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	44201110/23
Date de Publication	11 Octobre 2023
Risque	Important
Impact	Important

Systèmes affectés

- Adobe commerce 2.4.7-beta1 et versions antérieures
- Adobe commerce 2.4.6-p2 et versions antérieures
- Adobe commerce 2.4.5-p4 et versions antérieures
- Adobe commerce 2.4.4-p5 et versions antérieures
- Adobe commerce 2.4.3-ext-4 et versions antérieures
- Adobe commerce 2.4.2-ext-4 et versions antérieures
- Adobe commerce 2.4.1-ext-4 et versions antérieures
- Adobe commerce 2.4.0-ext-4 et versions antérieures
- Adobe commerce 2.3.7-p4-ext-4 et versions antérieures
- Magento Open Source 2.4.7-beta1 et versions antérieures
- Magento Open Source 2.4.6-p2 et versions antérieures
- Magento Open Source 2.4.5-p4 et versions antérieures
- Magento Open Source 2.4.4-p5 et versions antérieures
- Photoshop 2022 23.5.5 et versions antérieures sur Windows and macOS
- Photoshop 2023 24.7 et versions antérieures sur Windows and macOS
- Adobe Bridge 12.0.4 et versions antérieures sur Windows and macOS
- Adobe Bridge 13.0.3 et versions antérieures sur Windows and macOS

Identificateurs externes

CVE-2023-38216 CVE-2023-38217 CVE-2023-26370 CVE-2023-26366
CVE-2023-26367 CVE-2023-26368 CVE-2023-38218 CVE-2023-38219
CVE-2023-38220 CVE-2023-38221 CVE-2023-38249 CVE-2023-38250
CVE-2023-38251

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 contourner des mesures de sécurité.

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

Référence

Bulletins de sécurité d'Adobe:

- https://helpx.adobe.com/security/products/magento/apsb23-50.html
- https://helpx.adobe.com/security/products/photoshop/apsb23-51.html
- https://helpx.adobe.com/security/products/bridge/apsb23-49.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