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	45971402/24
Date de Publication	14 Février 2024
Risque	Important
Impact	Critique

Systèmes affectés

- Adobe Experience Manager Cloud Service versions antérieures à 2023.4
- Adobe Experience Manager Cloud Service versions antérieures à 6.5.17.0
- Adobe Commerce versions 2.4.6 antérieures à 2.4.6-p4
- Adobe Commerce versions 2.4.5 antérieures à 2.4.5-p6
- Adobe Commerce versions 2.4.4 antérieures à 2.4.4-p7
- 5Adobe Commerce versions 2.4.3 antérieures à 2.4.3-ext-6
- Adobe Commerce versions 2.4.1 antérieures à 2.4.2-ext-6
- Adobe Commerce versions 2.4.6 antérieures à 2.4.1-ext-6
- Adobe Commerce versions 2.4.0 antérieures à 2.4.0-ext-5
- Adobe Commerce versions 2.3.7-p4 antérieures à 2.3.7-p4-ext-6
- Magento Open Source versions 2.4.6 antérieures à 2.4.6-p4
- Magento Open Source versions 2.4.5 antérieures à 2.4.5-p6
- Magento Open Source versions 2.4.4 antérieures à 2.4.4-p
- Adobe Substance 3D Painter versions antérieures à 9.1.2 sur Windows et macOS
- Adobe Substance 3D Designer versions antérieures à 13.10 sur Windows et macOS
- Acrobat DC versions antérieures à 23.008.20533
- Acrobat Reader DC versions antérieures à 23.008.20533
- Acrobat 2020 versions antérieures à 20.005.30574
- Acrobat Reader 2020 versions antérieures à 20.005.30574
- Adobe FrameMaker Publishing Server versions antérieures à 2022.2
- Adobe Audition versions antérieures à 24.2
- Adobe Audition versions antérieures à 23.6.4

Identificateurs externes

CVE-2024-20719, CVE-2024-20720, CVE-2024-20716, CVE-2024-20717, CVE-2024-20718 CVE-2024-20722, CVE-2024-20723, CVE-2024-20724, CVE-2024-20725 VE-2024-20740, CVE-2024-20741, CVE-2024-20742, CVE-2024-20743, CVE-2024-20744, CVE-2024-20729, CVE-2024-20730, CVE-2024-20731, CVE-2024-20735, CVE-2024-20747, CVE-2024-20748, CVE-2024-20749, CVE-2024-20728, CVE-2024-20734, CVE-2024-20736, CVE-2024-20733, CVE-2024-20738, CVE-2024-20739, CVE-2024-20750

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, de contourner des mesures de sécurité 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 arbitraire
- Accès à des informations confidentielles
- Contournement de mesures de sécurité
- Déni de service

Références

Bulletins de sécurité d'Adobe:

- https://helpx.adobe.com/security/products/magento/apsb24-03.html
- https://helpx.adobe.com/security/products/substance3d_painter/apsb24-04.html
- https://helpx.adobe.com/security/products/acrobat/apsb24-07.html
- https://helpx.adobe.com/security/products/framemaker-publishing-server/apsb24-10.html
- https://helpx.adobe.com/security/products/audition/apsb24-11.html
- https://helpx.adobe.com/security/products/substance3d_designer/apsb24-13.html