Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

NCSC-2026-0292

Kwetsbaarheden verholpen in Adobe Commerce

NCSC Security Advisory
Prioriteit: Normaal
Gepubliceerd op: 12-08-2026

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 Commerce.

Duiding

De kwetsbaarheden betreffen voornamelijk incorrecte autorisatie, waardoor een aanvaller met verschillende privilege-niveaus beveiligingscontroles kan omzeilen. Dit stelt de aanvaller in staat om zonder gebruikersinteractie ongeautoriseerde lees- en schrijfrechten te verkrijgen, toegang te krijgen tot gevoelige data, en privileges te escaleren binnen het systeem. Daarnaast is er een stored Cross-Site Scripting (XSS) kwetsbaarheid die het mogelijk maakt voor laaggeprivilegieerde aanvallers om kwaadaardige JavaScript-code in formulier velden te injecteren. Deze code wordt uitgevoerd in de browsers van slachtoffers, wat kan leiden tot ongeautoriseerde acties zoals sessiekaping en toegang tot gebruikersaccounts. De exploitatie van deze kwetsbaarheden kan leiden tot wijzigingen in de integriteit van het platform, ongeautoriseerde toegang tot bronnen en mogelijke verstoring van de beschikbaarheid.

Oplossingen

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

Referenties

- https://helpx.adobe.com/security/products/magento/apsb26-92.html

Kwetsbaarheden

CVE	CVSS Score
CVE-2026-48411	6.5 MEDIUM
CVE-2026-48412	2.7 LOW
CVE-2026-48413	8.7 HIGH
CVE-2026-48414	7.7 HIGH
CVE-2026-48415	7.6 HIGH
CVE-2026-48416	7.5 HIGH

CVE-2026-71362	9.1 CRITICAL

CWE's

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

Getroffen producten

Adobe
Commerce
Commerce B2B
Magento Open Source

Disclaimer