ROYAUME DU MAROC
ADMINISTRATION
DE LA DEFENSE NATIONALE
Direction Générale de la Sécurité des Systèmes d'Information
Centre de Veille de Détection et de Réaction aux Attaques Informatiques

المملكة المغربية
إدارة الدفاع الوطني
المديرية العامة لأمن نظم المعلومات
مركز اليقظة والرصد والتصدي للهجمات المعلوماتية

BULLETIN DE SECURITE

Titre	Vulnérabilités affectant plusieurs produits d'Adobe
Numéro de Référence	61791103/26
Date de Publication	11 mars 2026
Risque	Important
Impact	Important

Systèmes affectés

- Adobe Commerce 2.4.9-alpha3 et versions antérieures
- Adobe Commerce 2.4.8-p3 et versions antérieures
- Adobe Commerce 2.4.7-p8 et versions antérieures
- Adobe Commerce 2.4.6-p13 et versions antérieures
- Adobe Commerce 2.4.5-p15 et versions antérieures
- Adobe Commerce 2.4.4-p16 et versions antérieures
- Adobe Commerce B2B 1.5.3-alpha3 et versions antérieures
- Adobe Commerce B2B 1.5.2-p3 et versions antérieures
- Adobe Commerce B2B 1.4.2-p8 et versions antérieures
- Adobe Commerce B2B 1.3.5-p13 et versions antérieures
- Adobe Commerce B2B 1.3.4-p15 et versions antérieures
- Adobe Commerce B2B 1.3.3-p16 et versions antérieures
- Magento Open Source 2.4.9-alpha3
- Magento Open Source 2.4.8-p3 et versions antérieures
- Magento Open Source 2.4.7-p8 et versions antérieures
- Magento Open Source 2.4.6-p13 et versions antérieures
- Magento Open Source 2.4.5-p15 et versions antérieures
- Illustrator 2025 29.8.4 et versions antérieures
- Illustrator 2026 30.1 et versions antérieures
- Adobe Substance 3D Painter 11.1.2 et versions antérieures
- Acrobat DC 25.001.21265 et versions antérieures
- Acrobat Reader DC 25.001.21265 et versions antérieures
- Acrobat 2024 Win - 24.001.30307 et versions antérieures
- Acrobat 2024 Mac - 24.001.30308 et versions antérieures

- Adobe Premiere Pro 25.5 et versions antérieures
- Adobe Experience Manager (AEM) AEM Cloud Service (CS)
- Adobe Experience Manager (AEM) 6.5 LTS SP1 et versions antérieures
- Adobe Experience Manager (AEM) 6.5.SP23 et versions antérieures
- Adobe Substance 3D Stager 3.1.7 et versions antérieures
- Adobe DNG Software Development Kit (SDK) DNG SDK 1.7.1 build 2471 et versions antérieures

Identificateurs externes

CVE-2026-21282 CVE-2026-21284 CVE-2026-21285 CVE-2026-21286 CVE-2026-21289
CVE-2026-21290 CVE-2026-21291 CVE-2026-21292 CVE-2026-21293 CVE-2026-21294
CVE-2026-21295 CVE-2026-21296 CVE-2026-21297 CVE-2026-21309 CVE-2026-21310
CVE-2026-21311 CVE-2026-21333 CVE-2026-21359 CVE-2026-21360 CVE-2026-21361
CVE-2026-21362 CVE-2026-27220 CVE-2026-27221 CVE-2026-27223 CVE-2026-27224
CVE-2026-27225 CVE-2026-27226 CVE-2026-27228 CVE-2026-27229 CVE-2026-27230
CVE-2026-27231 CVE-2026-27232 CVE-2026-27233 CVE-2026-27234 CVE-2026-27235
CVE-2026-27236 CVE-2026-27237 CVE-2026-27239 CVE-2026-27240 CVE-2026-27241
CVE-2026-27242 CVE-2026-27244 CVE-2026-27247 CVE-2026-27248 CVE-2026-27249
CVE-2026-27250 CVE-2026-27251 CVE-2026-27252 CVE-2026-27253 CVE-2026-27254
CVE-2026-27255 CVE-2026-27256 CVE-2026-27257 CVE-2026-27259 CVE-2026-27260
CVE-2026-27261 CVE-2026-27262 CVE-2026-27263 CVE-2026-27264 CVE-2026-27265
CVE-2026-27266 CVE-2026-27267 CVE-2026-27268 CVE-2026-27269 CVE-2026-27270
CVE-2026-27271 CVE-2026-27272 CVE-2026-27278

Bilan de la vulnérabilité

Adobe a publié des mises à jour de sécurité qui permettent de corriger plusieurs vulnérabilités affectant ses produits susmentionnés. L'exploitation de ces vulnérabilités peut permettre à un attaquant d'exécuter du code à distance, d'accéder à des données confidentielles, d'élever ses privilèges, de contourner des mesures de sécurité, d'injecter du contenu dans une page ou de causer un déni de service.

Solution

Veuillez se référer aux bulletins de sécurité d'Adobe pour l'obtention des correctifs.

Risques

- Exécution de code à distance
- Accès à des informations confidentielles

- Elévation de privilèges
- Injection de contenu dans une page
- Déni de service

Références

Bulletins de sécurité d'Adobe:

- https://helpx.adobe.com/security/products/magento/apsb26-05.html
- https://helpx.adobe.com/security/products/illustrator/apsb26-18.html
- https://helpx.adobe.com/security/products/substance3d_painter/apsb26-25.html
- https://helpx.adobe.com/security/products/acrobat/apsb26-26.html
- https://helpx.adobe.com/security/products/premiere_pro/apsb26-28.html
- https://helpx.adobe.com/security/products/experience-manager/apsb26-24.html
- https://helpx.adobe.com/security/products/substance3d_stager/apsb26-29.html
- https://helpx.adobe.com/security/products/dng-sdk/apsb26-30.html

Direction Générale de la Sécurité des Systèmes d'Information,
Centre de Veille de Détection et de Réaction aux Attaques Informatiques
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
هاتف: 47 21 57 37 05 – فاكس: 53 20 57 37 05
البريد الإلكتروني contact@macert.gov.ma