



# NCSC-2026-0152

## Kwetsbaarheden verholpen in Adobe Commerce

NCSC Advisory

Prioriteit: Normaal

Gepubliceerd op: 13-05-2026

### **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](http://www.first.org/tlp)).

Ontvangers van TLP:WHITE mogen de informatie publiek verspreiden.

Uw reacties zijn welkom op [info@ncsc.nl](mailto:info@ncsc.nl)

## Feiten

Adobe heeft meerdere kwetsbaarheden verholpen in Adobe Commerce.

## Duiding

De kwetsbaarheden bevinden zich in verschillende versies van Adobe Commerce, waaronder 2.4.9-beta1 en eerdere versies. Een Incorrect Authorization kwetsbaarheid maakt het mogelijk voor aanvallers om autorisatiecontroles te omzeilen en ongeautoriseerde schrijfrechten te verkrijgen zonder gebruikersinteractie. Daarnaast is er een Server-Side Request Forgery (SSRF) kwetsbaarheid die aanvallers in staat stelt beveiligingsmaatregelen te omzeilen en ongeautoriseerde leesrechten te verkrijgen door het serververzoek te manipuleren, waarvoor wel gebruikersinteractie via een kwaadaardige URL of webpagina nodig is. Verder is er een Uncontrolled Resource Consumption kwetsbaarheid die zonder gebruikersinteractie kan worden misbruikt om systeembronnen uit te putten, wat resulteert in een denial-of-service situatie die de beschikbaarheid van het Adobe Commerce platform beïnvloedt.

## 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/apsb26-49.html>

## Kwetsbaarheden

CVE	CVSS Score
➤ <a href="#">CVE-2026-34645</a>	7.5 HIGH
➤ <a href="#">CVE-2026-34646</a>	7.5 HIGH
➤ <a href="#">CVE-2026-34647</a>	7.4 HIGH
➤ <a href="#">CVE-2026-34648</a>	7.5 HIGH
➤ <a href="#">CVE-2026-34649</a>	7.5 HIGH
➤ <a href="#">CVE-2026-34650</a>	7.5 HIGH

## CWE's

CWE	Beschrijving
> <a href="#">CWE-400</a>	Uncontrolled Resource Consumption
> <a href="#">CWE-863</a>	Incorrect Authorization
> <a href="#">CWE-918</a>	Server-Side Request Forgery (SSRF)

## Getroffen producten

<b>Adobe</b>
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 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.