Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

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