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	50000910/24
Date de Publication	09 Octobre 2024
Risque	Important
Impact	Critique

Systèmes affectés

- Adobe Substance 3D Printer versions antérieures à 10.0.1
- Adobe Substance 3D Stager versions antérieures à 3.0.4
- Adobe Commerce version 2.4.7-x antérieures à 2.4.7-p3
- Adobe Commerce version 2.4.6-x antérieures à 2.4.6-p8
- Adobe Commerce version 2.4.5-x antérieures à 2.4.5-p10
- Adobe Commerce version 2.4.4-x antérieures à 2.4.4-p11
- Adobe Commerce B2B version 1.4.2-x antérieures à 1.4.2-p3
- Adobe Commerce B2B version 1.3.5-x antérieures à 1.3.5-p8
- Adobe Commerce B2B version 1.3.4-x antérieures à 1.3.4-p10
- Adobe Commerce B2B version 1.3.3-x antérieures à 1.3.3-p11
- Magento Open Source versions 2.4.7-x antérieures à 2.4.7-p3
- Magento Open Source versions 2.4.6-x antérieures à 2.4.6-p8
- Magento Open Source versions 2.4.5-x antérieures à 2.4.5-p10
- Magento Open Source versions 2.4.4-x antérieures à 2.4.4-p11
- Adobe Lightroom versions antérieures à 7.5
- Adobe Lightroom Classic versions antérieures à 13.5.1
- Adobe Lightroom Classic (LTS) versions antérieures à 12.5.2(LTS)
- Adobe Dimension versions antérieures à 4.0.4
- Adobe Animate 2023 versions antérieures à 23.0.8
- Adobe Animate 2024 versions antérieures à 24.0.5
- Adobe InCopy versions antérieures à 19.5
- Adobe InCopy versions antérieures à 18.5.4
- Adobe InDesign versions antérieures à 19.4
- Adobe InDesign versions antérieures à 18.5.3

- Adobe FrameMaker versions antérieures à 2020 update 7
- Adobe FrameMaker versions antérieures à 2022 update 5

Identificateurs externes

CVE-2024-20787	CVE-2024-45115	CVE-2024-45116	CVE-2024-45117
CVE-2024-45118	CVE-2024-45119	CVE-2024-45120	CVE-2024-45121
CVE-2024-45122	CVE-2024-45123	CVE-2024-45124	CVE-2024-45125
CVE-2024-45127	CVE-2024-45128	CVE-2024-45129	CVE-2024-45130
CVE-2024-45131	CVE-2024-45132	CVE-2024-45133	CVE-2024-45134
CVE-2024-45135	CVE-2024-45148	CVE-2024-45149	CVE-2024-45146
CVE-2024-45150	CVE-2024-47410	CVE-2024-47411	CVE-2024-47412
CVE-2024-47413	CVE-2024-47414	CVE-2024-47415	CVE-2024-47416
CVE-2024-47417	CVE-2024-47418	CVE-2024-47419	CVE-2024-47420
CVE-2024-45138	CVE-2024-45139	CVE-2024-45140	CVE-2024-45141
CVE-2024-45142	CVE-2024-45143	CVE-2024-45144	CVE-2024-45152
CVE-2024-45136	CVE-2024-45145	CVE-2024-45137	CVE-2024-47421
CVE-2024-47422	CVE-2024-47423	CVE-2024-47424	CVE-2024-47425

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 arbitraire, d'accéder à des informations confidentielles, d'élever ses privilèges ou de contourner les mesures de sécurité

Solution

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

Risques

- Exécution de code arbitraire
- Accès à des informations confidentielles
- Elévation de privilèges
- Contournement de mesures de sécurité

Références

Bulletins de sécurité d'Adobe:

- https://helpx.adobe.com/security/products/substance3d_painter/apsb24-52.html
- https://helpx.adobe.com/security/products/magento/apsb24-73.html
- https://helpx.adobe.com/security/products/dimension/apsb24-74.html
- https://helpx.adobe.com/security/products/animate/apsb24-76.html
- https://helpx.adobe.com/security/products/lightroom/apsb24-78.html
- https://helpx.adobe.com/security/products/incopy/apsb24-79.html
- https://helpx.adobe.com/security/products/indesign/apsb24-80.html
- https://helpx.adobe.com/security/products/substance3d_stager/apsb24-81.html
- https://helpx.adobe.com/security/products/framemaker/apsb24-82.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: 05 37 57 21 47 – فاكس: 05 37 57 20 53
البريد الإلكتروني contact@macert.gov.ma