	5.4 MEDIUM
CVE-2026-119019	5.4 MEDIUM
CVE-2026-119021	5.4 MEDIUM
CVE-2026-119579	8.7 HIGH
CVE-2026-121357	8.7 HIGH
CVE-2026-121358	5.4 MEDIUM
CVE-2026-121359	5.4 MEDIUM
CVE-2026-121363	5.4 MEDIUM
CVE-2026-121364	5.4 MEDIUM
CVE-2026-121366	5.4 MEDIUM
CVE-2026-121914	5.4 MEDIUM
CVE-2026-121915	5.4 MEDIUM
CVE-2026-121916	6.1 MEDIUM
CVE-2026-121917	5.4 MEDIUM
CVE-2026-121918	5.4 MEDIUM
CVE-2026-121919	5.4 MEDIUM

CVE	CVSS Score
CVE-2026-121920	5.4 MEDIUM
CVE-2026-121921	5.4 MEDIUM
CVE-2026-121922	5.4 MEDIUM
CVE-2026-121924	5.4 MEDIUM
CVE-2026-122105	5.4 MEDIUM
CVE-2026-122346	5.4 MEDIUM
CVE-2026-122349	5.4 MEDIUM
CVE-2026-122352	5.4 MEDIUM
CVE-2026-122355	5.4 MEDIUM
CVE-2026-122358	5.4 MEDIUM
CVE-2026-122361	5.4 MEDIUM
CVE-2026-122364	5.4 MEDIUM
CVE-2026-122367	5.4 MEDIUM
CVE-2026-122368	5.4 MEDIUM
CVE-2026-122370	5.4 MEDIUM
CVE-2026-122385	5.4 MEDIUM
CVE-2026-122388	5.4 MEDIUM
CVE-2026-122393	5.4 MEDIUM
CVE-2026-122396	5.4 MEDIUM
CVE-2026-122398	5.4 MEDIUM
CVE-2026-122400	5.4 MEDIUM
CVE-2026-122405	5.4 MEDIUM
CVE-2026-122407	5.4 MEDIUM
CVE-2026-122421	5.4 MEDIUM
CVE-2026-122428	5.4 MEDIUM
CVE-2026-122443	5.4 MEDIUM
CVE-2026-122445	5.4 MEDIUM
CVE-2026-122447	5.4 MEDIUM
CVE-2026-122450	5.4 MEDIUM
CVE-2026-122455	5.4 MEDIUM
CVE-2026-122457	5.4 MEDIUM

CVE	CVSS Score
CVE-2026-122462	5.4 MEDIUM
CVE-2026-122463	5.4 MEDIUM
CVE-2026-122467	5.4 MEDIUM
CVE-2026-122472	5.4 MEDIUM
CVE-2026-122500	5.4 MEDIUM
CVE-2026-122502	5.4 MEDIUM
CVE-2026-123219	5.4 MEDIUM
CVE-2026-123220	5.4 MEDIUM
CVE-2026-123221	5.4 MEDIUM
CVE-2026-123222	5.4 MEDIUM
CVE-2026-123223	5.4 MEDIUM
CVE-2026-123224	5.4 MEDIUM
CVE-2026-123225	5.4 MEDIUM
CVE-2026-123226	5.4 MEDIUM
CVE-2026-123227	5.4 MEDIUM
CVE-2026-123228	5.4 MEDIUM
CVE-2026-123229	5.4 MEDIUM
CVE-2026-123230	5.4 MEDIUM
CVE-2026-123231	5.4 MEDIUM
CVE-2026-123233	5.4 MEDIUM
CVE-2026-123236	5.4 MEDIUM
CVE-2026-123237	5.4 MEDIUM
CVE-2026-123240	5.4 MEDIUM
CVE-2026-123241	5.4 MEDIUM
CVE-2026-123242	5.4 MEDIUM
CVE-2026-123243	5.4 MEDIUM
CVE-2026-123244	5.4 MEDIUM
CVE-2026-123245	4.4 MEDIUM
CVE-2026-123246	5.4 MEDIUM
CVE-2026-123248	5.4 MEDIUM
CVE-2026-123249	5.4 MEDIUM

CVE	CVSS Score
CVE-2026-123250	5.4 MEDIUM
CVE-2026-123251	5.4 MEDIUM
CVE-2026-123252	5.4 MEDIUM
CVE-2026-123253	8.7 HIGH
CVE-2026-123255	3.4 LOW
CVE-2026-123256	7.1 HIGH
CVE-2026-123264	5.4 MEDIUM
CVE-2026-123266	9.9 CRITICAL
CVE-2026-132877	9.9 CRITICAL

CWE's

CWE	Beschrijving
CWE-79	Improper Neutralization of Input During Web Page Generation
CWE-94	Improper Control of Generation of Code
CWE-863	Incorrect Authorization
CWE-1336	Improper Neutralization of Special Elements Used in a Template Engine

Getroffen producten

Adobe
Adobe Experience Manager 6.5
Adobe Experience Manager 6.5 LTS
Adobe Experience Manager as a Cloud Service

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.