**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** | 46931504/24 |
| **Date de Publication** | 15 Avril 2024 |
| **Risque** | Important |
| **Impact** | Important |

## Systèmes affectés

- Adobe Experience Manager (AEM), AEM Cloud Service versions antérieures à 2024.03
- Adobe Experience Manager (AEM), versions antérieures à 6.5.20.0
- Adobe Animate 2023 versions antérieures à 23.0.5
- Adobe Animate 2024 versions antérieures à 24.0.2
- Adobe illustrator 2023 versions antérieures à 27.9.3
- Adobe illustrator 2024 versions antérieures à 28.4
- Adobe Bridge versions antérieures à 13.0.6
- Adobe Bridge versions antérieures à 14.0.2
- Adobe Media Encoder versions antérieures à 24.3
- Adobe Media Encoder versions antérieures à 23.6.5
- Adobe InDesign versions antérieures à ID19.3
- Adobe InDesign versions antérieures à ID18.5.2
- Adobe Commerce version 2.4.7-x antérieures à 2.4.7
- Adobe Commerce version 2.4.6-x antérieures à 2.4.6-p5
- Adobe Commerce version 2.4.5-x antérieures à 2.4.5-p7
- Adobe Commerce version 2.4.4-x antérieures à 2.4.4-p8
- Adobe Commerce version 2.4.3-ext-x antérieures à 2.4.3-ext-7
- Adobe Commerce version 2.4.2-ext-x antérieures à 2.4.2-ext-7
- Adobe Commerce version 2.4.1-ext-x antérieures à 2.4.1-ext-7
- Adobe Commerce version 2.4.0-ext-x antérieures à 2.4.0-ext-7
- Adobe Commerce version 2.3.7-p4-ext-x antérieures à 2.3.7-p4-ext-7
- Magento Open Source versions 2.4.7-x antérieures à 2.4.7
- Magento Open Source versions 2.4.6-x antérieures à 2.4.6-p5
- Magento Open Source versions 2.4.5-x antérieures à 2.4.5-p7

- Magento Open Source versions 2.4.4-x antérieures à 2.4.4-p8
- Photoshop 2023 versions antérieures à 24.7.3
- Photoshop 2024 versions antérieures à 25.4
- Adobe After Effects versions antérieures à 23.6.5

## Identificateurs externes

CVE-2024-20794, CVE-2024-20796, CVE-2024-20795, CVE-2024-20797, CVE-2024-20798, CVE-2024-30272, CVE-2024-30273, CVE-2024-30271, CVE-2024-20771, CVE-2024-20772, CVE-2024-26047, CVE-2024-26076, CVE-2024-26079, CVE-2024-26084, CVE-2024-26087, CVE-2024-26097, CVE-2024-26098, CVE-2024-26122, CVE-2024-20778 CVE-2024-20779 CVE-2024-20780, CVE-2024-20766, CVE-2024-20758, CVE-2024-20759, CVE-2024-20770 CVE-2024-20737

## 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 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
- Déni de service

## Références

Bulletins de sécurité d'Adobe:

- https://helpx.adobe.com/security/products/animate/apsb24-26.html
- https://helpx.adobe.com/security/products/illustrator/apsb24-25.html
- https://helpx.adobe.com/security/products/bridge/apsb24-24.html
- https://helpx.adobe.com/security/products/media-encoder/apsb24-23.html

- https://helpx.adobe.com/security/products/experience-manager/apsb24-21.html
- https://helpx.adobe.com/security/products/indesign/apsb24-20.html
- https://helpx.adobe.com/security/products/magento/apsb24-18.html
- https://helpx.adobe.com/security/products/photoshop/apsb24-16.html
- https://helpx.adobe.com/security/products/after_effects/apsb24-09.html