



BULLETIN DE SECURITE

Titre	Vulnérabilités critiques affectant plusieurs produits d'Adobe
Numéro de Référence	56701009/25
Date de Publication	10 Septembre 2025
Risque	Important
Impact	Critique

Systèmes affectés

- Acrobat DC versions antérieures à 25.001.20693 sur Windows et macOS
- Acrobat Reader DC versions antérieures à 25.001.20693 sur Windows et macOS
- Acrobat 2020 versions antérieures à 20.005.30793 sur Windows et 20.005.30791 sur macOS
- Acrobat Reader 2020 versions antérieures à 20.005.30793 sur Windows et 20.005.30791 sur macOS
- Acrobat 2024 versions antérieures à 24.001.30264 sur Windows et macOS
- Adobe After Effects versions antérieures à 24.6.8 sur Windows et macOS
- Adobe After Effects versions antérieures à 25.4 sur Windows et macOS
- Adobe Premiere Pro versions antérieures à 25.4 sur Windows et macOS
- Adobe Premiere Pro versions antérieures à 24.6.8 sur Windows et macOS
- Adobe Substance 3D Viewer versions antérieures à 0.25.2
- Adobe Commerce version 2.4.9-x sans le dernier Hotfix
- Adobe Commerce version 2.4.8-x sans le dernier Hotfix
- Adobe Commerce version 2.4.7-x sans le dernier Hotfix
- Adobe Commerce version 2.4.6-x sans le dernier Hotfix
- Adobe Commerce version 2.4.5-x sans le dernier Hotfix
- Adobe Commerce version 2.4.4-x sans le dernier Hotfix
- Adobe Commerce B2B version 1.5.3-x sans le dernier Hotfix
- Adobe Commerce B2B version 1.5.2-x sans le dernier Hotfix
- Adobe Commerce B2B version 1.4.2-x sans le dernier Hotfix
- Adobe Commerce B2B version 1.3.4-x sans le dernier Hotfix
- Adobe Commerce B2B version 1.3.3-x sans le dernier Hotfix

- Magento Open Source versions 2.4.9-x sans le dernier Hotfix
- Magento Open Source versions 2.4.8-x sans le dernier Hotfix
- Magento Open Source versions 2.4.7-x sans le dernier Hotfix
- Magento Open Source versions 2.4.6-x sans le dernier Hotfix
- Magento Open Source versions 2.4.5-x sans le dernier Hotfix
- Adobe Experience Manager (AEM) versions antérieures à AEM Cloud Service Release 2025.9
- Adobe Experience Manager (AEM) versions antérieures à 6.5 LTS SP1 (GRANITE-61551 Hotfix)
- Adobe Experience Manager (AEM) versions antérieures à 6.5.23 (GRANITE-61551 Hotfix)
- Adobe Dreamweaver versions antérieures à 21.6 sur Windows et macOS
- Adobe Substance 3D Modeler versions antérieures à 1.22.4
- ColdFusion 2025 versions antérieures à update 4
- ColdFusion 2023 versions antérieures à update 16
- ColdFusion 2021 versions antérieures à update 22

Identificateurs externes

CVE-2025-54257	CVE-2025-54255	CVE-2025-54239	CVE-2025-54240
CVE-2025-54241	CVE-2025-54242	CVE-2025-54236	CVE-2025-54243
CVE-2025-54244	CVE-2025-54245	CVE-2025-54248	CVE-2025-54246
CVE-2025-54247	CVE-2025-54249	CVE-2025-54250	CVE-2025-54251
CVE-2025-54252	CVE-2025-54256	CVE-2025-54258	CVE-2025-54260
CVE-2025-54259	CVE-2025-54261		

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.

Risques

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

Références

Bulletins de sécurité d'Adobe:

- <https://helpx.adobe.com/security/products/acrobat/apsb25-85.html>
- http://helpx.adobe.com/security/products/after_effects/apsb25-86.html
- https://helpx.adobe.com/security/products/premiere_pro/apsb25-87.html
- <https://helpx.adobe.com/security/products/magento/apsb25-88.html>
- <https://helpx.adobe.com/security/products/substance3d-viewer/apsb25-89.html>
- <https://helpx.adobe.com/security/products/experience-manager/apsb25-90.html>
- <https://helpx.adobe.com/security/products/dreamweaver/apsb25-91.html>
- <https://helpx.adobe.com/security/products/substance3d-modeler/apsb25-92.html>
- <https://helpx.adobe.com/security/products/coldfusion/apsb25-93.html>