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	45181312/23
Date de Publication	13 Décembre 2023
Risque	Important
Impact	Important

Systèmes affectés

- Adobe InDesign versions antérieures à la version ID19.1sur Windows et macOS
- Adobe InDesign versions antérieures à la version ID18.5.1 sur Windows et macOS
- Adobe Illustrator 2024 versions antérieures à la version 28.1
- Adobe Illustrator 2023 versions antérieures à la version 27.9.1
- Adobe Dimension versions antérieures à la version 3.4.11
- Adobe Experience Manager versions antérieures à la version 6.5.19.0
- Adobe Experience Manager Cloud service versions antérieures à la version 2023.11
- Adobe Substance 3D Sampler versions antérieures à la version 4.2.2
- Adobe After Effects versions antérieures à la version 24.0.3
- Adobe After Effects versions antérieures à la version 23.6.0
- Adobe Substance 3D Designer versions antérieures à la version 13.1.0

Identificateurs externes

CVE-2023-48636, CVE-2023-48637, CVE-2023-48638, CVE-2023-48639, CVE-2023-48632, CVE-2023-48633, CVE-2023-48634, CVE-2023-48635, CVE-2023-48625, CVE-2023-48626, CVE-2023-48627, CVE-2023-48628, CVE-2023-48629, CVE-2023-48630, CVE-2023-47080, CVE-2023-47081, CVE-2023-47078, CVE-2023-47079, CVE-2023-47061, CVE-2023-47062, CVE-2023-47074, CVE-2023-47075, CVE-2023-47063, CVE-2023-44362, CVE-2023-48440, CVE-2023-48512, CVE-2023-48513, CVE-2023-48515, CVE-2023-48533, CVE-2023-48534, CVE-2023-48537, CVE-2023-48572, CVE-2023-48573, CVE-2023-48574, CVE-2023-48575, CVE-2023-48576, CVE-2023-48579, CVE-2023-48580, CVE-2023-48581, CVE-2023-48582,

CVE-2023-48584, CVE-2023-48608

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.

Risque

- Exécution de code arbitraire
- Accès à des informations confidentielles
- Contournement de mesures de sécurité
- Déni de service

Référence

Bulletins de sécurité d'Adobe:

- https://helpx.adobe.com/security/products/prelude/apsb23-67.html
- https://helpx.adobe.com/security/products/illustrator/apsb23-68.html
- https://helpx.adobe.com/security/products/indesign/apsb23-70.html
- https://helpx.adobe.com/security/products/dimension/apsb23-71.html
- https://helpx.adobe.com/security/products/experience-manager/apsb23-72.html
- https://helpx.adobe.com/security/products/substance3d_stager/apsb23-73.html
- https://helpx.adobe.com/security/products/substance3d-sampler/apsb23-74.html
- https://helpx.adobe.com/security/products/after_effects/apsb23-75.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/substance3d_designer/apsb23-76.html