



BULLETIN DE SECURITE

Titre	Vulnérabilités affectant plusieurs produits d'Adobe
Numéro de Référence	40811503/23
Date de Publication	15 Mars 2023
Risque	Important
Impact	Important

Systemes affectés

- Adobe Commerce versions antérieures à 2.4.6, 2.4.5-p2, 2.4.4-p3
- Adobe Magento Open Source versions antérieures à 2.4.6, 2.4.5-p2, 2.4.4-p3
- Adobe Adobe Experience Manager (AEM) Cloud Service versions antérieures à 2023.1
- Adobe Adobe Experience Manager (AEM) versions antérieures à 6.5.16.0
- Adobe Illustrator 2023 versions antérieures à 27.3.1
- Adobe Dimension versions antérieures à 3.4.8
- Adobe Creative Cloud Desktop Application versions antérieures à 5.10 sur Windows
- Adobe Substance 3D Stager versions antérieures à 2.0.1
- Photoshop 2022 versions antérieures à 23.5.4
- Photoshop 2023 versions antérieures à 24.2.1
- Adobe ColdFusion 2018 versions antérieures à Update 16
- Adobe ColdFusion 2021 versions antérieures à Update 6

Identificateurs externes

CVE-2023-22247, CVE-2023-22249, CVE-2023-22250, CVE-2023-22251, CVE-2023-26426,
CVE-2023-22252, CVE-2023-22253, CVE-2023-22254, CVE-2023-22256, CVE-2023-22257,
CVE-2023-22258, CVE-2023-22259, CVE-2023-22260, CVE-2023-22261, CVE-2023-22262,
CVE-2023-22263, CVE-2023-22264, CVE-2023-22265, CVE-2023-22266, CVE-2023-22269,
CVE-2023-22271, CVE-2023-21615, CVE-2023-21616, CVE-2023-25859, CVE-2023-25860,
CVE-2023-25861, CVE-2023-25862, CVE-2023-25879, CVE-2023-25880, CVE-2023-25881,
CVE-2023-25882, CVE-2023-25883, CVE-2023-25884, CVE-2023-25885, CVE-2023-25886,
CVE-2023-25887, CVE-2023-25888, CVE-2023-25889, CVE-2023-25890, CVE-2023-25891,
CVE-2023-25892, CVE-2023-25893, CVE-2023-25894, CVE-2023-25895, CVE-2023-25896,
CVE-2023-25900, CVE-2023-25902, CVE-2023-25905, CVE-2023-25906, CVE-2023-25907,
CVE-2023-26327, CVE-2023-26328, CVE-2023-26329, CVE-2023-26333, CVE-2023-26335,
CVE-2023-26338, CVE-2023-26339, CVE-2023-26340, CVE-2023-26341, CVE-2023-26342,
CVE-2023-26343, CVE-2023-26344, CVE-2023-26345, CVE-2023-26346, CVE-2023-26348,
CVE-2023-26349, CVE-2023-25897, CVE-2023-25898, CVE-2023-25899, CVE-2023-25901,
CVE-2023-26330, CVE-2023-26331, CVE-2023-26350, CVE-2023-26351, CVE-2023-26352,
CVE-2023-26353, CVE-2023-26354, CVE-2023-26355, CVE-2023-26356, CVE-2023-26332,
CVE-2023-26334, CVE-2023-26336, CVE-2023-26337, CVE-2023-25903, CVE-2023-25904,
CVE-2023-26358, CVE-2023-25863, CVE-2023-25864, CVE-2023-25865, CVE-2023-25866,
CVE-2023-25867, CVE-2023-25868, CVE-2023-25869, CVE-2023-25870, CVE-2023-25871,
CVE-2023-25872, CVE-2023-25873, CVE-2023-25874, CVE-2023-25875, CVE-2023-25876,
CVE-2023-25877, CVE-2023-25878, CVE-2023-25908, CVE-2023-26359, CVE-2023-26360,
CVE-2023-26361

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 données confidentielles, ou de contourner des mesures de sécurité.

Solution

Veillez se référer aux bulletins de sécurité d'Adobe pour l'obtention des correctifs.

Risque

- Exécution de code arbitraire
- Accès à des données confidentielles
- Contournement de mesures de sécurité

Référence

Bulletins de sécurité d'Adobe:

<https://helpx.adobe.com/security/products/magento/apsb23-17.html>

<https://helpx.adobe.com/security/products/experience-manager/apsb23-18.html>

<https://helpx.adobe.com/security/products/illustrator/apsb23-19.html>

<https://helpx.adobe.com/security/products/dimension/apsb23-20.html>

<https://helpx.adobe.com/security/products/creative-cloud/apsb23-21.html>

https://helpx.adobe.com/security/products/substance3d_stager/apsb23-22.html

<https://helpx.adobe.com/security/products/photoshop/apsb23-23.html>

<https://helpx.adobe.com/security/products/coldfusion/apsb23-25.html>