



NCSC-2025-0259

Kwetsbaarheden verholpen in Adobe Commerce en Magento

NCSC Advisory

Prioriteit: Normaal

Gepubliceerd op: 13-08-2025

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 kwetsbaarheden verholpen in Adobe Commerce en Magento (Versies 2.4.9-alpha1 en eerder).

Duiding

De kwetsbaarheden bevinden zich in de manier waarop Adobe Commerce omgaat met beveiligingsmaatregelen. Aanvallers met verhoogde rechten kunnen misbruik maken van een opgeslagen Cross-Site Scripting (XSS) kwetsbaarheid door kwaadaardige scripts in formulier velden te injecteren, wat kan leiden tot de uitvoering van schadelijke JavaScript in de browsers van gebruikers. Daarnaast zijn er kwetsbaarheden die het mogelijk maken voor aanvallers om beveiligingsmaatregelen te omzeilen, waardoor ongeautoriseerde toegang tot gevoelige delen van de applicatie mogelijk is zonder enige gebruikersinteractie. Dit kan leiden tot ongeautoriseerde wijzigingen en toegang tot gevoelige informatie.

Oplossingen

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

Referenties

➤ <https://helpx.adobe.com/security/products/magento/apsb25-71.html>

Kwetsbaarheden

CVE	CVSS Score
➤ CVE-2025-49554	7.5 HIGH
➤ CVE-2025-49555	8.1 HIGH
➤ CVE-2025-49556	7.5 HIGH
➤ CVE-2025-49557	8.7 HIGH
➤ CVE-2025-49558	5.9 MEDIUM
➤ CVE-2025-49559	5.3 MEDIUM

CWE's

CWE	Beschrijving
> CWE-367	Time-of-check Time-of-use (TOCTOU) Race Condition
> CWE-352	Cross-Site Request Forgery (CSRF)
> CWE-863	Incorrect Authorization
> CWE-22	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')
> CWE-20	Improper Input Validation
> CWE-79	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')

Getroffen producten

Adobe
Commerce
Magento
Adobe Commerce

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.