ROYAUME DU MAROC
ADMINISTRATION
DE LA DEFENSE NATIONALE
Direction Générale de la Sécurité des Systèmes d'Information

المملكة المغربية
إدارة الدفاع الوطني
المديرية العامة لأمن نظم المعلومات

BULLETIN DE SECURITE

Titre	Vulnérabilités critiques dans les produits Adobe
Numéro de Référence	63201504/26
Date de Publication	15 Avril 2026
Risque	Critique
Impact	Critique

Systèmes affectés

- Adobe ColdFusion 2025 versions antérieures à la version Update 7
- Adobe ColdFusion 2023 versions antérieures à la version Update 19
- Photoshop 2026 versions antérieures à 27.5
- Illustrator 2025 versions antérieures à 29.8.6
- Illustrator 2026 versions antérieures à 30.3
- Acrobat DC versions antérieures à 26.001.21431
- Acrobat Reader DC versions antérieures à 26.001.21431
- Acrobat 2024 (Windows) versions antérieures à 24.001.30365
- Adobe InDesign versions antérieures à ID21.3
- Adobe InDesign versions antérieures à ID20.5.3
- Adobe InCopy versions antérieures à 20.5.3
- Adobe InCopy versions antérieures à 21.3
- Adobe Experience Manager (AEM) Écrans 6.5 Service Pack 24 ou version antérieure
- Adobe Experience Manager (AEM) Écrans Feature Pack 11.7 ou version antérieure
- Adobe FrameMaker 2022 Version mise à jour 8 et antérieure

Direction Générale de la Sécurité des Systèmes d'Information,
Centre de Veille de Détection et de Réaction aux Attaques Informatiques, Méchouar Saïd,
B.P. 1048 Rabat – 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 ، المشور السعيد، ص.ب. 1048 الرباط
هاتف: 47 21 57 37 05 – فاكس: 53 20 57 37 05
البريد الإلكتروني contact@macert.gov.ma

- Adobe Connect version 12.10 et antérieurs
- Adobe Connect Desktop Application version antérieure à 2025.9
- Adobe Bridge 15.1.4 (LTS) et versions antérieures
- Adobe Bridge 16.0.2 et versions antérieures
- Kit de développement logiciel Adobe DNG SDK 1.7.1 build 2502 et versions antérieures

Identificateurs externes

- CVE-2026-21331 CVE-2026-27222 CVE-2026-27238 CVE-2026-27243 CVE-2026-27245
- CVE-2026-27246 CVE-2026-27258 CVE-2026-27259 CVE-2026-27260 CVE-2026-27282
- CVE-2026-27283 CVE-2026-27284 CVE-2026-27285 CVE-2026-27286 CVE-2026-27287
- CVE-2026-27288 CVE-2026-27289 CVE-2026-27290 CVE-2026-27291 CVE-2026-27292
- CVE-2026-27293 CVE-2026-27294 CVE-2026-27295 CVE-2026-27296 CVE-2026-27297
- CVE-2026-27298 CVE-2026-27299 CVE-2026-27300 CVE-2026-27301 CVE-2026-27302
- CVE-2026-27303 CVE-2026-27304 CVE-2026-27305 CVE-2026-27306 CVE-2026-27307
- CVE-2026-27308 CVE-2026-27310 CVE-2026-27311 CVE-2026-27312 CVE-2026-27313
- CVE-2026-34614 CVE-2026-34615 CVE-2026-34617 CVE-2026-34618 CVE-2026-34619
- CVE-2026-34621 CVE-2026-34622 CVE-2026-34623 CVE-2026-34624 CVE-2026-34625
- CVE-2026-34626 CVE-2026-34627 CVE-2026-34628 CVE-2026-34629 CVE-2026-34630
- CVE-2026-34631

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 distant non authentifié ou faiblement privilégié d'exécuter du code arbitraire, de causer un déni de service, de contourner des mécanismes de sécurité, de réussir une élévation de privilèges ou de compromettre les systèmes ciblés.

Solution

Veuillez se référer au bulletin de sécurité Adobe du 14 Avril 2026**.**

Risque

- Accès aux informations confidentielles ;
- Contournement de la politique de sécurité ;

- Elévation de privilèges ;
- Déni de service (DoS) ;
- Exécution du code arbitraire à distance ;

Annexe

Bulletin de sécurité Adobe du 14 Avril 2026**:**

- https://helpx.adobe.com/security/products/indesign/apsb26-32.html
- https://helpx.adobe.com/security/products/incopy/apsb26-33.html
- https://helpx.adobe.com/security/products/aem-screens/apsb26-34.html
- https://helpx.adobe.com/security/products/framemaker/apsb26-36.html
- https://helpx.adobe.com/security/products/connect/apsb26-37.html
- https://helpx.adobe.com/security/products/bridge/apsb26-39.html
- https://helpx.adobe.com/security/products/dng-sdk/apsb26-41.html
- https://helpx.adobe.com/security/products/photoshop/apsb26-40.html
- https://helpx.adobe.com/security/products/illustrator/apsb26-42.html
- https://helpx.adobe.com/security/products/acrobat/apsb26-43.html
- https://helpx.adobe.com/security/products/coldfusion/apsb26-38.html
- https://helpx.adobe.com/security/products/acrobat/apsb26-44.html

Direction Générale de la Sécurité des Systèmes d'Information,
Centre de Veille de Détection et de Réaction aux Attaques Informatiques, Méchouar Saïd,
B.P. 1048 Rabat – 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 ، المشور السعيد، ص.ب. 1048 الرباط
هاتف: 47 21 57 37 05 – فاكس: 53 20 57 37 05
البريد الإلكتروني contact@macert.gov.ma