ROYAUME DU MAROC
ADMINISTRATION
DE LA DEFENSE NATIONALE
Direction Générale de la Sécurité des Systèmes d'Information

المملكة المغربية
إدارة الدفاع الوطني
المديرية العامة لأمن نظم المعلومات

BULLETIN DE SECURITE

Titre	Exploitation active d'une vulnérabilité critique dans Magento (CVE-2025-54236 « SessionReaper »)
Numéro de Référence	60543001/26
Date de Publication	30 Janvier 2026
Risque	Critique
Impact	Critique

Systèmes affectés

- Adobe Commerce 2.4.9-alpha2 et versions antérieures
- Adobe Commerce 2.4.8-p2 et versions antérieures
- Adobe Commerce 2.4.7-p7 et versions antérieures
- Adobe Commerce 2.4.6-p12 et versions antérieures
- Adobe Commerce 2.4.5-p14 et versions antérieures
- Adobe Commerce 2.4.4-p15 et versions antérieures
- Adobe Commerce B2B 1.5.3-alpha2 et versions antérieures
- Adobe Commerce B2B 1.5.2-p2 et versions antérieures
- Adobe Commerce B2B 1.4.2-p7 et versions antérieures
- Adobe Commerce B2B 1.3.4-p14 et versions antérieures
- Adobe Commerce B2B 1.3.3-p15 et versions antérieures
- Magento Open Source 2.4.9-alpha2 et versions antérieures
- Magento Open Source 2.4.8-p2 et versions antérieures
- Magento Open Source 2.4.7-p7 et versions antérieures
- Magento Open Source 2.4.6-p12 et versions antérieures
- Magento Open Source 2.4.5-p14 et versions antérieures

Identificateurs externes

- CVE-2025-54236 ;

Direction Générale de la Sécurité des Systèmes d'Information,
Centre de Veille de Détection et de Réaction aux Attaques Informatiques, Méchouar Saïd,
B.P. 1048 Rabat – Tél : 05 37 57 21 47 – Fax : 05 37 57 20 53
Email : contact@macert.gov.ma

المديرية العامة لأمن نظم المعلومات ,مديرية تدبير مركز اليقظة والرصد والتصدي للهجمات المعلوماتية ، المشور السعيد، ص.ب. 1048 الرباط
هاتف: 47 21 57 37 05 – فاكس: 53 20 57 37 05
البريد الإلكتروني contact@macert.gov.ma

Bilan de la vulnérabilité

Une campagne d'exploitation massive est actuellement en cours, ciblant la vulnérabilité critique CVE-2025-54236 (SessionReaper) affectant les plateformes e-commerce Magento et Adobe Commerce. Cette vulnérabilité, faisant l'objet du bulletin de sécurité maCERT n°56701009/25, permet une exécution de code à distance (RCE) et est activement exploitée à grande échelle après identification via des scanners automatisés. Son exploitation conduit notamment à la compromission de comptes administrateurs, au déploiement de web shells, à l'exfiltration de données sensibles ainsi qu'au maintien d'un accès persistant aux serveurs affectés.

Solution

- Appliquer immédiatement les correctifs disponibles fournis par Adobe pour corriger la vulnérabilité CVE-2025-54236.
- Vérifier si l'instance Magento est exposée ou compromise :
    - Examiner les journaux d'accès pour comportements suspects.
    - Rechercher la présence de fichiers inconnus (web shells).
    - Auditer les comptes utilisateurs pour accès non autorisés.
- Changer les identifiants d'administration et les clés API après remédiation.
- Restaurer les systèmes à partir de sauvegardes sûres si une compromission est confirmée.
- Limiter l'accès des services d'administration (IP whitelisting, VPN, MFA, etc.).

Risque

- Exécution du code arbitraire à distance ;

Référence

Bulletin de sécurité maCERT/DGSSI du 10 Septembre 2025**:**

- https://www.dgssi.gov.ma/fr/bulletins/vulnerabilites-affectant-plusieurs-produits-dadobe-22

Bulletin de sécurité Adobe du 14 Janvier 2026**:**

- https://experienceleague.adobe.com/en/docs/experience-cloud-kcs/kbarticles/ka-27397#

Direction Générale de la Sécurité des Systèmes d'Information,
Centre de Veille de Détection et de Réaction aux Attaques Informatiques, Méchouar Saïd,
B.P. 1048 Rabat – Tél : 05 37 57 21 47 – Fax : 05 37 57 20 53
Email : contact@macert.gov.ma

المديرية العامة لأمن نظم المعلومات, مديرية تدبير مركز اليقظة والرصد والتصدي للهجمات المعلوماتية ، المشور السعيد، ص.ب. 1048 الرباط
هاتف: 05 37 57 21 47 – فاكس: 05 37 57 20 53
البريد الإلكتروني contact@macert.gov.ma