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	47811206/24
Date de Publication	12 Juin 2024
Risque	Important
Impact	Critique

Systèmes affectés

- Acrobat Android versions antérieures à 24.5.0.33694
- Creative Cloud Desktop Application, versions antérieures à 6.2.0.554
- Adobe Substance 3D Stager versions antérieures à 3.0.2
- ColdFusion 2023 versions antérieures à Update 8
- ColdFusion 2021 versions antérieures à Update 14
- Adobe Media Encoder versions antérieures à 24.4.1
- Adobe Media Encoder versions antérieures à 23.6.6
- Adobe Audition versions antérieures à 24.4.1
- Adobe Audition versions antérieures à 23.6.6
- Adobe Commerce version 2.4.7-x antérieures à 2.4.7-p1
- Adobe Commerce version 2.4.6-x antérieures à 2.4.6-p6
- Adobe Commerce version 2.4.5-x antérieures à 2.4.5-p8
- Adobe Commerce version 2.4.4-x antérieures à 2.4.4-p9
- Adobe Commerce version 2.4.3-ext-x antérieures à 2.4.3-ext-8
- Adobe Commerce version 2.4.2-ext-x antérieures à 2.4.2-ext-8
- Adobe Commerce version 2.4.1-ext-x antérieures à 2.4.1-ext-8
- Adobe Commerce version 2.4.0-ext-x antérieures à 2.4.0-ext-8
- Adobe Commerce version 2.3.7-p4-ext-x antérieures à 2.3.7-p4-ext-8
- Magento Open Source versions 2.4.7-x antérieures à 2.4.7-p1
- Magento Open Source versions 2.4.6-x antérieures à 2.4.6-p6
- Magento Open Source versions 2.4.5-x antérieures à 2.4.5-p8
- Magento Open Source versions 2.4.4-x antérieures à 2.4.4-p9
- Adobe FrameMaker Publishing Server versions antérieures à Version 2022.3

- Photoshop 2023 versions antérieures à 24.7.7
- Photoshop 2024 versions antérieures à 25.9
- Adobe Experience Manager (AEM) versions antérieures à AEM Cloud Service Release 2024.5
- Adobe Experience Manager (AEM) versions antérieures à 6.5.21

Identificateurs externes

CVE-2024-34129, CVE-2024-34130, CVE-2024-34116, CVE-2024-34115, CVE-2024-34102
CVE-2024-34108, CVE-2024-34109, CVE-2024-34110, CVE-2024-34104, CVE-2024-34107, CVE-2024-34103, CVE-2024-34105, CVE-2024-34111, CVE-2024-34106, CVE-2024-30299, CVE-2024-30300, CVE-2024-30278, CVE-2024-30276, CVE-2024-30285
CVE-2024-20753, CVE-2024-26036, CVE-2024-26037, CVE-2024-26039, CVE-2024-26053, CVE-2024-26057, CVE-2024-26058, CVE-2024-26072, CVE-2024-26074, CVE-2024-26075, CVE-2024-26077, CVE-2024-26078, CVE-2024-26081, CVE-2024-26082, CVE-2024-26083, CVE-2024-26085, CVE-2024-26089, CVE-2024-26090, CVE-2024-26091, CVE-2024-26054, CVE-2024-26055, CVE-2024-26086, CVE-2024-36172, CVE-2024-36181, CVE-2024-36182, CVE-2024-36183, CVE-2024-36185, CVE-2024-36186, CVE-2024-36187, CVE-2024-36188, CVE-2024-36189, CVE-2024-36190, CVE-2024-36192, CVE-2024-36193, CVE-2024-36194, CVE-2024-36195, CVE-2024-36196, CVE-2024-36197, CVE-2024-36220, CVE-2024-36222, CVE-2024-36223, CVE-2024-36224, CVE-2024-36228, CVE-2024-36229, CVE-2024-36230, CVE-2024-36231, CVE-2024-36233, CVE-2024-36234, CVE-2024-36235, CVE-2024-36236, CVE-2024-36238, CVE-2024-36239, CVE-2024-26029, CVE-2024-26066, CVE-2024-26068, CVE-2024-26070, CVE-2024-26071, CVE-2024-26088, CVE-2024-26092, CVE-2024-2609, CVE-2024-26095, CVE-2024-26110, CVE-2024-26111, CVE-2024-26113, CVE-2024-26114, CVE-2024-26115, CVE-2024-26116, CVE-2024-26117, CVE-2024-26121, CVE-2024-26123, CVE-2024-20769, CVE-2024-20784, CVE-2024-26060, CVE-2024-34119, CVE-2024-34120, CVE-2024-36141, CVE-2024-36142, CVE-2024-36143, CVE-2024-36144, CVE-2024-36146, CVE-2024-36147, CVE-2024-36148, CVE-2024-36149, CVE-2024-36150, CVE-2024-36151, CVE-2024-36152, CVE-2024-36153, CVE-2024-36154, CVE-2024-36155, CVE-2024-36156, CVE-2024-36157, CVE-2024-36158, CVE-2024-36159, CVE-2024-36160, CVE-2024-36161, CVE-2024-36162, CVE-2024-36163, CVE-2024-36164, CVE-2024-36165, CVE-2024-36166, CVE-2024-36167, CVE-2024-36168, CVE-2024-36169, CVE-2024-36170, CVE-2024-36171, CVE-2024-36173, CVE-2024-36174, CVE-2024-36175, CVE-2024-36176, CVE-2024-36177, CVE-2024-36178, CVE-2024-36179, CVE-2024-36180, CVE-2024-36184, CVE-2024-36191, CVE-2024-36198, CVE-2024-36199, CVE-2024-36200, CVE-2024-36201, CVE-2024-36202, CVE-2024-36203, CVE-2024-36204, CVE-2024-36205, CVE-2024-36206, CVE-2024-36207, CVE-2024-36208, CVE-2024-36209, CVE-2024-36210, CVE-2024-36211, CVE-2024-36212, CVE-2024-36213, CVE-2024-36214, CVE-2024-36215, CVE-2024-36216, CVE-2024-36217, CVE-2024-36218, CVE-2024-36219, CVE-2024-36221, CVE-2024-36225, CVE-2024-26049,

CVE-2024-26126, CVE-2024-26127, CVE-2024-36226, CVE-2024-36232

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 ou d'accéder à des informations confidentielles.

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
- Déni de service

Références

Bulletins de sécurité d'Adobe:

- https://helpx.adobe.com/security/products/acrobat-android/apsb24-50.html
- https://helpx.adobe.com/security/products/creative-cloud/apsb24-44.html
- https://helpx.adobe.com/security/products/substance3d_stager/apsb24-43.html
- https://helpx.adobe.com/security/products/coldfusion/apsb24-41.html
- https://helpx.adobe.com/security/products/magento/apsb24-40.html
- https://helpx.adobe.com/security/products/framemaker-publishing-server/apsb24-38.html
- https://helpx.adobe.com/security/products/media-encoder/apsb24-34.html
- https://helpx.adobe.com/security/products/audition/apsb24-32.html
- https://helpx.adobe.com/security/products/photoshop/apsb24-27.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