Nationaal Cyber Security Centrum
*Ministerie van Justitie en Veiligheid*

# NCSC-2026-0246

## Kwetsbaarheden verholpen in Adobe Experience Manager

NCSC Security Advisory
Prioriteit: Normaal
Gepubliceerd op: 17-07-2026

**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

De kwetsbaarheden in Adobe Experience Manager omvatten onder andere het ontbreken van authenticatie op een kritieke functie, waardoor onbevoegde schrijfacties mogelijk zijn zonder gebruikersinteractie. Daarnaast is er een Server-Side Request Forgery (SSRF) kwetsbaarheid die een aanvaller met lage privileges in staat stelt om willekeurige code op de server uit te voeren en toegang te verkrijgen tot accounts of sessies. Verder zijn er meerdere Cross-Site Scripting (XSS) kwetsbaarheden, zowel stored als DOM-based, die het mogelijk maken voor aanvallers om kwaadaardige JavaScript-code te injecteren en uit te voeren in de browsers van gebruikers, wat kan leiden tot het kapen van sessies en het uitvoeren van ongeautoriseerde acties. Ook is er een Path Traversal kwetsbaarheid die het mogelijk maakt om bestanden buiten de bedoelde directorystructuur te lezen zonder gebruikersinteractie. Daarnaast is er een XML External Entity (XXE) kwetsbaarheid die het uitvoeren van willekeurige code, toegang tot gevoelige bestanden en privilege-escalatie mogelijk maakt zonder gebruikersinteractie. Deze kwetsbaarheden beïnvloeden de vertrouwelijkheid, integriteit en beschikbaarheid van systemen waarop Adobe Experience Manager draait.

## 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/apsb26-74.html

## Kwetsbaarheden

| CVE | CVSS Score |
| --- | --- |
| CVE-2026-48252 | 8.6 HIGH |
| CVE-2026-48259 | 9.6 CRITICAL |
| CVE-2026-48263 | 5.4 MEDIUM |
| CVE-2026-48310 | 8.6 HIGH |

| | |
|---|---|
| CVE-2026-48355 | 5.4 MEDIUM |
| CVE-2026-48359 | 9.6 CRITICAL |
| CVE-2026-48253 | 5.4 MEDIUM |
| CVE-2026-48254 | 5.4 MEDIUM |
| CVE-2026-48255 | 5.4 MEDIUM |
| CVE-2026-48257 | 5.4 MEDIUM |
| CVE-2026-48260 | 5.4 MEDIUM |
| CVE-2026-48261 | 5.4 MEDIUM |
| CVE-2026-48262 | 5.4 MEDIUM |
| CVE-2023-25690 | 9.8 CRITICAL |
| CVE-2025-64538 | 9.3 CRITICAL |
| CVE-2025-64537 | 9.3 CRITICAL |
| CVE-2025-64539 | 9.3 CRITICAL |

## CWE's

| CWE | Beschrijving |
|---|---|
| CWE-22 | Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') |
| CWE-79 | Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') |
| CWE-113 | Improper Neutralization of CRLF Sequences in HTTP Headers ('HTTP Request/Response Splitting') |
| CWE-306 | Missing Authentication for Critical Function |
| CWE-444 | Inconsistent Interpretation of HTTP Requests ('HTTP Request/Response Smuggling') |
| CWE-611 | Improper Restriction of XML External Entity Reference |

| | |
|---|---|
| CWE-918 | Server-Side Request Forgery (SSRF) |

## Getroffen producten

| **Adobe** |
|---|
| Adobe Experience Manager (AEM) |
| Adobe Experience Manager 6.5 |
| Adobe Experience Manager 6.5 LTS |
| Adobe Experience Manager as a Cloud Service |

## Disclaimer