



NCSC-2025-0054

Kwetsbaarheden verholpen in Adobe Commerce en Magento

NCSC Advisory

Prioriteit: Normaal

Gepubliceerd op: 13-02-2025

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.

Duiding

De kwetsbaarheden omvatten onder andere een Path Traversal, ongeautoriseerde acties, informatie-expositie, onjuiste autorisatie, en verschillende opgeslagen XSS-kwetsbaarheden. Deze kwetsbaarheden stellen aanvallers in staat om ongeautoriseerde toegang te verkrijgen, gevoelige informatie te onthullen, en schadelijke scripts in te voegen, wat kan leiden tot sessieovername en ernstige risico's voor de vertrouwelijkheid en integriteit van de systemen. De meeste kwetsbaarheden vereisen geen gebruikersinteractie en een aantal vereisen geen voorafgaande gebruikersrechten.

Oplossingen

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

Referenties

➤ <https://helpx.adobe.com/security/products/magento/apsb25-08.html>

Kwetsbaarheden

CVE	CVSS Score
➤ CVE-2025-24406	7.5 HIGH
➤ CVE-2025-24407	7.1 HIGH
➤ CVE-2025-24408	8.1 HIGH
➤ CVE-2025-24409	8.2 HIGH
➤ CVE-2025-24410	5.1 MEDIUM
➤ CVE-2025-24411	8.8 HIGH
➤ CVE-2025-24412	5.1 MEDIUM
➤ CVE-2025-24413	5.1 MEDIUM

> CVE-2025-24414	5.1 MEDIUM
> CVE-2025-24415	5.1 MEDIUM
> CVE-2025-24416	5.1 MEDIUM
> CVE-2025-24417	5.1 MEDIUM
> CVE-2025-24418	8.1 HIGH
> CVE-2025-24419	4.3 MEDIUM
> CVE-2025-24420	4.3 MEDIUM
> CVE-2025-24421	4.3 MEDIUM
> CVE-2025-24422	6.5 MEDIUM
> CVE-2025-24423	4.3 MEDIUM
> CVE-2025-24424	6.5 MEDIUM
> CVE-2025-24425	5.3 MEDIUM
> CVE-2025-24426	6.5 MEDIUM
> CVE-2025-24427	6.5 MEDIUM
> CVE-2025-24428	5.1 MEDIUM
> CVE-2025-24429	3.5 LOW
> CVE-2025-24430	3.7 LOW
> CVE-2025-24432	3.7 LOW
> CVE-2025-24434	9.4 CRITICAL
> CVE-2025-24435	4.3 MEDIUM
> CVE-2025-24436	4.3 MEDIUM
> CVE-2025-24437	5.4 MEDIUM
> CVE-2025-24438	5.1 MEDIUM

CWE's

CWE	Beschrijving
> CWE-657	Violation of Secure Design Principles
> CWE-840	CWE-840
> CWE-367	Time-of-check Time-of-use (TOCTOU) Race Condition
> CWE-285	Improper Authorization
> CWE-284	Improper Access Control
> CWE-863	Incorrect Authorization
> CWE-22	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')
> CWE-200	Exposure of Sensitive Information to an Unauthorized Actor
> CWE-79	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')

Getroffen producten

adobe
adobe_commerce_b2b
adobe_commerce
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 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.