**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** | 51491212/24 |
| **Date de Publication** | 12 Décembre 2024 |
| **Risque** | Important |
| **Impact** | Critique |

## Systèmes affectés

- Adobe FrameMaker versions antérieures à 2020 Update 7 sur Windows
- Adobe FrameMaker versions antérieures à r 2022 Update 5 sur Windows
- Adobe Substance 3D Painter versions antérieures à 10.1.2
- Adobe Premiere Pro versions antérieures à 25.1 sur Windows et macOS
- Adobe Premiere Pro versions antérieures à 24.6.4 sur Windows et macOS
- Adobe Bridge versions antérieures à 14.1.4 sur Windows et macOS
- Adobe Bridge versions antérieures à 15.0.1 sur Windows et macOS
- Adobe Substance 3D Modeler versions antérieures à 1.15.0
- Adobe Photoshop 2025 versions antérieures à 26.1 sur Windows et macOS
- Adobe Substance 3D Sampler versions antérieures à 4.5.2
- Adobe Connect versions antérieures à 12.7
- Adobe Connect versions antérieures à 11.4.9
- Adobe PDFL Software Development Kit versions antérieures à 21.0.0.7 sur Windows, macOS et Linux
- Adobe InDesign versions antérieures à ID20.0 sur Windows et macOS
- Adobe InDesign versions antérieures à ID19.5.1 sur Windows et macOS
- Adobe Animane 2023 versions antérieures à 23.0.9 sur Windows et macOS
- Adobe Animane 2024 versions antérieures à 24.0.6 sur Windows et macOS
- Adobe After Effects versions antérieures à 24.6.3 sur Windows et macOS
- Adobe After Effects versions antérieures à 25.1 sur Windows et macOS
- Illustrator 2025 versions antérieures à 29.1 sur Windows et macOS
- Illustrator 2024 versions antérieures à 28.7.3 sur Windows et macOS
- Adobe Media Encoder versions antérieures à 24.6.4 sur Windows et macOS
- Adobe Media Encoder versions antérieures à 25.1 sur Windows et macOS

- Acrobat DC versions antérieures à 24.005.20320 sur Windows et macOS
- Acrobat Reader DC versions antérieures à 24.005.20320 sur Windows et macOS
- Acrobat 2020 versions antérieures à 20.005.30748 sur Windows et macOS
- Acrobat Reader 2020 versions antérieures à 20.005.30748 sur Windows et macOS
- Acrobat 2024 versions antérieures à 24.001.30225 sur Windows et macOS
- Adobe Experience Manager Cloud Service versions antérieures à 2024.11
- Adobe Experience Manager versions antérieures à 6.5.22

## Identificateurs externes

| | | | |
|---|---|---|---|
| CVE-2024-53957 | CVE-2024-53958 | CVE-2024-53959 | CVE-2024-53956 |
| CVE-2024-53955 | CVE-2024-52999 | CVE-2024-53000 | CVE-2024-53001 |
| CVE-2024-53002 | CVE-2024-53004 | CVE-2024-53005 | CVE-2024-53003 |
| CVE-2024-53006 | CVE-2024-53007 | CVE-2024-52997 | CVE-2024-52994 |
| CVE-2024-52995 | CVE-2024-52996 | CVE-2024-49550 | CVE-2024-49550 |
| CVE-2024-54032 | CVE-2024-54032 | CVE-2024-54033 | CVE-2024-54033 |
| CVE-2024-54034 | CVE-2024-54034 | CVE-2024-54035 | CVE-2024-54035 |
| CVE-2024-54036 | CVE-2024-54036 | CVE-2024-54037 | CVE-2024-54037 |
| CVE-2024-54038 | CVE-2024-54038 | CVE-2024-54039 | CVE-2024-54039 |
| CVE-2024-54040 | CVE-2024-54040 | CVE-2024-54041 | CVE-2024-54041 |
| CVE-2024-54042 | CVE-2024-54042 | CVE-2024-54043 | CVE-2024-54043 |
| CVE-2024-54044 | CVE-2024-54044 | CVE-2024-54045 | CVE-2024-54045 |
| CVE-2024-54046 | CVE-2024-54046 | CVE-2024-54047 | CVE-2024-54047 |
| CVE-2024-54048 | CVE-2024-54048 | CVE-2024-54049 | CVE-2024-54049 |
| CVE-2024-54050 | CVE-2024-54050 | CVE-2024-54051 | CVE-2024-54051 |
| CVE-2024-54052 | CVE-2024-54052 | CVE-2024-49513 | CVE-2024-49543 |
| CVE-2024-49544 | CVE-2024-49545 | CVE-2024-49546 | CVE-2024-49547 |
| CVE-2024-49548 | CVE-2024-49549 | CVE-2024-53951 | CVE-2024-53952 |
| CVE-2024-45155 | CVE-2024-45156 | CVE-2024-52982 | CVE-2024-52983 |
| CVE-2024-52984 | CVE-2024-52985 | CVE-2024-52986 | CVE-2024-52987 |
| CVE-2024-52988 | CVE-2024-52989 | CVE-2024-52990 | CVE-2024-53953 |
| CVE-2024-53954 | CVE-2024-49537 | CVE-2024-49538 | CVE-2024-49541 |
| CVE-2024-49552 | CVE-2024-49553 | CVE-2024-49554 | CVE-2024-49551 |
| CVE-2024-49532 | CVE-2024-49533 | CVE-2024-49534 | CVE-2024-49530 |
| CVE-2024-49531 | CVE-2024-49535 | CVE-2024-43711 | CVE-2024-43712 |
| CVE-2024-43713 | CVE-2024-43714 | CVE-2024-43715 | CVE-2024-43716 |
| CVE-2024-43717 | CVE-2024-43718 | CVE-2024-43719 | CVE-2024-43720 |
| CVE-2024-43721 | CVE-2024-43722 | CVE-2024-43723 | CVE-2024-43724 |
| CVE-2024-43725 | CVE-2024-43726 | CVE-2024-43727 | CVE-2024-43728 |
| CVE-2024-43729 | CVE-2024-43730 | CVE-2024-43731 | CVE-2024-43732 |
| CVE-2024-43733 | CVE-2024-43734 | CVE-2024-43735 | CVE-2024-43736 |
| CVE-2024-43737 | CVE-2024-43738 | CVE-2024-43739 | CVE-2024-43740 |
| CVE-2024-43742 | CVE-2024-43743 | CVE-2024-43744 | CVE-2024-43745 |
| CVE-2024-43746 | CVE-2024-43747 | CVE-2024-43748 | CVE-2024-43749 |
| CVE-2024-43750 | CVE-2024-43751 | CVE-2024-43752 | CVE-2024-43754 |
| CVE-2024-43755 | CVE-2024-52816 | CVE-2024-52817 | CVE-2024-52818 |
| CVE-2024-52822 | CVE-2024-52823 | CVE-2024-52824 | CVE-2024-52825 |

| | | | |
|---|---|---|---|
| CVE-2024-52826 | CVE-2024-52827 | CVE-2024-52828 | CVE-2024-52829 |
| CVE-2024-52830 | CVE-2024-52831 | CVE-2024-52832 | CVE-2024-52834 |
| CVE-2024-52835 | CVE-2024-52836 | CVE-2024-52837 | CVE-2024-52838 |
| CVE-2024-52839 | CVE-2024-52840 | CVE-2024-52841 | CVE-2024-52842 |
| CVE-2024-52843 | CVE-2024-52844 | CVE-2024-52845 | CVE-2024-52846 |
| CVE-2024-52847 | CVE-2024-52848 | CVE-2024-52849 | CVE-2024-52850 |
| CVE-2024-52851 | CVE-2024-52852 | CVE-2024-52853 | CVE-2024-52854 |
| CVE-2024-52855 | CVE-2024-52857 | CVE-2024-52858 | CVE-2024-52859 |
| CVE-2024-52860 | CVE-2024-52861 | CVE-2024-52862 | CVE-2024-52864 |
| CVE-2024-52865 | CVE-2024-52991 | CVE-2024-52992 | CVE-2024-52993 |
| CVE-2024-53960 | | | |

## 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/experience-manager/apsb24-69.html
- https://helpx.adobe.com/security/products/acrobat/apsb24-92.html
- https://helpx.adobe.com/security/products/media-encoder/apsb24-93.html
- https://helpx.adobe.com/security/products/illustrator/apsb24-94.html
- https://helpx.adobe.com/security/products/after_effects/apsb24-95.html
- https://helpx.adobe.com/security/products/animate/apsb24-96.html
- https://helpx.adobe.com/security/products/indesign/apsb24-97.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

- https://helpx.adobe.com/security/products/pdfl-sdk1/apsb24-98.html
- https://helpx.adobe.com/security/products/connect/apsb24-99.html
- https://helpx.adobe.com/security/products/substance3d-sampler/apsb24-100.html
- https://helpx.adobe.com/security/products/photoshop/apsb24-101.html
- https://helpx.adobe.com/security/products/substance3d-modeler/apsb24-102.html
- https://helpx.adobe.com/security/products/bridge/apsb24-103.html
- https://helpx.adobe.com/security/products/premiere_pro/apsb24-104.html
- https://helpx.adobe.com/security/products/substance3d_painter/apsb24-105.html
- https://helpx.adobe.com/security/products/framemaker/apsb24-106.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