



NCSC-2026-0361

Kwetsbaarheden verholpen in Adobe Commerce

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 Commerce.

Duiding

De kwetsbaarheden betreffen onder andere stored Cross-Site Scripting (XSS) waarbij aanvallers kwaadaardige JavaScript-code kunnen injecteren in formulier velden binnen de applicatie. Deze code wordt uitgevoerd in de context van de browser van het slachtoffer en kan ongeautoriseerde acties uitvoeren, zoals het kapen van sessies of het escaleren van privileges. Daarnaast zijn er meerdere incorrecte autorisatieproblemen geïdentificeerd die het mogelijk maken voor aanvallers om hun privileges binnen het systeem te verhogen, ongeautoriseerde toegang te verkrijgen tot gevoelige informatie, en beveiligingscontroles te omzeilen zonder dat gebruikersinteractie nodig is. Verder is er een path traversal kwetsbaarheid die aanvallers met hoge privileges in staat stelt om beveiligingsmechanismen te omzeilen en toegang te krijgen tot bestanden of mappen buiten de bedoelde scope. Sommige van deze kwetsbaarheden kunnen leiden tot beperkte verstoring van de beschikbaarheid van diensten. Alle genoemde kwetsbaarheden zijn specifiek voor Adobe Commerce en kunnen door kwaadwillenden op afstand worden misbruikt.

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/apsb26-138.html>

Kwetsbaarheden

CVE	CVSS Score
➤ CVE-2026-76200	9.3 CRITICAL
➤ CVE-2026-76201	9.3 CRITICAL
➤ CVE-2026-76202	8.2 HIGH
➤ CVE-2026-77108	7.5 HIGH
➤ CVE-2026-77109	8.6 HIGH

> CVE-2026-77110	7.6 HIGH
> CVE-2026-77111	8.7 HIGH
> CVE-2026-77774	8.6 HIGH

CWE's

CWE	Beschrijving
> CWE-863	Incorrect Authorization
> 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')

Getroffen producten

Adobe
Commerce
Commerce B2B
Magento Open Source

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 or 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.