



## Advisory NCSC-2026-0436

PRIORITEIT: NORMAAL

# Kwetsbaarheden verholpen in Adobe Commerce

Publicatiedatum: 16-10-2026

Toegestane verspreiding: TLP:WHITE  
(Traffic Light Protocol)

Deze publicatie bevat het label TLP:WHITE en wordt door het Nationaal Cyber Security Center (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.

Reacties zijn welkom op [info@ncsc.nl](mailto: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 formulievelden 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 kwetsbaarheden in de template engine van Adobe Commerce die leiden tot improper neutralization van speciale elementen, waardoor een aanvaller zonder gebruikersinteractie willekeurige code kan uitvoeren.

Verder zijn er problemen met incorrecte autorisatie die het mogelijk maken voor aanvallers met minimale privileges om beveiligingsmaatregelen te omzeilen, ongeautoriseerde lees- en schrijfbewerkingen uit te voeren, en in sommige gevallen ook remote code execution te realiseren.

Ook zijn er kwetsbaarheden in de inputvalidatie die het mogelijk maken voor aanvallers met verschillende privilege-niveaus om beveiligingscontroles te omzeilen en ongeautoriseerde acties uit te voeren.

## Oplossingen

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

## Referenties

- <https://www.adobe.com/trust/security/products/commerce/apsb26-153.html>

## Kwetsbaarheden

| CVE             | CVSS Score    |
|-----------------|---------------|
| CVE-2026-100133 | 9.3 CRITICAL  |
| CVE-2026-103849 | 10.0 CRITICAL |
| CVE-2026-75650  | 10.0 CRITICAL |
| CVE-2026-91013  | 9.3 CRITICAL  |
| CVE-2026-92464  | 9.1 CRITICAL  |
| CVE-2026-92908  | 8.3 HIGH      |
| CVE-2026-92909  | 9.8 CRITICAL  |
| CVE-2026-92910  | 7.2 HIGH      |
| CVE-2026-92911  | 8.7 HIGH      |
| CVE-2026-92922  | 8.1 HIGH      |
| CVE-2026-95630  | 4.3 MEDIUM    |
| CVE-2026-95631  | 8.7 HIGH      |

## CWE's

| CWE      | Beschrijving                                                                         |
|----------|--------------------------------------------------------------------------------------|
| CWE-79   | Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') |
| CWE-863  | Incorrect Authorization                                                              |
| CWE-1336 | Improper Neutralization of Special Elements Used in a Template Engine                |

## Getroffen producten

|                     |
|---------------------|
| Adobe               |
| Commerce            |
| Commerce B2B        |
| Magento             |
| 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.