



.....  
Centre de Veille de Détection et de  
Réaction aux Attaques Informatiques

## BULLETIN DE SECURITE

|                            |                                                               |
|----------------------------|---------------------------------------------------------------|
| <b>Titre</b>               | Vulnérabilités critiques affectant plusieurs produits d'Adobe |
| <b>Numéro de Référence</b> | 54401405/25                                                   |
| <b>Date de Publication</b> | 14 Mai 2025                                                   |
| <b>Risque</b>              | Important                                                     |
| <b>Impact</b>              | Critique                                                      |

### Systèmes affectés

- Adobe lightroom versions antérieures à 8.3
- Adobe Dreamweaver versions antérieures à 21.5
- Adobe Connect versions antérieures à 12.9
- Adobe InDesign versions antérieures à ID20.3 sur Windows et macOS
- Adobe InDesign versions antérieures à ID19.5.3 sur Windows et macOS
- Adobe Substance 3D Painter versions antérieures à 11.0.1
- Adobe Photoshop 2025 versions antérieures à 26.6
- Adobe Photoshop 2024 versions antérieures à 25.12.3
- Adobe Animate 2023 versions antérieurs à 23.0.12 sur Windows et macOS
- Adobe Animate 2024 versions antérieurs à 24.0.9 sur Windows et macOS
- Illustrator 2025 versions antérieures à 29.4 sur Windows et macOS
- Illustrator 2024 versions antérieures à 28.7.6 sur Windows et macOS
- Adobe Bridge versions antérieures à 14.1.7 sur Windows et macOS
- Adobe Bridge versions antérieures à 15.0.4 sur Windows et macOS
- Adobe Dimension versions antérieures à 4.1.2
- Adobe Substance 3D Stager versions antérieures à 3.1.2
- Adobe Substance 3D Modeler versions antérieures à 1.22.0
- Adobe Coldusion 2025 versions antérieures à update 2
- Adobe Coldusion 2023 versions antérieures à update 14
- Adobe Coldusion 2021 versions antérieures à update 20

## Identificateurs externes

|                |                |                |                |                |
|----------------|----------------|----------------|----------------|----------------|
| CVE-2025-43561 | CVE-2025-43563 | CVE-2025-43564 | CVE-2025-43566 | CVE-2025-43559 |
| CVE-2025-43560 | CVE-2025-43562 | CVE-2025-43565 | CVE-2025-43553 | CVE-2025-43554 |
| CVE-2025-43549 | CVE-2025-43568 | CVE-2025-43570 | CVE-2025-43571 | CVE-2025-43551 |
| CVE-2025-43569 | CVE-2025-43548 | CVE-2025-43572 | CVE-2025-43545 | CVE-2025-43546 |
| CVE-2025-43547 | CVE-2025-30330 | CVE-2025-30329 | CVE-2025-43555 | CVE-2025-43556 |
| CVE-2025-43557 | CVE-2025-30324 | CVE-2025-30325 | CVE-2025-30326 | CVE-2025-30322 |
| CVE-2025-30318 | CVE-2025-30319 | CVE-2025-30320 | CVE-2025-30314 | CVE-2025-30315 |
| CVE-2025-30316 | CVE-2025-43567 | CVE-2025-30328 | CVE-2025-30310 | CVE-2025-27197 |

## Bilan de la vulnérabilité

Adobe a publié des mises à jour de sécurité qui permettent de corriger plusieurs vulnérabilités critiques affectant ses produits susmentionnés. L'exploitation de ces vulnérabilités peut permettre à un attaquant d'exécuter du code arbitraire, d'élever ses privilèges, d'accéder à des informations confidentielles ou de causer un déni de service

## Solution

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

## Risques

- Exécution de code arbitraire
- Elévation de privilèges
- Accès à des informations confidentielles
- Déni de service

## Références

Bulletins de sécurité d'Adobe:

- <https://helpx.adobe.com/security/products/lightroom/apsb25-29.html>
- <https://helpx.adobe.com/security/products/dreamweaver/apsb25-35.html>
- <https://helpx.adobe.com/security/products/connect/apsb25-36.html>
- <https://helpx.adobe.com/security/products/indesign/apsb25-37.html>
- [https://helpx.adobe.com/security/products/substance3d\\_paint/apsb25-38.html](https://helpx.adobe.com/security/products/substance3d_paint/apsb25-38.html)
- <https://helpx.adobe.com/security/products/photoshop/apsb25-40.html>

- <https://helpx.adobe.com/security/products/animate/apsb25-42.html>
- <https://helpx.adobe.com/security/products/illustrator/apsb25-43.html>
- <https://helpx.adobe.com/security/products/bridge/apsb25-44.html>
- <https://helpx.adobe.com/security/products/dimension/apsb25-45.html>
- [https://helpx.adobe.com/security/products/substance3d\\_stager/apsb25-46.html](https://helpx.adobe.com/security/products/substance3d_stager/apsb25-46.html)
- <https://helpx.adobe.com/security/products/substance3d-modeler/apsb25-51.html>
- <https://helpx.adobe.com/security/products/coldfusion/apsb25-52.html>