Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

NCSC-2025-0241

Kwetsbaarheden verholpen in Adobe Experience Manager

NCSC Advisory
Prioriteit: Normaal
Gepubliceerd op: 17-10-2025
Revisie: 1.0.1

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

Update Revisie 1

CISA meldt via de KEV dat actief misbruik is waargenomen

Feiten

Adobe heeft kwetsbaarheden verholpen in Adobe Experience Manager (versies 6.5.23 en eerder).

Duiding

De kwetsbaarheden bevinden zich in de configuratie van Adobe Experience Manager, waardoor aanvallers in staat zijn om willekeurige code uit te voeren zonder enige interactie van de gebruiker. Dit kan leiden tot ongeautoriseerde toegang en controle over de getroffen systemen. Daarnaast is er een kwetsbaarheid gerapporteerd die te maken heeft met een onjuiste beperking van XML External Entity Reference (XXE), waardoor aanvallers bestanden van het lokale bestandssysteem kunnen lezen zonder gebruikersinteractie. Beide kwetsbaarheden vormen een ernstig risico voor de integriteit van gegevens en systemen.

Adobe geeft aan dat voor beide kwetsbaarheden PoC code publiek beschikbaar is.

Het Amerikaanse CISA heeft de kwetsbaarheid met kenmerk CVE-2025-54253 op de KEV-lijst geplaatst, wat aangeeft dat zij actief misbruik hebben waargenomen binnen de Amerikaanse federale overheid. Er worden verder geen details gegeven. Mede door de recente aandacht op diverse blogs voor deze kwetsbaarheid, wordt het aannemelijk dat de reeds langer beschikbare Proof-of-Concept-code kan leiden tot een verhoging in scan- en misbruikverkeer.

Het NCSC adviseert om de updates zo spoedig mogelijk in te zetten, indien dit nog niet is gebeurd.

Oplossingen

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

Referenties

- https://helpx.adobe.com/security/products/aem-forms/apsb25-82.html

Kwetsbaarheden

CVE	CVSS Score
CVE-2025-54253	10.0 CRITICAL
CVE-2025-54254	8.6 HIGH

CWE's

CWE	Beschrijving
CWE-16	CWE-16
CWE-611	Improper Restriction of XML External Entity Reference

Getroffen producten

Adobe
Adobe Experience Manager

Disclaimer